

Contents

[Security Center documentation](#)

[Overview](#)

[About Security Center](#)

[Supported platforms](#)

[Supported features](#)

[Quickstarts](#)

[Azure subscriptions](#)

[Windows computers](#)

[Linux computers](#)

[Azure Stack virtual machines](#)

[Tutorials](#)

[Protect your resources](#)

[Respond to incidents](#)

[Improve your regulatory compliance](#)

[Concepts](#)

[Secure Score in Security Center](#)

[The enhanced Secure Score](#)

[Permissions](#)

[Data security](#)

[Use recommendations to enhance security](#)

[Cross-tenant management](#)

[Container security](#)

[Container security overview](#)

[Integration with Azure Container Registry](#)

[Integration with Azure Kubernetes Service](#)

[Threat protection and security alerts](#)

[Security alerts overview](#)

[Reference list of alerts](#)

[Manage security alerts](#)

- [Manage security incidents](#)
- [Threat protection in Azure Security Center](#)
- [Cloud Smart Alert correlation \(incidents\)](#)
- [Security alerts map and threat intelligence](#)
- [Alert validation \(EICAR test file\)](#)
- [How-to guides](#)
 - [Upgrade to advanced security](#)
 - [Scan your VMs for vulnerabilities](#)
 - [Vulnerability scanning overview](#)
 - [Integrated vulnerability scanner for VMs](#)
 - [Using external scanners](#)
 - [Monitor your containers](#)
 - [Protect your servers with Microsoft Defender ATP](#)
 - [Use advanced data security for SQL on Azure VMs](#)
 - [Use App Service to protect your applications](#)
 - [Use security policies](#)
 - [Overview of security policies](#)
 - [Use built-in security policies](#)
 - [Create custom security policies](#)
 - [Manage policies with the Azure Policy REST API](#)
 - [Add dynamic compliance packages](#)
 - [Customize the information protection policy](#)
 - [Manage security solutions](#)
 - [Automate onboarding using PowerShell](#)
 - [Integrate with Windows Admin Center](#)
 - [Compare baselines using File Integrity Monitoring](#)
 - [Automate responses to alerts and recommendations](#)
 - [Export alerts and recommendations](#)
 - [Configure your data collection](#)
 - [Set up advanced threat protection for Azure Key Vault](#)
 - [Set up email notifications](#)
 - [Pricing](#)

[Gain tenant-wide visibility](#)

[Implement security recommendations](#)

[What are security recommendations](#)

[Remediate recommendations](#)

[Strengthen security posture](#)

[Reference list of recommendations](#)

[Protect your machines and apps](#)

[Protect network resources](#)

[Protect data and storage services](#)

[Protect identity and access](#)

[Apply cloud defenses](#)

[Manage just-in-time access](#)

[Adaptive application controls](#)

[File integrity monitoring](#)

[Adaptive network hardening](#)

[Archive](#)

[Apply disk encryption](#)

[Apply system updates](#)

[Install Endpoint Protection](#)

[Threat reports](#)

[Alert confidence score](#)

[Investigation](#)

[Manage investigation user data](#)

[Planning and operations](#)

[Reference](#)

[REST APIs](#)

[FAQ for Azure Security Center](#)

[General questions](#)

[Billing questions](#)

[Permissions questions](#)

[Data collection and agent questions](#)

[Virtual Machines questions](#)

[Existing users of Azure Log Analytics](#)

[Release notes](#)

[Features and API retirement \(July 2019\)](#)

[Endpoint protection assessment and recommendations](#)

[Resources](#)

[Build your skills with Microsoft Learn](#)

[Manage user data](#)

[Azure Security Center for IoT documentation](#)

[Azure security documentation](#)

[Azure updates](#)

[Readiness Roadmap](#)

[Azure Security, Privacy, & Compliance blog](#)

[Azure Security Center on Stack Overflow](#)

[Videos](#)

[Pricing](#)

[Regional availability](#)

[Troubleshooting guide](#)

What is Azure Security Center?

2/27/2020 • 9 minutes to read • [Edit Online](#)

Azure Security Center is a unified infrastructure security management system that strengthens the security posture of your data centers, and provides advanced threat protection across your hybrid workloads in the cloud - whether they're in Azure or not - as well as on premises.

Keeping your resources safe is a joint effort between your cloud provider, Azure, and you, the customer. You have to make sure your workloads are secure as you move to the cloud, and at the same time, when you move to IaaS (infrastructure as a service) there is more customer responsibility than there was in PaaS (platform as a service), and SaaS (software as a service). Azure Security Center provides you the tools needed to harden your network, secure your services and make sure you're on top of your security posture.

Azure Security Center addresses the three most urgent security challenges:

- **Rapidly changing workloads** – It's both a strength and a challenge of the cloud. On the one hand, end users are empowered to do more. On the other, how do you make sure that the ever-changing services people are using and creating are up to your security standards and follow security best practices?
- **Increasingly sophisticated attacks** – Wherever you run your workloads, the attacks keep getting more sophisticated. You have to secure your public cloud workloads, which are, in effect, an Internet facing workload that can leave you even more vulnerable if you don't follow security best practices.
- **Security skills are in short supply** – The number of security alerts and alerting systems far outnumbers the number of administrators with the necessary background and experience to make sure your environments are protected. Staying up-to-date with the latest attacks is a constant challenge, making it impossible to stay in place while the world of security is an ever-changing front.

To help you protect yourself against these challenges, Security Center provides you with the tools to:

- **Strengthen security posture:** Security Center assesses your environment and enables you to understand the status of your resources, and whether they are secure.
- **Protect against threats:** Security Center assesses your workloads and raises threat prevention recommendations and security alerts.
- **Get secure faster:** In Security Center, everything is done in cloud speed. Because it is natively integrated, deployment of Security Center is easy, providing you with autoprovioning and protection with Azure services.

NOTE

This service supports [Azure delegated resource management](#), which lets service providers sign in to their own tenant to manage subscriptions and resource groups that customers have delegated. For more info, see [Azure Lighthouse](#).

Architecture

Because Security Center is natively part of Azure, PaaS services in Azure - including Service Fabric, SQL databases, and storage accounts - are monitored and protected by Security Center without necessitating any deployment.

In addition, Security Center protects non-Azure servers and virtual machines in the cloud or on premises, for both Windows and Linux servers, by installing the Microsoft Monitoring Agent on them. Azure virtual machines are

auto-provisioned in Security Center.

The events collected from the agents and from Azure are correlated in the security analytics engine to provide you tailored recommendations (hardening tasks), that you should follow to make sure your workloads are secure, and security alerts. You should investigate such alerts as soon as possible to make sure malicious attacks aren't taking place on your workloads.

When you enable Security Center, the security policy built-in to Security Center is reflected in Azure Policy as a built in initiative under Security Center category. The built-in initiative is automatically assigned to all Security Center registered subscriptions (Free or Standard tiers). The built-in initiative contains only Audit policies. For more information about Security Center policies in Azure Policy, see [Working with security policies](#).

Strengthen security posture

Azure Security Center enables you to strengthen your security posture. This means it helps you identify and perform the hardening tasks recommended as security best practices and implement them across your machines, data services, and apps. This includes managing and enforcing your security policies, and making sure your Azure virtual machines, non-Azure servers, and Azure PaaS services are compliant. Security Center provides you with the tools you need to have a bird's eye view on your workloads, with focused visibility on your network security estate.

Manage organization security policy and compliance

It's a security basic to know and make sure your workloads are secure, and it starts with having tailored security policies in place. Because all the policies in Security Center are built on top of Azure policy controls, you're getting the full range and flexibility of a **world-class policy solution**. In Security Center, you can set your policies to run on management groups, across subscriptions, and even for a whole tenant.

 Policy Management

Manage the security policies by choosing a subscription or management group from the list below. In order to define additional policies, manage exclusions and advanced settings, go to [Azure policies >](#)

[Click here to learn more >](#)

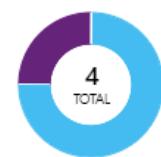
7 MANAGEMENT GROUPS 4 SUBSCRIPTIONS 20 WORKSPACES

| NAME | POLICY INITIATIVE ASSIGNMENT(S) | COMPLIANCE | COVERAGE | SETTINGS |
|---|---|------------|------------------------------------|------------------------------------|
| Rome ILDC - Detection Prod Test 1 | ASC Default (subscription: 845d028d-fc71-4c45-b41d-a47b | 32% | Standard | Edit settings > |
| Visual Studio Enterprise | | --- | Free | Edit settings > |
| 72f988bf-86f1-41af-91ab-2d7cd011db47 (2 of 8 subscriptions) | ⚠ Limited permissions | --- | Edit settings > | |
| BenKligerMG (1 of 1 subscriptions) | ⚠ Limited permissions | --- | | |
| ASC DEMO | [Preview]: Enable Monitoring in Azure Security Center | 27% | Standard | Edit settings > |
| Contoso (1 of 7 subscriptions) | ⚠ Limited permissions | --- | | |
| Applications (0 of 5 subscriptions) | ⚠ Limited permissions | --- | | |
| IT (1 of 2 subscriptions) | ⚠ Limited permissions | --- | | |
| Application Team (1 of 1 subscriptions) | ⚠ Limited permissions | --- | | |
| Contoso IT - demo | [Preview]: Enable Monitoring in Azure Security Center | 13% | Standard | Edit settings > |
| Infrastructure Team (0 of 1 subscriptions) | ⚠ Limited permissions | --- | | |

Security Center helps you **identify Shadow IT subscriptions**. By looking at subscriptions labeled **not covered** in your dashboard, you can know immediately when there are newly created subscriptions and make sure they are covered by your policies, and protected by Azure Security Center.

Policy & compliance

Subscription coverage



394 Covered resources

Policy compliance

Overall compliance



17%

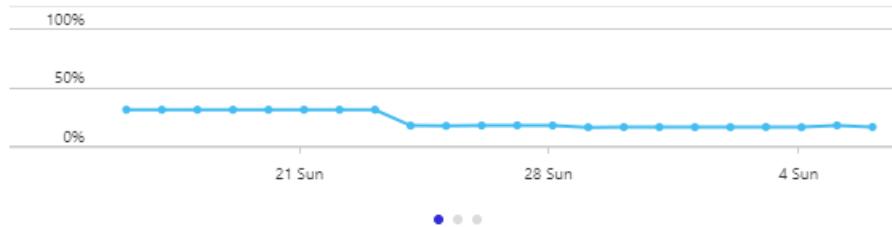
Least compliant subscriptions

- Contoso IT - demo 13%
- ASC DEMO 27%

Show policy compliance of your environment >

The advanced monitoring capabilities in Security Center also let you **track and manage compliance and governance over time**. The **overall compliance** provides you with a measure of how much your subscriptions are compliant with policies associated with your workload.

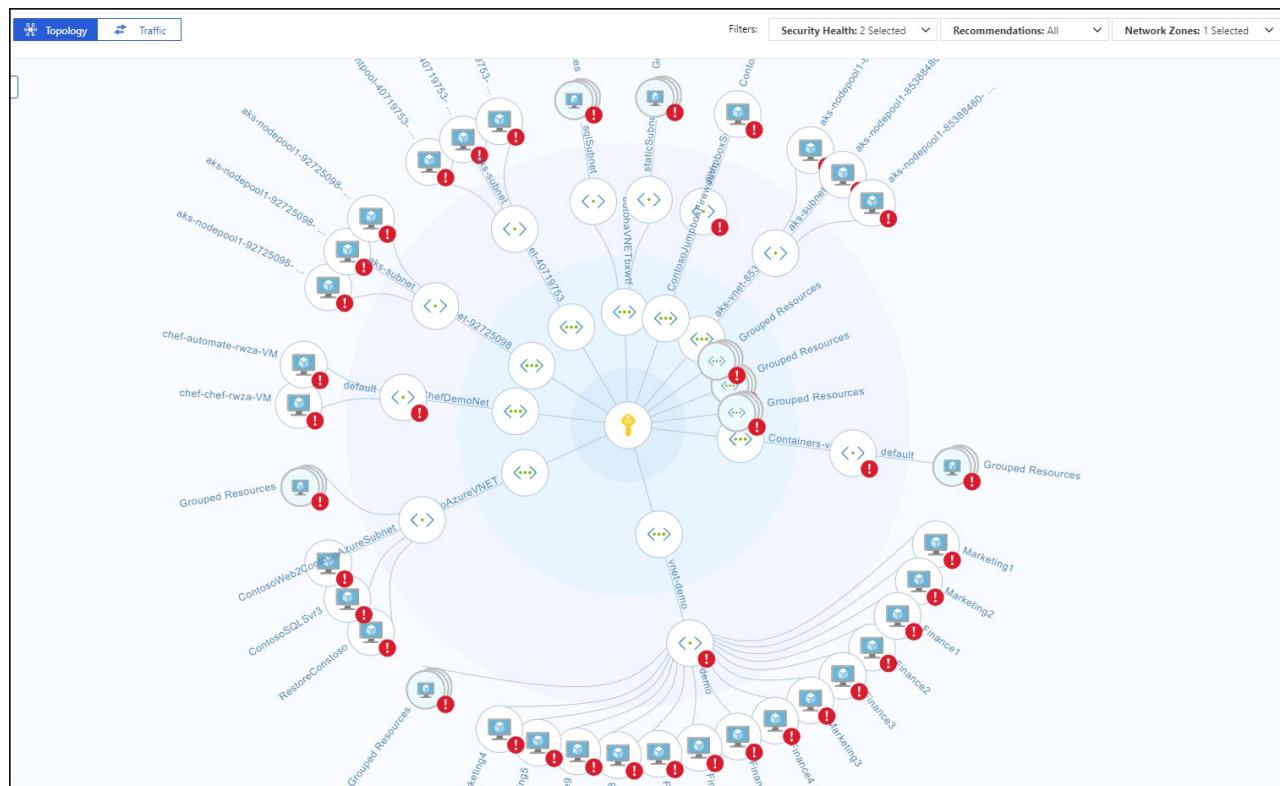
Policy compliance over time



Continuous assessments

Security Center continuously discovers new resources that are being deployed across your workloads and assesses whether they are configured according to security best practices, if not, they're flagged and you get a prioritized list of recommendations for what you need to fix in order to protect your machines.

One of the most powerful tools Security Center provides for continuously monitoring the security status of your network is the **Network map**. The map enables you to see the topology of your workloads, so you can see if each node is properly configured. You can see how your nodes are connected, which helps you block unwanted connections that could potentially make it easier for an attacker to creep along your network.

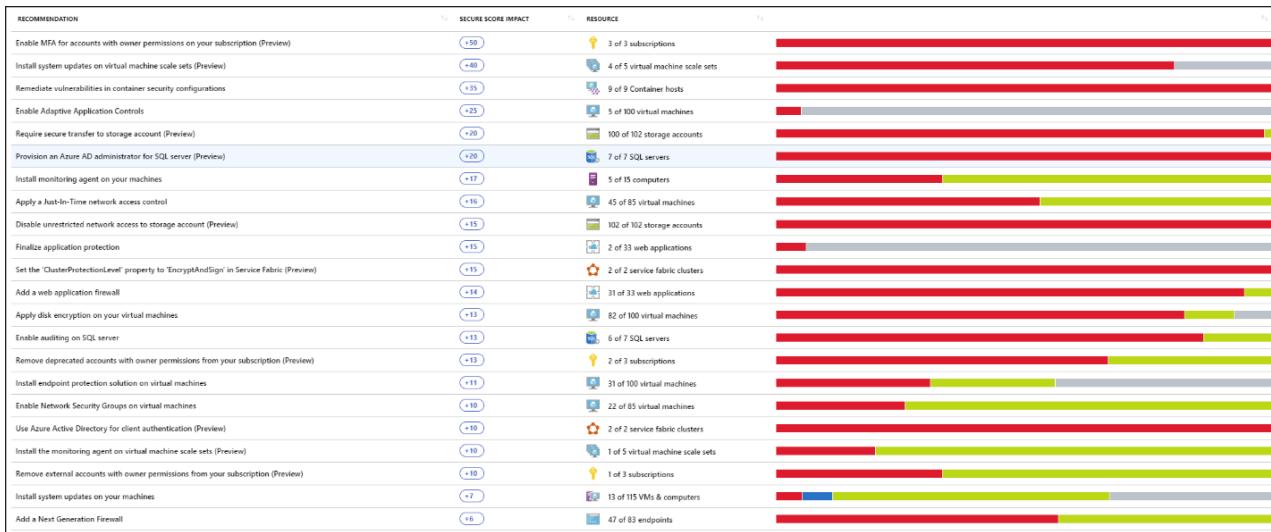


Security Center makes mitigating your security alerts one step easier, by adding a **Secure Score**. The Secure Scores are now associated with each recommendation you receive to help you understand how important each recommendation is to your overall security posture. This is crucial in enabling you to **prioritize your security work**.



Optimize and improve security by configuring recommended controls

The heart of Azure Security Center's value lies in its recommendations. The recommendations are tailored to the particular security concerns found on your workloads, and Security Center does the security admin work for you, by not only finding your vulnerabilities, but providing you with specific instructions for how to get rid of them.



In this way, Security Center enables you not just to set security policies, but to apply secure configuration standards across your resources.

The recommendations help you to reduce the attack surface across each of your resources. That includes Azure virtual machines, non-Azure servers, and Azure PaaS services such as SQL and Storage accounts and more - where each type of resource is assessed differently and has its own standards.

Enable auditing on SQL server

Description
Enable auditing on your SQL Server to track database activities across all databases on the server and save them in an audit log.

General Information

| | |
|-----------------------|------|
| RECOMMENDATION SCORE | 2/15 |
| RECOMMENDATION IMPACT | +15 |
| USER IMPACT | Low |
| IMPLEMENTATION COST | Low |

Threats

- Data exfiltration
- Data spillage
- Malicious insider
- Threat resistance

Remediation steps

To enable SQL server auditing:

1. Select the SQL server.
2. Under Auditing, select On.
3. Select Storage details and configure a storage account for the audit log.
4. Click Save.

Unhealthy resources Healthy resources
6 **1**

Unhealthy resources (6) [Healthy resources \(1\)](#) [Uncanned resources \(0\)](#)

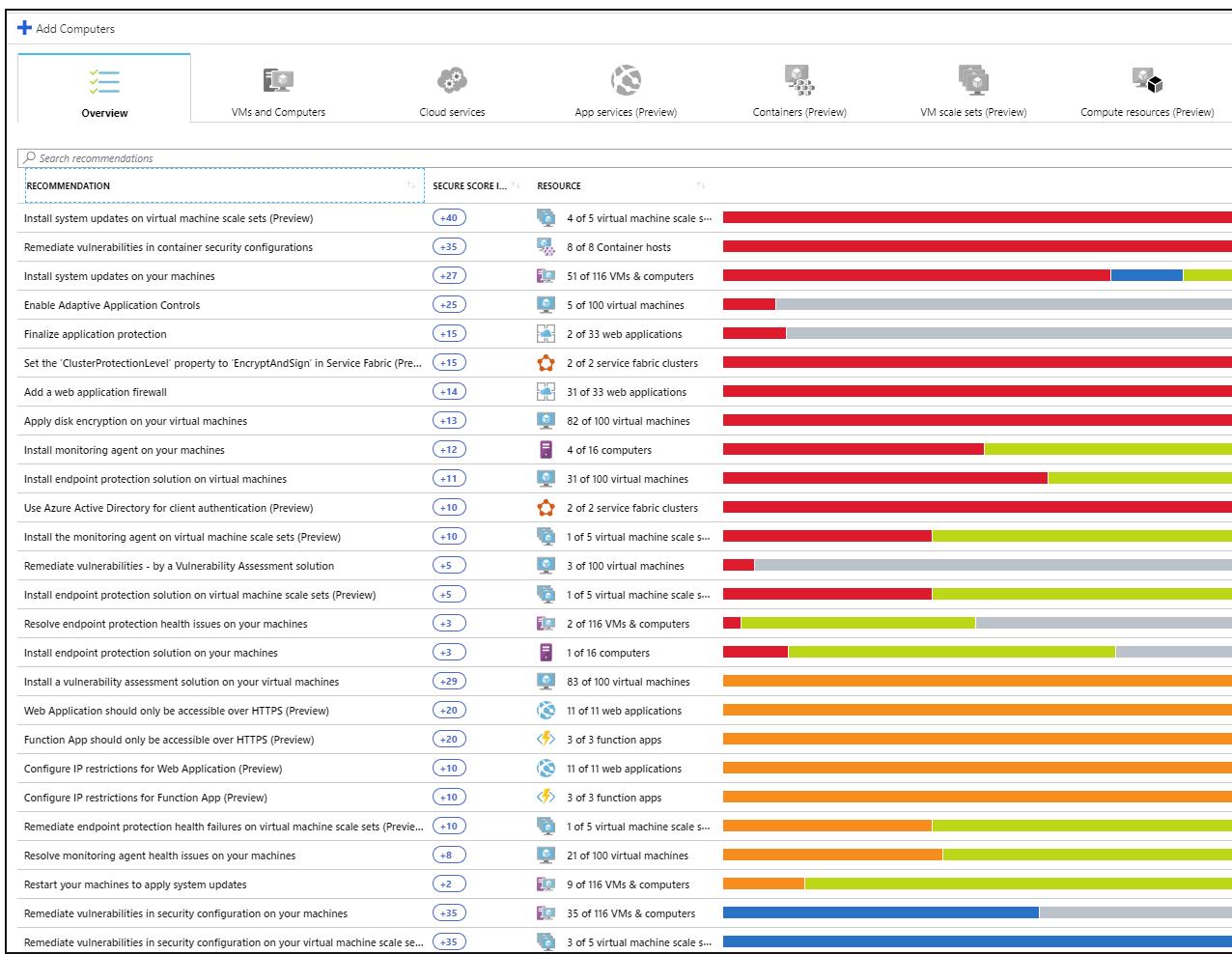
[Search SQL servers](#)

| NAME | SUBSCRIPTION |
|----------------------------|--------------------------------------|
| sqlserver1ascdemo | ASC DEMO |
| sqlserver2ascdemo | ASC DEMO |
| contososerver23 | Contoso IT - demo |
| contososembs | Contoso IT - demo |
| socsqldb | Microsoft Azure Internal Consumption |
| csids | Rome ILDC - Detection Prod Test |
| sqlinjectionalertgenerator | |

Protect against threats

Security Center's threat protection enables you to detect and prevent threats at the Infrastructure as a Service (IaaS) layer, non-Azure servers as well as for Platforms as a Service (PaaS) in Azure.

Security Center's threat protection includes fusion kill-chain analysis, which automatically correlates alerts in your environment based on cyber kill-chain analysis, to help you better understand the full story of an attack campaign, where it started and what kind of impact it had on your resources.



Integration with Microsoft Defender Advanced threat protection

Security Center includes automatic, native integration with Microsoft Defender Advanced Threat Protection. This means that without any configuration, your Windows and Linux machines are fully integrated with Security Center's recommendations and assessments.

In addition, Security Center lets you automate application control policies on server environments. The adaptive application controls in Security Center enable end-to-end app whitelisting across your Windows servers. You don't need to create the rules and check violations, it's all done automatically for you.

Protect PaaS

Security Center helps you detect threats across Azure PaaS services. You can detect threats targeting Azure services including Azure App Service, Azure SQL, Azure Storage Account, and more data services. You can also take advantage of the native integration with Microsoft Cloud App Security's User and Entity Behavioral Analytics (UEBA) to perform anomaly detection on your Azure activity logs.

Block brute force attacks

Security Center helps you limit exposure to brute force attacks. By reducing access to virtual machine ports, using the just-in-time VM access, you can harden your network by preventing unnecessary access. You can set secure access policies on selected ports, for only authorized users, allowed source IP address ranges or IP addresses, and for a limited amount of time.

Security incident detected

Incident Detected

| | |
|-------------------|--|
| DESCRIPTION | The incident which started on 2018-11-06 01:02:00Z and most recently detected on 2018-11-07 10:02:00Z indicate that an attacker has attacked other resources from your virtual machine vm1 |
| ACTIVITY TIME | Wednesday, November 7, 2018, 12:02:00 PM |
| SEVERITY | ! High |
| STATE | Active |
| ATTACKED RESOURCE | vm1 |
| SUBSCRIPTION | ASC DEMO (212f9889-769e-45ae-ab43-6da33674bd26) |
| DETECTED BY | ■ Microsoft |
| ACTION TAKEN | Detected |
| ENVIRONMENT | Azure |
| REMEDIATION STEPS | <ol style="list-style-type: none"> Escalate the alert to the information security team. Review the remediation steps of each one of the alerts |

Alerts included in this incident

| DESCRIPTION | COUNT | ACTIVITY TIME | ATTACKED RESOURCE | SEVERITY |
|---|-------|-------------------|-------------------|--|
| SQL injection blocked | 1 | 11/06/18, 3:02 AM | vm1 | ! Low |
| Failed RDP Brute Force Attack | 1 | 11/06/18, 4:02 AM | vm1 | ! Low |
| Successful RDP brute force attack | 1 | 11/07/18, 4:02 AM | vm1 | ! High |
| Suspicious SVCHOST process executed | 1 | 11/07/18, 5:02 AM | vm1 | ! Low |
| Multiple Domain Accounts Queried | 1 | 11/07/18, 6:02 AM | vm1 | ! Low |
| Network communication with a malicious m... | 1 | 11/07/18, 7:02 AM | vm1 | ! Medium |

Protect data services

Security Center includes capabilities that help you perform automatic classification of your data in Azure SQL. You can also get assessments for potential vulnerabilities across Azure SQL and Storage services, and recommendations for how to mitigate them.

Protect IoT and hybrid cloud workloads

Azure Security Center for IoT (Internet of Things) simplifies hybrid workload protection by delivering unified visibility and control, adaptive threat prevention, and intelligent threat protection and response across workloads running on edge, on-premises, in Azure, and in other clouds. For more information, see [Azure Security Center for IoT](#).

Get secure faster

Native Azure integration (including Azure Policy and Azure Monitor logs) combined with seamless integration with other Microsoft security solutions, such as Microsoft Cloud App Security and Windows Defender Advanced Threat Protection help make sure your security solution is comprehensive as well as simple to onboard and roll out.

In addition, you can extend the full solution beyond Azure to workloads running on other clouds and in on-premises data centers.

Automatically discover and onboard Azure resources

Security Center provides seamless, native integration with Azure and Azure resources. That means that you can pull together a complete security story involving Azure Policy and built-in Security Center policies across all your Azure resources, and make sure that the whole thing is automatically applied to newly discovered resources as you create them in Azure.

Extensive log collection - logs from Windows and Linux are all leveraged in the security analytics engine and used to create recommendations and alerts.

Next steps

- To get started with Security Center, you need a subscription to Microsoft Azure. If you do not have a subscription, you can sign up for a [free trial](#).
- Security Center's free pricing tier is enabled with your Azure subscription. To take advantage of advanced security management and threat protection capabilities, you must upgrade to the standard pricing tier. The standard tier can be tried for free for 30 days. For more information, see the [Security Center pricing page](#).
- If you're ready to enable Security Center standard now, the [Quickstart: Onboard your Azure subscription to Security Center Standard](#) walks you through the steps.

Supported platforms

2/27/2020 • 2 minutes to read • [Edit Online](#)

Virtual machines / servers

Security Center supports virtual machines / servers on different types of hybrid environments:

- Only Azure
- Azure and on-premises
- Azure and other clouds
- Azure, other clouds, and on-premises

For an Azure environment activated on an Azure subscription, Azure Security Center will automatically discover IaaS resources that are deployed within the subscription.

NOTE

To receive the full set of security features, you must have the [Log Analytics Agent](#), which is used by Azure Security Center, installed and [properly configured to send data to Azure Security Center](#).

The following sections list the supported server operating systems on which the [Log Analytics Agent](#), which is used by Azure Security Center, can run.

Windows server operating systems

| OS | SUPPORTED BY AZURE SECURITY CENTER | SUPPORT FOR INTEGRATION WITH MICROSOFT DEFENDER ATP |
|------------------------|------------------------------------|---|
| Windows Server 2019 | ✓ | X |
| Windows Server 2016 | ✓ | ✓ |
| Windows Server 2012 R2 | ✓ | ✓ |
| Windows Server 2008 R2 | ✓ | ✓ |

To learn more about the supported features for the Windows operating systems, listed above, see [Virtual machine / server supported features](#).

Windows operating systems

Azure Security Center integrates with Azure services to monitor and protect your Windows-based virtual machines.

Linux operating systems

64-bit

- CentOS 6 and 7
- Amazon Linux 2017.09
- Oracle Linux 6 and Oracle Linux 7
- Red Hat Enterprise Linux Server 6 and 7
- Debian GNU/Linux 8 and 9

- Ubuntu Linux 14.04 LTS, 16.04 LTS, and 18.04 LTS
- SUSE Linux Enterprise Server 12

32-bit

- CentOS 6
- Oracle Linux 6
- Red Hat Enterprise Linux Server 6
- Debian GNU/Linux 8 and 9
- Ubuntu Linux 14.04 LTS, and 16.04 LTS

NOTE

Since the list of supported Linux operating systems is constantly changing, if you prefer, click [here](#) to view the most up-to-date list of supported versions, in case there have been changes since this topic was last published.

To learn more about the supported features for the Linux operating systems, listed above, see [Virtual machine / server supported features](#).

Managed virtual machine services

Virtual machines are also created in a customer subscription as part of some Azure managed services as well, such as Azure Kubernetes (AKS), Azure Databricks, and more. These virtual machines are also discovered by Azure Security Center, and the Log analytics agent can be installed and configured according the supported [Windows/Linux operating systems](#), listed above.

Cloud Services

Virtual machines that run in a cloud service are also supported. Only cloud services web and worker roles that run in production slots are monitored. To learn more about cloud services, see [Overview of Azure Cloud Services](#).

PaaS Services

The following Azure PaaS resources are supported by Azure Security Center:

- SQL
- PostGreSQL
- MySQL
- CosmosDB
- Storage account
- App service
- Function
- Cloud Service
- VNet
- Subnet
- NIC
- NSG
- Batch account
- Service fabric account
- Automation account
- Load balancer
- Search
- Service bus namespace

- Stream analytics
- Event hub namespace
- Logic apps
- Redis
- Data Lake Analytics
- Data Lake Store
- Key vault

To learn more about the supported features for the above list of PaaS resources, see [PaaS services supported features](#).

Protection for Virtual Machines residing in Azure Stack is also supported. For more information about Security Center's integration with Azure Stack, see [Onboard your Azure Stack virtual machines to Security Center](#).

Next steps

- Learn how [Security Center collects data and the Log Analytics Agent](#).
- Learn how [Security Center manages and safeguards data](#).
- Learn how to [plan and understand the design considerations to adopt Azure Security Center](#).
- Learn about [features available for the different cloud environments](#).
- Learn more about [threat protection for Windows and Linux machines in Azure Security Center](#).

Supported features available in Azure Security Center

2/27/2020 • 4 minutes to read • [Edit Online](#)

NOTE

Some features are only available with the Standard tier. If you have not already signed up for Security Center's Standard tier, a free trial period is available. For more information, see the [Security Center pricing page](#).

The following sections show Security Center features that are available for their [supported platforms](#).

- [Virtual machines / servers](#)
- [PaaS services](#)

Virtual machine / server supported features

- [Windows](#)
- [Linux](#)

| | Azure Virtual Machines | Azure Virtual Machine Scale Sets | Non-Azure Machines | Pricing | | | |
|--|------------------------------|----------------------------------|--------------------|--|--|--|--|
| Microsoft Defender ATP integration | ✓ (on supported versions) | ✓ (on supported versions) | ✓ | Standard | | | |
| Virtual Machine Behavioral Analytics (and security alerts) | ✓ | ✓ | ✓ | Recommendations (Free) Security alerts (Standard) | | | |
| Fileless security alerts | ✓ | ✓ | ✓ | Standard | | | |
| Network-based security alerts | ✓ | ✓ | - | Standard | | | |
| Just-In-Time VM access | ✓ | - | - | Standard | | | |

| | | | | | |
|--|---|---|---|----------|--|
| | | | | | |
| Native vulnerability assessment | ✓ | - | - | Standard | |
| File Integrity Monitoring | ✓ | ✓ | ✓ | Standard | |
| Adaptive application controls | ✓ | - | ✓ | Standard | |
| Network map | ✓ | ✓ | - | Standard | |
| Adaptive network hardening | ✓ | - | - | Standard | |
| Adaptive network controls | ✓ | ✓ | - | Standard | |
| Regulatory Compliance dashboard & reports | ✓ | ✓ | ✓ | Standard | |
| Recommendations and threat protection on Docker-hosted IaaS containers | - | - | - | Standard | |
| Missing OS patches assessment | ✓ | ✓ | ✓ | Free | |
| Security misconfigurations assessment | ✓ | ✓ | ✓ | Free | |
| Endpoint protection assessment | ✓ | ✓ | ✓ | Free | |
| Disk encryption assessment | ✓ | ✓ | - | Free | |
| Third-party vulnerability assessment | ✓ | - | - | Free | |

| | | | | | | | |
|-----------------------------|---|---|---|------|--|--|--|
| Network security assessment | ✓ | ✓ | - | Free | | | |
|-----------------------------|---|---|---|------|--|--|--|

Supported endpoint protection solutions

The following table provides a matrix of:

- Whether you can use Azure Security Center to install each solution for you.
- Which endpoint protection solutions Security Center can discover. If an endpoint protection solution from this list is discovered, Security Center won't recommend installing one.

For information about when recommendations are generated for each of these protections, see [Endpoint Protection Assessment and Recommendations](#).

| ENDPOINT PROTECTION | PLATFORMS | SECURITY CENTER INSTALLATION | SECURITY CENTER DISCOVERY |
|---|--|------------------------------|---------------------------|
| Windows Defender (Microsoft Antimalware) | Windows Server 2016 | No, Built in to OS | Yes |
| System Center Endpoint Protection (Microsoft Antimalware) | Windows Server 2012 R2, 2012, 2008 R2 (see note below) | Via Extension | Yes |
| Trend Micro – All versions* | Windows Server Family | No | Yes |
| Symantec v12.1.1100+ | Windows Server Family | No | Yes |
| McAfee v10+ | Windows Server Family | No | Yes |
| McAfee v10+ | Linux Server Family | No | Yes * |
| Sophos V9+ | Linux Server Family | No | Yes * |

* The coverage state and supporting data is currently only available in the Log Analytics workspace associated to your protected subscriptions. It isn't reflected in the Azure Security Center portal.

NOTE

- Detection of System Center Endpoint Protection (SCEP) on a Windows Server 2008 R2 virtual machine requires SCEP to be installed after PowerShell 3.0 (or an upper version).
- Detection of Trend Micro protection is supported for Deep Security agents. OfficeScan agents are not supported.

PaaS services supported features

The following PaaS resources are supported by Azure Security Center:

| SERVICE | RECOMMENDATIONS (FREE) | SECURITY ALERTS (STANDARD) | VULNERABILITY ASSESSMENT (STANDARD) |
|---------------|------------------------|----------------------------|-------------------------------------|
| SQL Databases | ✓ | ✓ | ✓ |

| Service | Recommendations (Free) | Security Alerts (Standard) | Vulnerability Assessment (Standard) |
|--------------------------------|------------------------|----------------------------|-------------------------------------|
| Azure Container Registry | - | - | ✓ |
| Azure Kubernetes Service | ✓ | ✓ | - |
| Azure Database for PostgreSQL* | ✓ | ✓ | - |
| Azure Database for MySQL* | ✓ | ✓ | - |
| Azure CosmosDB* | - | ✓ | - |
| Storage Accounts | ✓ | - | - |
| Blob Storage | ✓ | ✓ | - |
| App Service | ✓ | ✓ | - |
| Function app | ✓ | - | - |
| Cloud Services | ✓ | - | - |
| Virtual Network | ✓ | - | - |
| Subnet | ✓ | - | - |
| NIC | ✓ | - | - |
| Network Security Groups | ✓ | - | - |
| Subscription | ✓ ** | ✓ | - |
| Batch account | ✓ | - | - |
| Service Fabric account | ✓ | - | - |
| Automation account | ✓ | - | - |
| Load Balancer | ✓ | - | - |
| Cognitive Search | ✓ | - | - |
| Service Bus namespace | ✓ | - | - |
| Stream analytics | ✓ | - | - |
| Event hub namespace | ✓ | - | - |
| Logic apps | ✓ | - | - |
| Cache for Redis | ✓ | - | - |

| Service | Recommendations (Free) | Security Alerts (Standard) | Vulnerability Assessment (Standard) |
|-------------------------|------------------------|----------------------------|-------------------------------------|
| Data Lake Analytics | ✓ | - | - |
| Azure Data Lake Storage | ✓ | - | - |
| Key Vault | ✓ | ✓ * | - |

* These features are currently supported in preview.

** Azure Active Directory (Azure AD) recommendations are available only for Standard subscriptions.

Next steps

- Learn how [Security Center collects data and the Log Analytics Agent](#).
- Learn how [Security Center manages and safeguards data](#).
- Learn how to [plan and understand the design considerations to adopt Azure Security Center](#).
- Review the [platforms that support security center](#).
- Learn more about [threat protection for Windows and Linux machines in Azure Security Center](#).
- Find [frequently asked questions about Azure Security Center](#).

Quickstart: Onboard your Azure subscription to Security Center Standard

11/6/2019 • 4 minutes to read • [Edit Online](#)

Azure Security Center provides unified security management and threat protection across your hybrid cloud workloads. While the Free tier offers limited security for your Azure resources only, the Standard tier extends these capabilities to on-premises and other clouds. Security Center Standard helps you find and fix security vulnerabilities, apply access and application controls to block malicious activity, detect threats using analytics and intelligence, and respond quickly when under attack. You can try Security Center Standard at no cost. To learn more, see the [pricing page](#).

In this article, you upgrade to the Standard tier for added security and install the Microsoft Monitoring Agent on your virtual machines to monitor for security vulnerabilities and threats.

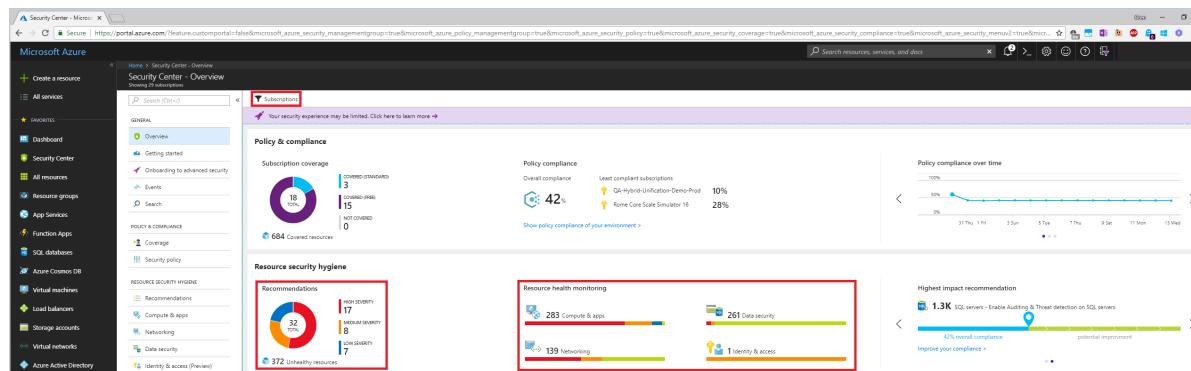
Prerequisites

To get started with Security Center, you must have a subscription to Microsoft Azure. If you do not have a subscription, you can sign up for a [free account](#).

To upgrade a subscription to the Standard tier, you must be assigned the role of Subscription Owner, Subscription Contributor, or Security Admin.

Enable your Azure subscription

1. Sign into the [Azure portal](#).
2. On the **Microsoft Azure** menu, select **Security Center**. **Security Center - Overview** opens.



Security Center – Overview provides a unified view into the security posture of your hybrid cloud workloads, enabling you to discover and assess the security of your workloads and to identify and mitigate risk. Security Center automatically enables any of your Azure subscriptions not previously onboarded by you or another subscription user to the Free tier.

You can view and filter the list of subscriptions by clicking the **Subscriptions** menu item. Security Center will now begin assessing the security of these subscriptions to identify security vulnerabilities. To customize the types of assessments, you can modify the security policy. A security policy defines the desired configuration of your workloads and helps ensure compliance with company or regulatory security requirements.

Within minutes of launching Security Center the first time, you may see:

- **Recommendations** for ways to improve the security of your Azure subscriptions. Clicking the

Recommendations tile will launch a prioritized list.

- An inventory of **Compute & apps**, **Networking**, **Data security**, and **Identity & access** resources that are now being assessed by Security Center along with the security posture of each.

To take full advantage of Security Center, you need to complete the steps below to upgrade to the Standard tier and install the Microsoft Monitoring Agent.

Upgrade to the Standard tier

For the purpose of the Security Center quickstarts and tutorials you must upgrade to the Standard tier. There's a free trial of Security Center Standard. To learn more, see the [pricing page](#).

1. Under the Security Center main menu, select **Getting started**.

Make sure all your subscriptions are upgraded to Security Center Standard Plan. Get started with 60-day free trial

Upgrade to get advanced capabilities including hybrid support, networking, security policies, just-in-time administration and application whitelisting.

Resource Security Hygiene
Understand your security state across cloud workloads from recommendations and resource health monitoring and take action.

Policy & compliance
Gain visibility into your security state and compliance from an organizational level instead of a subscription level.

Intelligent threat detection
Built-in behavioral analysis and machine learning identify potential threats so you can quickly scope the impact of an attack.

Network controls
Identify and remediate network vulnerabilities as well as limit access to your management ports.

Advanced threat protection
Enable actionable adaptive protections powered by machine learning to reduce your overall surface area to attack.

Start trial

Change your plan anytime. After 60 days, Azure Security Center Standard will be applied \$15/node/month. For full threat protection and security management capabilities, start your trial with the Standard plan.

2. Under **Upgrade**, Security Center lists subscriptions and workspaces eligible for onboarding.

- You can click on the expandable **Apply your trial** to see a list of all subscriptions and workspaces with their trial eligibility status.
- You can upgrade subscriptions and workspaces that are not eligible for trial.
- You can select eligible workspaces and subscriptions to start your trial.

3. Click **Start trial** to start your trial on the selected subscriptions.

Make sure all your subscriptions are upgraded to Security Center Standard Plan. Get started with 60-day free trial

Upgrade to get advanced capabilities including hybrid support, networking, security policies, just-in-time administration and application whitelisting.

Resource Security Hygiene
Understand your security state across cloud workloads from recommendations and resource health monitoring and take action.

Policy & compliance
Gain visibility into your security state and compliance from an organizational level instead of a subscription level.

Intelligent threat detection
Built-in behavioral analysis and machine learning identify and notify you of attacks so you can quickly scope the impact of an attack.

Network controls
Identify and remediate network vulnerabilities as well as limit access to your management ports.

Advanced threat protection
Enable actionable adaptive protections powered by machine learning to reduce your overall surface area to attack.

Start trial

Change your plan anytime. After 60 days, Azure Security Center Standard will be applied \$15/node/month. For full threat protection and security management capabilities, start your trial with the Standard plan.

| NAME | RESOURCES | 60 days left in trial |
|-----------|-----------|-----------------------|
| Contoso-1 | 1 | 60 days left in trial |

Automate data collection

Security Center collects data from your Azure VMs and non-Azure computers to monitor for security vulnerabilities and threats. Data is collected using the Microsoft Monitoring Agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. By default, Security Center will create a new workspace for you.

When automatic provisioning is enabled, Security Center installs the Microsoft Monitoring Agent on all supported Azure VMs and any new ones that are created. Automatic provisioning is strongly recommended.

To enable automatic provisioning of the Microsoft Monitoring Agent:

1. Under the Security Center main menu, select **Pricing & settings**.
2. On the row of the subscription, click on the subscription on which you'd like to change the settings.
3. In the **Data Collection** tab, set **Auto provisioning** to **On**.
4. Select **Save**.

The screenshot shows the 'Settings - Data Collection' page in the Azure Security Center. The left sidebar has a 'Data Collection' tab selected. The main area shows the 'Auto Provisioning' section, which is currently set to 'On'. A note explains that this enables automatic installation of the Microsoft Monitoring Agent on all VMs in the subscription. Below this is the 'Default workspace configuration' section, where the 'Use another workspace' option is selected, pointing to a dropdown menu containing 'contosoretail-IT'. A informational callout at the bottom right states: 'Any other solutions enabled on the selected workspace will be applied to Azure VMs that are connected to it. For paid solutions, this could result in additional charges. For data privacy considerations, please make sure your selected workspace is in your desired region.'

With this new insight into your Azure VMs, Security Center can provide additional Recommendations related to system update status, OS security configurations, endpoint protection, as well as generate additional Security alerts.

Recommendations

Filter

Filtered by: State: Open, Resolved

| DESCRIPTION | RESOURCE | STATE | SEVERITY |
|---|--------------------|-------|----------|
| Enable advanced security for subscriptions | 1 subscriptions | Open | High |
| Endpoint Protection not installed on Azure VMs | 6 virtual machines | Open | High |
| Endpoint Protection health failures | 1 VMs & computers | Open | High |
| Add a Next Generation Firewall | 2 endpoints | Open | High |
| Enable Network Security Groups on subnets | shsubnet | Open | High |
| Route traffic through NGFW only | vm3 | Open | High |
| Enable Auditing & Threat detection on SQL servers | 2 SQL Servers | Open | High |
| Remediate vulnerabilities (by Qualys) | 2 virtual machines | Open | High |
| Apply system updates | 2 VMs & computers | Open | High |
| Security configurations mismatch | 60 VMs & computers | Open | Low |

Clean up resources

Other quickstarts and tutorials in this collection build upon this quickstart. If you plan to continue on to work with subsequent quickstarts and tutorials, continue running the Standard tier and keep automatic provisioning enabled. If you do not plan to continue or wish to return to the Free tier:

1. Return to the Security Center main menu and select **Pricing & settings**.
2. Click on the subscription that you want to change to the free tier.
3. Select **Pricing tier** and select **Free** to change subscription from Standard tier to Free tier.
4. Select **Save**.

If you wish to disable automatic provisioning:

1. Return to the Security Center main menu and select **Pricing & settings**.
2. Clean on the subscription that you want to disable automatic provisioning on.
3. In the **Data Collection** tab, set **Auto provisioning** to **Off**.
4. Select **Save**.

NOTE

Disabling automatic provisioning does not remove the Microsoft Monitoring Agent from Azure VMs where the agent has been provisioned. Disabling automatic provisioning limits security monitoring for your resources.

Next steps

In this quickstart you upgraded to Standard tier and provisioned the Microsoft Monitoring Agent for unified security management and threat protection across your hybrid cloud workloads. To learn more about how to use Security Center, continue to the quickstart for onboarding Windows computers that are on-premises and in other clouds.

[Quickstart: Onboard Windows computers to Azure Security Center](#)

Quickstart: Onboard Windows computers to Azure Security Center

11/6/2019 • 3 minutes to read • [Edit Online](#)

After you onboard your Azure subscriptions, you can enable Security Center for resources running outside of Azure, for example on-premises or in other clouds, by provisioning the Microsoft Monitoring Agent.

This quickstart shows you how to install the Microsoft Monitoring Agent on a Windows computer.

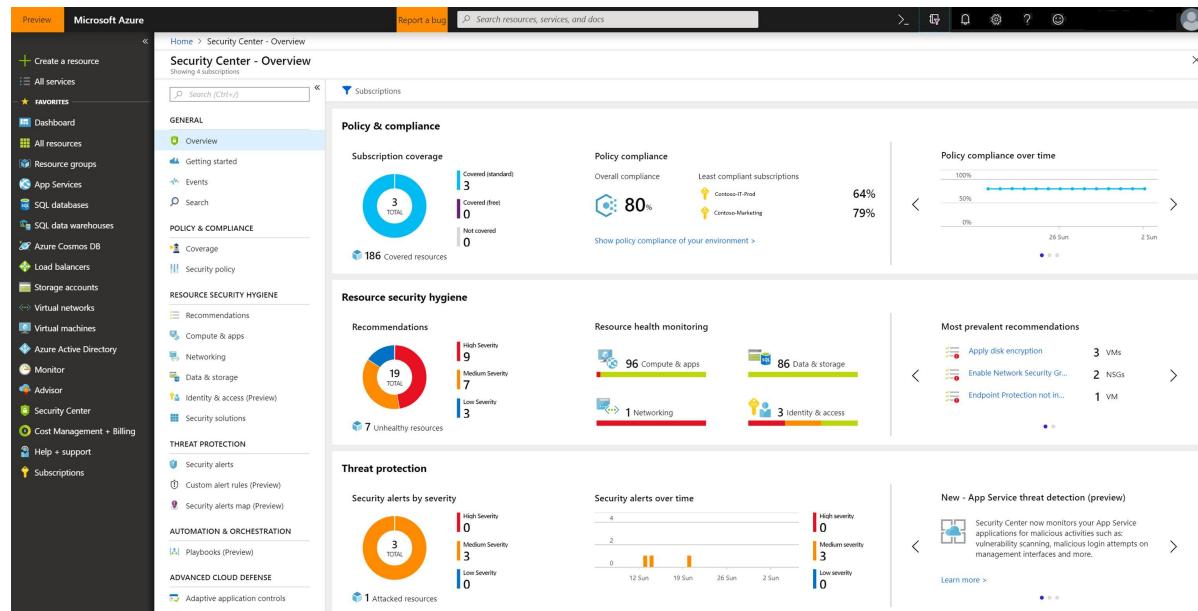
Prerequisites

To get started with Security Center, you must have a subscription to Microsoft Azure. If you do not have a subscription, you can sign up for a [free account](#).

You must be on Security Center's Standard pricing tier before starting this quickstart. See [Onboard your Azure subscription to Security Center Standard](#) for upgrade instructions. You can try Security Center's Standard at no cost. To learn more, see the [pricing page](#).

Add new Windows computer

1. Sign into the [Azure portal](#).
2. On the **Microsoft Azure** menu, select **Security Center**. **Security Center - Overview** opens.



3. Under the Security Center main menu, select **Getting started**.
4. Select the **Get started** tab.

5. Click **Configure** under **Add new non-Azure computers**. A list of your Log Analytics workspaces is shown. The list includes, if applicable, the default workspace created for you by Security Center when automatic provisioning was enabled. Select this workspace or another workspace you want to use.

The **Direct Agent** blade opens with a link for downloading a Windows agent and keys for your workspace ID to use in configuring the agent.

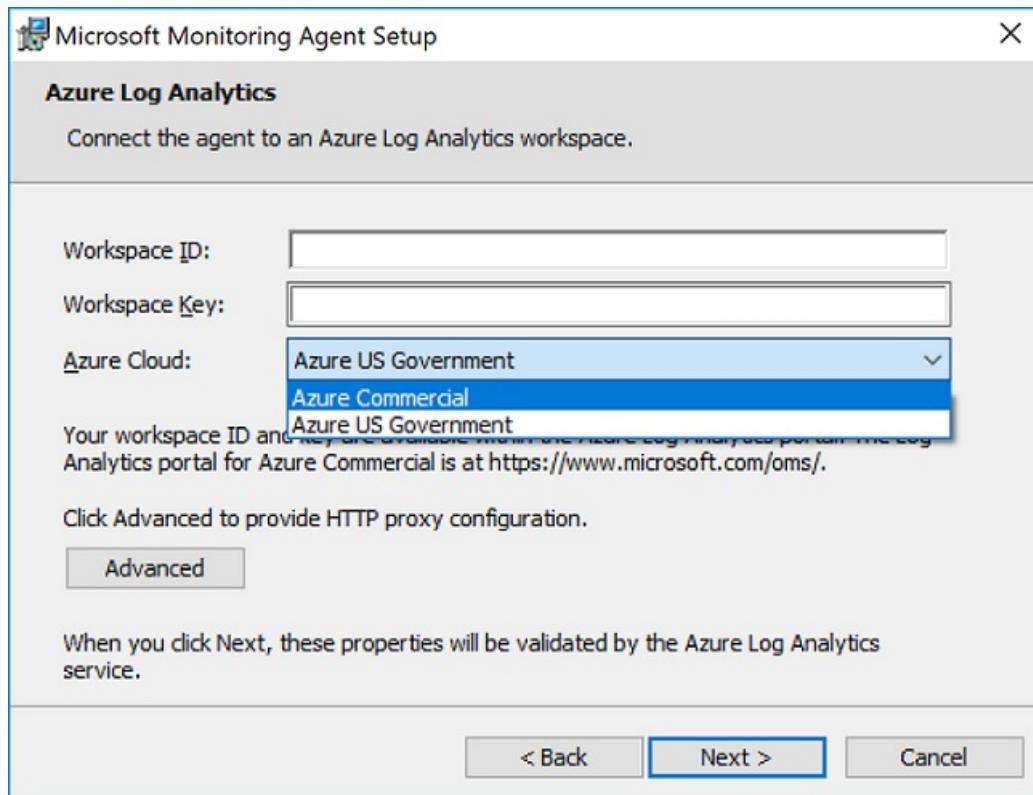
6. Select the **Download Windows Agent** link applicable to your computer processor type to download the setup file.
7. On the right of **Workspace ID**, select the copy icon and paste the ID into Notepad.
8. On the right of **Primary Key**, select the copy icon and paste the key into Notepad.

Install the agent

You must now install the downloaded file on the target computer.

1. Copy the file to the target computer and Run Setup.
2. On the **Welcome** page, select **Next**.
3. On the **License Terms** page, read the license and then select **I Agree**.

4. On the **Destination Folder** page, change or keep the default installation folder and then select **Next**.
5. On the **Agent Setup Options** page, choose to connect the agent to Azure Log Analytics and then select **Next**.
6. On the **Azure Log Analytics** page, paste the **Workspace ID** and **Workspace Key (Primary Key)** that you copied into Notepad in the previous procedure.
7. If the computer should report to a Log Analytics workspace in Azure Government cloud, select **Azure US Government** from the **Azure Cloud** dropdown list. If the computer needs to communicate through a proxy server to the Log Analytics service, select **Advanced** and provide the URL and port number of the proxy server.
8. Select **Next** once you have completed providing the necessary configuration settings.



9. On the **Ready to Install** page, review your choices and then select **Install**.

10. On the **Configuration completed successfully** page, select **Finish**

When complete, the **Microsoft Monitoring Agent** appears in **Control Panel**. You can review your configuration there and verify that the agent is connected.

For further information on installing and configuring the agent, see [Connect Windows computers](#).

Now you can monitor your Azure VMs and non-Azure computers in one place. Under **Compute**, you have an overview of all VMs and computers along with recommendations. Each column represents one set of recommendations. The color represents the VM's or computer's current security state for that recommendation. Security Center also surfaces any detections for these computers in Security alerts.

Filtered By: Power State: Running

| NAME | MONITORED | SYSTEM UPDATES | ENDPOINT PROTECTION | VULNERABILITIES | DISK ENCRYPTION |
|---------------------------|-----------|----------------|---------------------|-----------------|-----------------|
| mgmtvm2 | ▲ | ● | ● | ▲ | ● |
| dr01knWinSrv | ▲ | ● | ● | ▲ | ● |
| dr01knWinSrv-test | ▲ | ● | ● | ▲ | ● |
| ContosoWebVM1 | ▲ | ● | ● | ▲ | ● |
| ContosoAzSRVMI | ▲ | ● | ● | ▲ | ● |
| ContosoAzSRVM2 | ▲ | ● | ● | ▲ | ● |
| ContosoClient1 | ▲ | ● | ● | ● | ● |
| ContosoClient2 | ▲ | ● | ● | ▲ | ● |
| aks-nodepool1-85388480-0 | ▲ | ● | ● | ▲ | ● |
| ContosoAzLnx1 | ▲ | ● | ● | ● | ● |
| vm0 | ● | ● | ● | ▲ | ● |
| infoweb02.contoso.com | ● | ● | ● | ● | ● |
| OpsInsights02.contoso.com | ● | ● | ● | ● | ● |

There are two types of icons represented on the **Compute** blade:



Non-Azure computer



Azure VM

Clean up resources

When no longer needed, you can remove the agent from the Windows computer.

To remove the agent:

1. Open **Control Panel**.
2. Open **Programs and Features**.
3. In **Programs and Features**, select **Microsoft Monitoring Agent** and click **Uninstall**.

Next steps

In this quickstart, you provisioned the Microsoft Monitoring Agent on a Windows computer. To learn more about how to use Security Center, continue to the tutorial for configuring a security policy and assessing the security of your resources.

[Tutorial: Define and assess security policies](#)

Quickstart: Onboard Linux computers to Azure Security Center

11/6/2019 • 2 minutes to read • [Edit Online](#)

After you onboard your Azure subscriptions, you can enable Security Center for Linux resources running outside of Azure, for example on-premises or in other clouds, by provisioning an Agent. The Agent is called the Microsoft Monitoring Agent (MMA), but it is also known as the OMS agent.

This quickstart shows you how to install the Agent on a Linux computer.

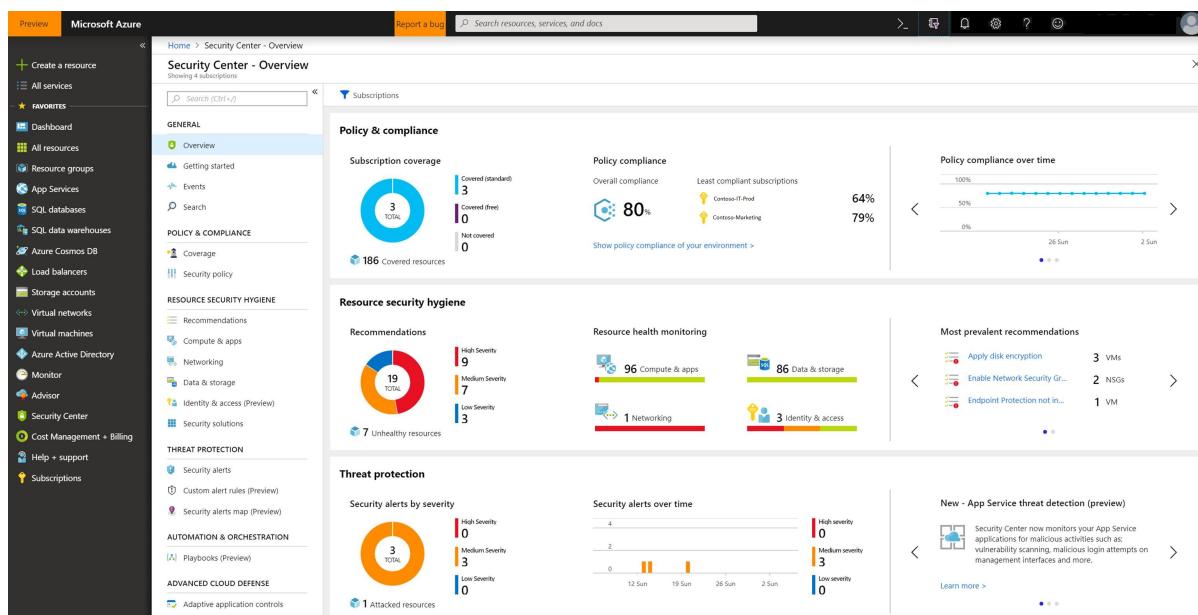
Prerequisites

To get started with Security Center, you must have a subscription to Microsoft Azure. If you do not have a subscription, you can sign up for a [free account](#).

You must be on Security Center's Standard pricing tier before starting this quickstart. See [Onboard your Azure subscription to Security Center Standard](#) for upgrade instructions. You can try Security Center's Standard at no cost. To learn more, see the [pricing page](#).

Add new Linux computer

1. Sign into the [Azure portal](#).
2. On the **Microsoft Azure** menu, select **Security Center**. **Security Center - Overview** opens.



3. Under the Security Center main menu, select **Getting started**.
4. Select the **Get started** tab.

Make sure all your subscriptions are upgraded to Security Center Standard Plan. Get started with 60-day free trial

Upgrade to get advanced capabilities including hybrid support, networking, security policies, just-in-time administration and application whitelisting.

Resource Security Hygiene
Understand your security state across cloud workloads from recommendations and resource health monitoring and take action.

Policy & compliance
Gain visibility into your security state and compliance from an organizational level instead of a subscription level.

Network controls
Identify and remediate network vulnerabilities as well as limit access to your management ports.

Security posture assessments for PaaS
Enable proactive, unified machine-to-machine communication between virtual machines to prevent against threats targeting PaaS resources.

Intelligent threat detection
Rely on behavioral analysis and machine learning identify and notify you of attacks so you can quickly mitigate the impact of an attack.

Advanced threat protection
Enable proactive, adaptive protections powered by machine learning to reduce your overall surface area to attack.

Start trial

Change your plan anytime. After 60 days, Azure Security Center Standard will be applied \$15/month/month. For full threat protection and security management capabilities, start your trial with the Standard plan.

- Click **Configure** under **Add new non-Azure computers**, a list of your Log Analytics workspaces is shown. The list includes, if applicable, the default workspace created for you by Security Center when automatic provisioning was enabled. Select this workspace or another workspace you want to use.

Azure Security Center
Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.

Learn more >

Gain tenant-wide visibility
Gain visibility and manage the security posture of all Azure subscriptions by leveraging Azure management groups and assigning a security role on the root management group.

Learn More

Configure security policies
Set policies to define workload configuration, help ensure compliance, and protect sensitive data.

Configure

Add non-Azure computers
Use the Microsoft Monitoring Agent to extend Security Center agents to computers running outside of Azure, including resources running on-premises and in other clouds.

Configure

- On the **Direct Agent** page, under **DOWNLOAD AND ONBOARD AGENT FOR LINUX**, select the **copy** button to copy the `wget` command.
- Open Notepad, and paste this command. Save this file to a location that can be accessible from your Linux computer.

Install the agent

- On your Linux computer, open the file that was previously saved. Select the entire content, copy, open a terminal console, and paste the command.
- Once the installation is finished, you can validate that the `omsagent` is installed by running the `pgrep` command. The command will return the `omsagent` PID (Process ID) as shown below:

```

FileEditViewSearchTerminalHelp
root@kronos:~# pgrep omsagent
7899
root@kronos:~# 

```

The logs for the Agent can be found at: `/var/opt/microsoft/omsagent/<workspace id>/log/`

```

2017-12-12 13:04:47 -0600 [info]: reading config file path="/etc/opt/microsoft/omsagent/[REDACTED]/conf/omsagent.conf"
2017-12-12 13:04:47 -0600 [info]: starting fluentd-0.12.24 without supervision
2017-12-12 13:04:47 -0600 [info]: gem 'fluentd' version '0.12.24'
2017-12-12 13:04:47 -0600 [info]: adding filter pattern="oms.health.**" type="filter"
2017-12-12 13:04:47 -0600 [info]: adding match pattern="oms.health.**" type="match"
2017-12-12 13:04:47 -0600 [info]: adding source type="out_oms"
2017-12-12 13:04:47 -0600 [info]: adding filter pattern="oms.operation.auditd_plug"
2017-12-12 13:04:47 -0600 [info]: adding filter pattern="oms.operation.**" type="filter"
2017-12-12 13:04:47 -0600 [info]: adding filter pattern="oms.syslog.**" type="filter"
2017-12-12 13:04:47 -0600 [info]: adding match pattern="oms.blob.**" type="out_oms"
2017-12-12 13:04:47 -0600 [info]: adding match pattern="oms.** docker.**" type="filter"
2017-12-12 13:04:47 -0600 [info]: adding match pattern="diag.oms diag.oms.**" type="filter"
2017-12-12 13:04:47 -0600 [info]: adding source type="heartbeat_request"
2017-12-12 13:04:47 -0600 [info]: adding source type="monitor_agent"
2017-12-12 13:04:47 -0600 [info]: adding source type="oms_heartbeat"
2017-12-12 13:04:47 -0600 [info]: adding source type="dsc_monitor"
2017-12-12 13:04:47 -0600 [info]: adding source type="tail"
2017-12-12 13:04:47 -0600 [info]: adding source type="syslog"
2017-12-12 13:04:47 -0600 [info]: adding source type="exec"

```

After some time, it may take up to 30 minutes, the new Linux computer will appear in Security Center.

Now you can monitor your Azure VMs and non-Azure computers in one place. Under **Compute**, you have an overview of all VMs and computers along with recommendations. Each column represents one set of recommendations. The color represents the VM's or computer's current security state for that recommendation. Security Center also surfaces any detections for these computers in Security alerts.

| NAME | MONITORED | SYSTEM UPDATES | ENDPOINT PROTECTION | VULNERABILITIES | DISK ENCRYPTION |
|---------------------------|-----------|----------------|---------------------|-----------------|-----------------|
| mgmtvm2 | ▲ | ● | ● | ▲ | ● |
| dr01knWinSrv | ▲ | ● | ● | ▲ | ● |
| dr01knWinSrv-test | ▲ | ● | ● | ▲ | ● |
| ContosoWebVM1 | ▲ | ● | ● | ▲ | ● |
| ContosoAzASRVM1 | ▲ | ● | ● | ▲ | ● |
| ContosoAzASRVM2 | ▲ | ● | ● | ▲ | ● |
| ContosoClient1 | ▲ | ● | ● | ● | ● |
| ContosoClient2 | ▲ | ● | ● | ▲ | ● |
| aks-nodepool1-85388480-0 | ▲ | ● | ● | ▲ | ● |
| ContosoA2Lnx1 | ▲ | ● | ● | ● | ● |
| vm0 | ● | ● | ● | ▲ | ● |
| infoweb02.contoso.com | ● | ● | ● | ● | ● |
| OpsInsights02.contoso.com | ● | ● | ● | ● | ● |

There are two types of icons represented on the **Compute** blade:



Non-Azure computer



Azure VM

Clean up resources

When no longer needed, you can remove the agent from the Linux computer.

To remove the agent:

1. Download the Linux agent [universal script](#) to the computer.
2. Run the bundle .sh file with the `--purge` argument on the computer, which completely removes the agent and its configuration.

```
sudo sh ./omsagent-<version>.universal.x64.sh --purge
```

Next steps

In this quickstart, you provisioned the agent on a Linux computer. To learn more about how to use Security Center, continue to the tutorial for configuring a security policy and assessing the security of your resources.

[Tutorial: Define and assess security policies](#)

Quickstart: Onboard your Azure Stack virtual machines to Security Center

11/6/2019 • 3 minutes to read • [Edit Online](#)

After you onboard your Azure subscription, you can enable Security Center to protect your virtual machines running on Azure Stack by adding the **Azure Monitor, Update and Configuration Management** virtual machine extension from the Azure Stack marketplace.

This quickstart shows you how to add the **Azure Monitor, Update and Configuration Management** virtual machine extension on a virtual machine (Linux and Windows are both supported) running on Azure Stack.

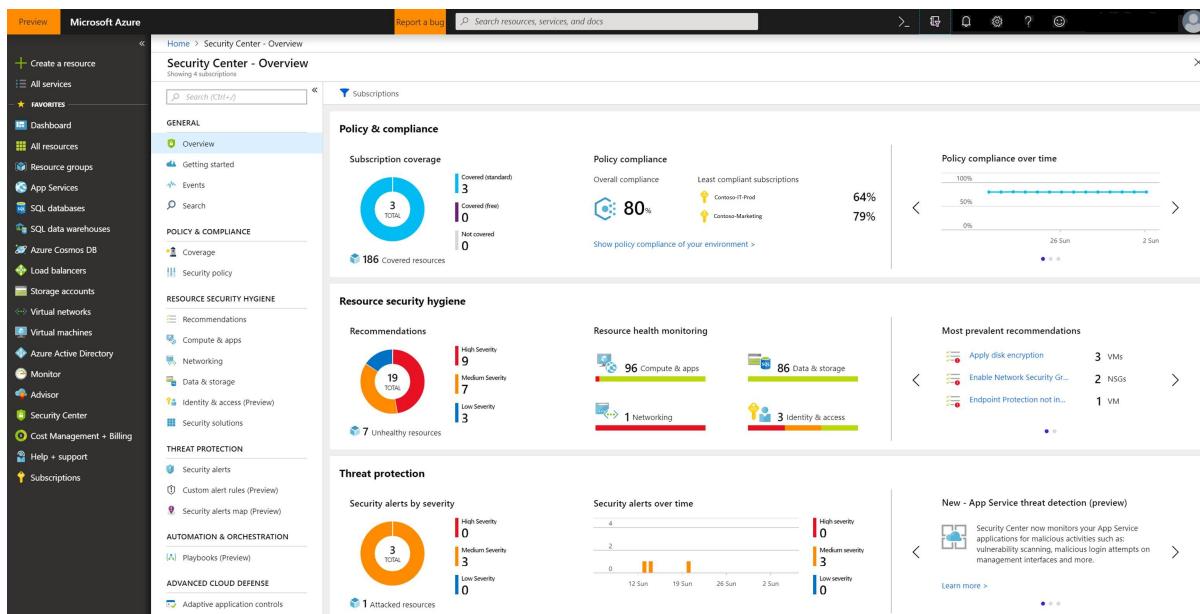
Prerequisites

To get started with Security Center, you must have a subscription to Microsoft Azure. If you do not have a subscription, you can sign up for a [free account](#).

You must have an Azure subscription on Security Center's Standard tier before starting this quickstart. See [Onboard your Azure subscription to Security Center Standard](#) for upgrade instructions. You can try Security Center Standard tier at no cost for 30 days. To learn more, see the [pricing page](#).

Select your workspace in Azure Security Center

1. Sign into the [Azure portal](#).
2. On the **Microsoft Azure** menu, select **Security Center**. **Security Center - Overview** opens.



3. Under the Security Center main menu, select **Getting started**.
4. Select the **Get started** tab.

The screenshot shows the Microsoft Azure Security Center - Getting started page. On the left, there's a sidebar with navigation links for various Azure services like All services, Networks, Dashboard, Resource groups, App Services, SQL databases, Azure Cosmos DB, Load Balancers, Storage accounts, Virtual machines, Virtual networks, Azure Active Directory, Monitor, Advisor, Security Center, Cost Management + Billing, Help + support, and Subscriptions. The main content area has a heading 'Make sure all your subscriptions are upgraded to Security Center Standard Plan. Get started with 60-day free trial'. It includes sections for 'Resource Security Hygiene' (Recommendations, Compute & apps, Networking, Data & storage, Identity & access), 'Policy & compliance' (Security alerts, Custom alert rules (Preview), Security alerts map (Preview)), 'Network controls' (Custom roles (Preview), Security alerts map (Preview)), and 'Threat protection' (Security posture assessments for PaaS, Adaptive application controls, Just in time VM access, File integrity monitoring (Preview)). A 'Start trial' button is present, along with a note about the trial period and cost. To the right, there are four cards: 'Intelligent threat detection' (built-in behavioral analytics and machine learning identity and notify you of threats so you can quickly assess the impact of an attack), 'Advanced threat protection' (built-in behavioral baseline protections powered by machine learning to reduce your overall surface area to attack), and two other cards partially visible.

- Click **Configure** under **Add new non-Azure computers**. A list of your Log Analytics workspaces is shown. The list includes, if applicable, the default workspace created for you by Security Center when automatic provisioning was enabled. Select this workspace or another workspace you want the Azure Stack VM to report security data to.

The screenshot shows the Microsoft Azure Security Center - Getting started page. The sidebar is identical to the previous screenshot. The main content area has a heading 'Azure Security Center' with a sub-section 'Gain tenant-wide visibility' (Learn More) which describes how to gain visibility and manage the security posture of your entire organization by leveraging Azure management groups and assigning a security role on the root management group. It also has a 'Configure security policies' section (Configure) which sets policies to define workload configuration, help ensure compliance, and protect sensitive data. Finally, there's a 'Add non-Azure computers' section (Configure) which uses the Microsoft Monitoring Agent to extend Security Center capabilities to computers running outside of Azure, including resources running on-premises and in other clouds.

The **Direct Agent** blade opens with a link for downloading the agent and keys for your workspace ID to use in configuring the agent.

NOTE

You do NOT need to download the agent manually. The agent will be installed as a VM extension in the steps below.

- On the right of **Workspace ID**, select the copy icon and paste the ID into Notepad.
- On the right of **Primary Key**, select the copy icon and paste the key into Notepad.

Add the virtual machine extension to your existing Azure Stack virtual machines

You must now add the **Azure Monitor, Update and Configuration Management** virtual machine extension to the virtual machines running on your Azure Stack.

1. In a new browser tab, log into your **Azure Stack** portal.
2. Go to the **Virtual machines** page, select the virtual machine that you want to protect with Security Center. For information on how to create a virtual machine on Azure Stack, see [this quickstart for Windows virtual machines](#) or [this quickstart for Linux virtual machines](#).
3. Select **Extensions**. The list of virtual machine extensions installed on this virtual machine is shown.
4. Click the **Add** tab. The **New Resource** menu blade opens and shows the list of available virtual machine extensions.
5. Select the **Azure Monitor, Update and Configuration Management** extension and click **Create**. The **Install extension** configuration blade opens up.

NOTE

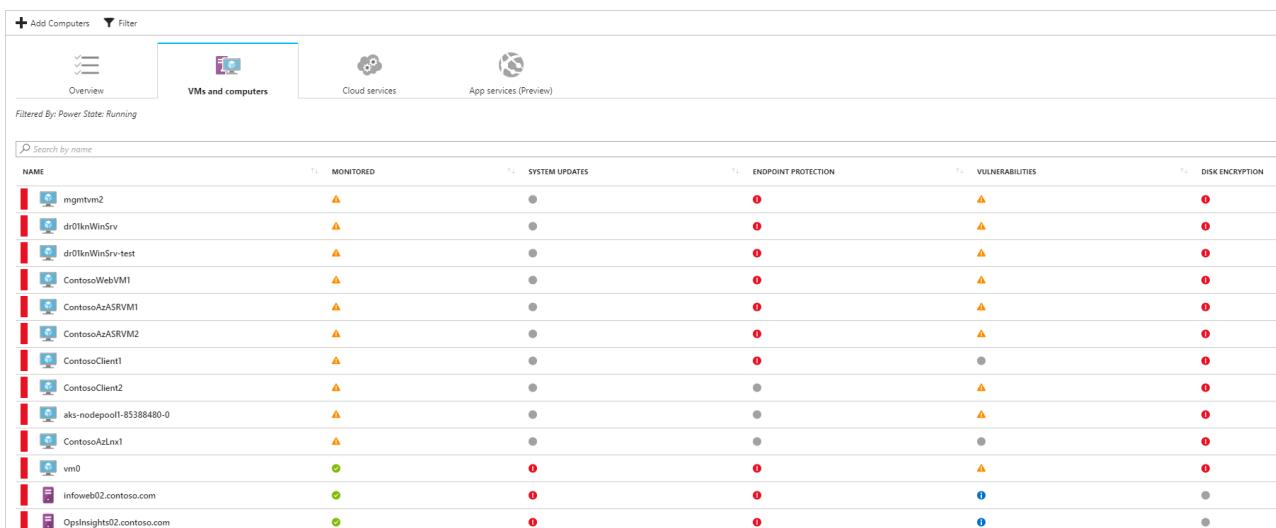
If you do not see the **Azure Monitor, Update and Configuration Management** extension listed in your marketplace, please reach out to your Azure Stack operator to make it available.

6. On the **Install extension** configuration blade, paste the **Workspace ID** and **Workspace Key (Primary Key)** that you copied into Notepad in the previous procedure.
7. When you are done providing the necessary configuration settings, click **OK**.
8. Once the extension installation completes, its status will show as **Provisioning Succeeded**. It might take up to one hour for the virtual machine to appear in the Security Center portal.

For further information on installing and configuring the agent for Windows, see [Connect Windows computers](#).

For Linux troubleshooting of agent issues, see [Troubleshoot Azure Log Analytics Linux Agent](#).

Now you can monitor your Azure VMs and non-Azure computers in one place. In the Security Center portal on Azure, under **Compute**, you have an overview of all VMs and computers along with their recommendations. Security Center also surfaces any detection for these computers in Security alerts.



The screenshot shows the Azure Security Center Compute blade. At the top, there are four navigation tabs: Overview, VMs and computers (which is selected and highlighted in blue), Cloud services, and App services (Preview). Below the tabs, a search bar says "Search by name" and a filter button says "Filtered By: Power State: Running". The main area is a table with columns: NAME, MONITORED, SYSTEM UPDATES, ENDPOINT PROTECTION, VULNERABILITIES, and DISK ENCRYPTION. The table lists 14 resources, each with a small icon and a status indicator (green circle for healthy, red circle for failing). The resources include various VMs and cloud services, such as mgmtvm2, dr01knWinSrv, ContosoWebVMI, and several instances of ContosoAzSRVM and ContosoClient.

| NAME | MONITORED | SYSTEM UPDATES | ENDPOINT PROTECTION | VULNERABILITIES | DISK ENCRYPTION |
|---------------------------|-----------|----------------|---------------------|-----------------|-----------------|
| mgmtvm2 | ▲ | ● | ● | ▲ | ● |
| dr01knWinSrv | ▲ | ● | ● | ▲ | ● |
| dr01knWinSrv-test | ▲ | ● | ● | ▲ | ● |
| ContosoWebVMI | ▲ | ● | ● | ▲ | ● |
| ContosoAzSRVM1 | ▲ | ● | ● | ▲ | ● |
| ContosoAzSRVM2 | ▲ | ● | ● | ▲ | ● |
| ContosoClient1 | ▲ | ● | ● | ● | ● |
| ContosoClient2 | ▲ | ● | ● | ▲ | ● |
| aks-nodepool1-85388480-0 | ▲ | ● | ● | ▲ | ● |
| ContosoAzLnx1 | ▲ | ● | ● | ● | ● |
| vm0 | ● | ● | ● | ▲ | ● |
| infoweb02.contoso.com | ● | ● | ● | ● | ● |
| OpsInsights02.contoso.com | ● | ● | ● | ● | ● |

There are two types of icons represented on the **Compute** blade:



Clean up resources

When no longer needed, you can remove the extension from the virtual machine via the Azure Stack portal.

To remove the extension:

1. Open the **Azure Stack Portal**.
2. Go to **Virtual machines** page, select the virtual machine from which you want to remove the extension.
3. Select **Extensions**, select the extension **Microsoft.EnterpriseCloud.Monitoring**.
4. Click on **Uninstall**, and confirm your selection by clicking **Yes**.

Next steps

In this quickstart, you provisioned the Azure Monitor, Update and Configuration Management extension on a virtual machine running on Azure Stack. To learn more about how to use Security Center, continue to the tutorial for configuring a security policy and assessing the security of your resources.

[Tutorial: Define and assess security policies](#)

Tutorial: Protect your resources with Azure Security Center

11/6/2019 • 4 minutes to read • [Edit Online](#)

Security Center limits your exposure to threats by using access and application controls to block malicious activity. Just-in-time (JIT) virtual machine (VM) access reduces your exposure to attacks by enabling you to deny persistent access to VMs. Instead, you provide controlled and audited access to VMs only when needed. Adaptive application controls help harden VMs against malware by controlling which applications can run on your VMs. Security Center uses machine learning to analyze the processes running in the VM and helps you apply whitelisting rules using this intelligence.

In this tutorial you learn how to:

- Configure a just-in-time VM access policy
- Configure an application control policy

Prerequisites

To step through the features covered in this tutorial, you must be on Security Center's Standard pricing tier. You can try Security Center Standard at no cost. To learn more, see the [pricing page](#). The quickstart [Onboard your Azure subscription to Security Center Standard](#) walks you through how to upgrade to Standard.

Manage VM access

JIT VM access can be used to lock down inbound traffic to your Azure VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed.

Management ports do not need to be open at all times. They only need to be open while you are connected to the VM, for example to perform management or maintenance tasks. When just-in-time is enabled, Security Center uses Network Security Group (NSG) rules, which restrict access to management ports so they cannot be targeted by attackers.

1. In the Security Center main menu, select **Just-in-time VM access** under **ADVANCED CLOUD DEFENSE**.

Virtual machines

| VIRTUAL MACHINE | APPROVED | LAST ACCESS | LAST USER | ... |
|-----------------|------------|-------------|-----------|-----|
| contoso1 | 0 Requests | N/A | N/A | ... |

Just-in-time VM access provides information on the state of your VMs:

- **Configured** - VMs that have been configured to support just-in-time VM access.
- **Recommended** - VMs that can support just-in-time VM access but have not been configured to.
- **No recommendation** - Reasons that can cause a VM not to be recommended are:
 - Missing NSG - The just-in-time solution requires an NSG to be in place.
 - Classic VM - Security Center just-in-time VM access currently supports only VMs deployed through Azure Resource Manager.
 - Other - A VM is in this category if the just-in-time solution is turned off in the security policy of the subscription or the resource group, or that the VM is missing a public IP and doesn't have an NSG in place.

2. Select a recommended VM and click **Enable JIT on 1 VM** to configure a just-in-time policy for that VM:

You can save the default ports that Security Center recommends or you can add and configure a new port on which you want to enable the just-in-time solution. In this tutorial, let's add a port by selecting **Add**.

The screenshot shows two windows side-by-side. On the left is the 'JIT VM access configuration' window for a 'standalone-vm'. It has a table of ports (22, 3389, 5985, 5986) with columns for Port, Protocol, Allowed source IPs, IP Range, and Time Range. A red box highlights the '+ Add' button. On the right is the 'Add port configuration' window. It has fields for Port (marked with a red asterisk), Protocol (Any, TCP, UDP), Allowed source IPs (Per request, CIDR block), IP range, and Max request time (a slider set to 3 hours). A red box highlights the entire configuration form.

3. Under **Add port configuration**, you identify:

- The port
- The protocol type
- Allowed source IPs - IP ranges allowed to get access upon an approved request
- Maximum request time - maximum time window that a specific port can be opened

4. Select **OK** to save.

Harden VMs against malware

Adaptive application controls help you define a set of applications that are allowed to run on configured resource groups, which among other benefits helps harden your VMs against malware. Security Center uses machine learning to analyze the processes running in the VM and helps you apply whitelisting rules using this intelligence.

1. Return to the Security Center main menu. Under **ADVANCED CLOUD DEFENSE**, select **Adaptive application controls**.

Adaptive application controls



What is application control?

Application control helps you deal with malicious and/or unauthorized software, by allowing only specific applications to run on your VMs

How does it work?

Security Center analyzes data of processes to find VMs for which there is a constant set of running applications. Security Center creates whitelisting rules for each resource group and presents the rules in the form of a recommendation. Once the recommendation is resolved, Security Center configures it by leveraging Applocker capabilities.

[For more information go to the documentation>](#)

Resource groups

| Configured | Recommended | No recommendation |
|---|-------------|-------------------|
| Resource groups for which an application whitelist is already applied and can be centrally managed. | | |
| NAME | VMS | MODE |
| ASC DEMO | 2 | Audit |
| WL1 | 2 | Audit |

The **Resource groups** section contains three tabs:

- Configured:** List of resource groups containing the VMs that were configured with application control.
- Recommended:** List of resource groups for which application control is recommended.
- No recommendation:** List of resource groups containing VMs without any application control recommendations. For example, VMs on which applications are always changing, and haven't reached a steady state.

2. Select the **Recommended** tab for a list of resource groups with application control recommendations.

Adaptive application controls

What is application control?
Application control helps you deal with malicious and/or unauthorized software, by allowing only specific applications to run on your VMs

How does it work?
Security Center analyzes data of processes to find VMs for which there is a constant set of running applications. Security Center creates whitelisting rules for each resource group and presents the rules in the form of a recommendation. Once the recommendation is resolved, Security Center configures it by leveraging Applocker capabilities.

[For more information go to the documentation>](#)

Resource groups

| NAME | VMS | STATE | SEVERITY |
|------------|-----|-------|----------|
| ASC DEMO | 7 | | |
| ASCDEMORG | 3 | Open | High |
| CONTOSOWEB | 4 | Open | High |

Create application control rules
ASCDEMORG

Description
The steps below will guide you through the process of creating the rules that are unique to this specific resource group.

Select VMs

| VIRTUAL MACHINE | STATE | SEVERITY |
|-----------------|-------|----------|
| vm3 | Open | |
| vm1 | Open | |
| vm2 | Open | |

Select processes for whitelisting rules

| NAME | PROCESSES | COMMON | EXPLOITABLE |
|--|-----------|--------|-------------|
| C:\Windows | 91 | No | |
| C:\Packages\Plugins | 14 | No | |
| C:\WindowsAzure\GuestAgent_2.7.41491.855 | 6 | No | |
| C:\Program Files | 10 | No | |
| C:\Program Files (x86)\Qualys\QualysAgent... | 1 | Yes | |

3. Select a resource group to open the **Create application control rules** option. In the **Select VMs**, review the list of recommended VMs and uncheck any you do not want to apply application control to. In the **Select processes for whitelisting rules**, review the list of recommended applications, and uncheck any you do not want to apply. The list includes:

- **NAME:** The full application path
- **PROCESSES:** How many applications reside within every path
- **COMMON:** "Yes" indicates that these processes have been executed on most VMs in this resource group
- **EXPLOITABLE:** A warning icon indicates if the applications could be used by an attacker to bypass application whitelisting. It is recommended to review these applications prior to their approval.

4. Once you finish your selections, select **Create**.

Clean up resources

Other quickstarts and tutorials in this collection build upon this quickstart. If you plan to continue to work with subsequent quickstarts and tutorials, continue running the Standard tier and keep automatic provisioning enabled. If you do not plan to continue or wish to return to the Free tier:

1. Return to the Security Center main menu and select **Security Policy**.
2. Select the subscription or policy that you want to return to Free. **Security policy** opens.
3. Under **POLICY COMPONENTS**, select **Pricing tier**.
4. Select **Free** to change subscription from Standard tier to Free tier.
5. Select **Save**.

If you wish to disable automatic provisioning:

1. Return to the Security Center main menu and select **Security policy**.
2. Select the subscription that you wish to disable automatic provisioning.
3. Under **Security policy – Data Collection**, select **Off** under **Onboarding** to disable automatic provisioning.
4. Select **Save**.

NOTE

Disabling automatic provisioning does not remove the Microsoft Monitoring Agent from Azure VMs where the agent has been provisioned. Disabling automatic provisioning limits security monitoring for your resources.

Next steps

In this tutorial, you learned how to limit your exposure to threats by:

- Configuring a just-in-time VM access policy to provide controlled and audited access to VMs only when needed
- Configuring an adaptive application controls policy to control which applications can run on your VMs

Advance to the next tutorial to learn about responding to security incidents.

[Tutorial: Respond to security incidents](#)

Tutorial: Respond to security incidents

11/27/2019 • 5 minutes to read • [Edit Online](#)

Security Center continuously analyzes your hybrid cloud workloads using advanced analytics and threat intelligence to alert you to malicious activity. In addition, you can integrate alerts from other security products and services into Security Center, and create custom alerts based on your own indicators or intelligence sources. Once an alert is generated, swift action is needed to investigate and remediate. In this tutorial, you will learn how to:

- Triage security alerts
- Investigate further to determine the root cause and scope of a security incident
- Search security data to aid in investigation

If you don't have an Azure subscription, create a [free account](#) before you begin.

Prerequisites

To step through the features covered in this tutorial, you must be on Security Center's Standard pricing tier. You can try Security Center Standard at no cost. To learn more, see the [pricing page](#). The quickstart [Onboard your Azure subscription to Security Center Standard](#) walks you through how to upgrade to Standard.

Scenario

Contoso recently migrated some of their on-premises resources to Azure, including some virtual machine-based line-of-business workloads and SQL databases. Currently, Contoso's Core Computer Security Incident Response Team (CSIRT) has a problem investigating security issues because of security intelligence not being integrated with their current incident response tools. This lack of integration introduces a problem during the Detect stage (too many false positives), as well as during the Assess and Diagnose stages. As part of this migration, they decided to opt in for Security Center to help them address this problem.

The first phase of this migration finished after they onboarded all resources and addressed all of the security recommendations from Security Center. Contoso CSIRT is the focal point for dealing with computer security incidents. The team consists of a group of people with responsibilities for dealing with any security incident. The team members have clearly defined duties to ensure that no area of response is left uncovered.

For the purpose of this scenario, we're going to focus on the roles of the following personas that are part of Contoso CSIRT:



Judy is in security operations. Their responsibilities include:

- Monitoring and responding to security threats around the clock.

- Escalating to the cloud workload owner or security analyst as needed.

Sam is a security analyst and their responsibilities include:

- Investigating attacks.
- Remediating alerts.
- Working with workload owners to determine and apply mitigations.

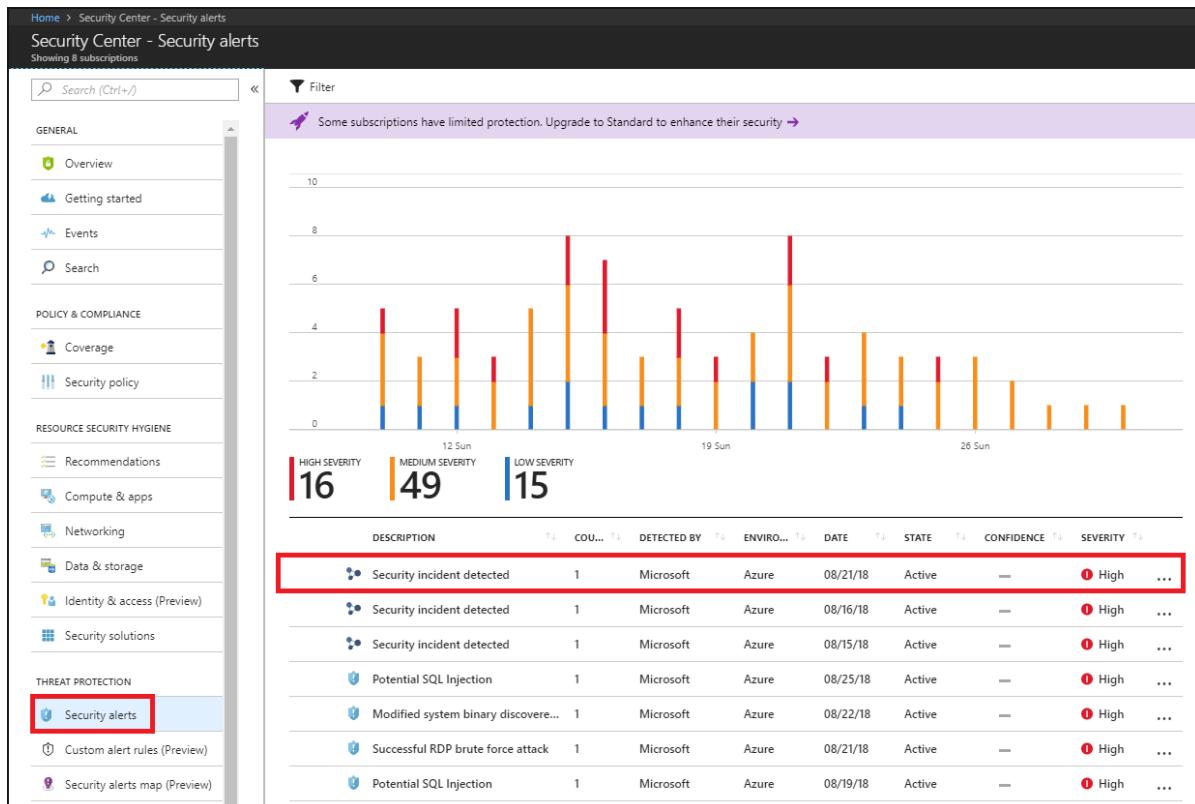
As you can see, Judy and Sam have different responsibilities, and they must work together to share Security Center information.

Triage security alerts

Security Center provides a unified view of all security alerts. Security alerts are ranked based on the severity and when possible related alerts are combined into a security incident. When triaging alerts and incidents, you should:

- Dismiss alerts for which no additional action is required, for example if the alert is a false positive
- Act to remediate known attacks, for example blocking network traffic from a malicious IP address
- Determine alerts that require further investigation

- On the Security Center main menu under **DETECTION**, select **Security alerts**:



- In the list of alerts, click on a security incident, which is a collection of alerts, to learn more about this incident. **Security incident detected** opens.

Security incident detected

Incident Detected

DESCRIPTION

The incident which started on 2018-01-01T12:00:00.000Z and most recently detected on 2018-01-02T19:00:00.000Z indicate that an attacker has attacked other resources from your virtual machine ContosoWebFE1

DETECTION TIME

Thursday, January 4, 2018, 3:02:00 AM

SEVERITY

! High

STATE

Active

ATTACKED RESOURCE

ContosoWebFE1

SUBSCRIPTION

<Subscription ID>

DETECTED BY

 Microsoft

ENVIRONMENT

 Azure

REMEDIATION STEPS

1. Escalate the alert to the information security team.
2. Review the remediation steps of each one of the alerts

Alerts included in this incident

| DESCRIPTION | COUNT | DETECTION TIME | ATTACKED RESOURCE | SEVERITY |
|--|-------|-------------------|-------------------|---|
|  Successful RDP brute force attack | 1 | 01/04/18, 4:20 AM | ContosoWebFE1 | ! High |
|  Suspicious SVCHOST process executed | 1 | 01/04/18, 5:19 AM | ContosoWebFE1 | i Low |
|  Multiple Domain Accounts Queried | 1 | 01/04/18, 5:21 AM | ContosoWebFE1 | i Low |

Continue investigation

3. On this screen you have the security incident description on top, and the list of alerts that are part of this incident. Click on the alert that you want to investigate further to obtain more information.

Successful RDP brute force attack
ContosoWebFE1

[Learn more](#)

General information

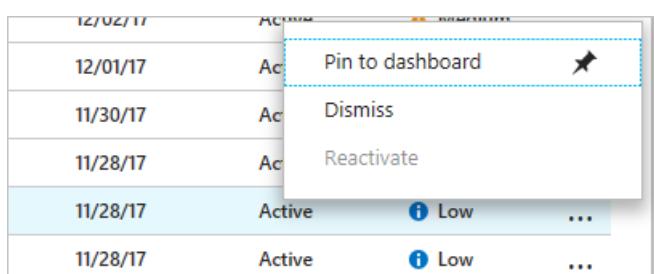
Several Remote Desktop login attempts were detected from FreeRDP (96.81.218.10), some of which were able to successfully login to the machine. Event logs analysis shows that in the last 30 minutes there were 60 failed attempts. 20 of the failed login attempts aimed at non-existent users. 1 of the failed login attempts aimed at existing users.

| | |
|------------------------|--|
| DESCRIPTION | Several Remote Desktop login attempts were detected from FreeRDP (96.81.218.10), some of which were able to successfully login to the machine. Event logs analysis shows that in the last 30 minutes there were 60 failed attempts. 20 of the failed login attempts aimed at non-existent users. 1 of the failed login attempts aimed at existing users. |
| DETECTION TIME | Thursday, January 4, 2018, 4:20:00 AM |
| SEVERITY | ! High |
| STATE | Active |
| ATTACKED RESOURCE | ContosoWebFE1 |
| SUBSCRIPTION | <Subscription ID> |
| DETECTED BY | ■ Microsoft |
| ENVIRONMENT | ■ Azure |
| RESOURCE TYPE | ■ Virtual Machine |
| TIMEGENERATEDOFFSETMIN | 30 |
| SOURCE | FreeRDP (96.81.218.10) |
| SUCCESSFUL LOGINS | 1 |
| ATTACK DURATION | 30 minutes |
| FAILED ATTEMPTS | 60 |
| NON-EXISTENT USERS | 20 |
| EXISTING USERS | 1 |
| REPORTS | Report: RDP Brute Forcing |
| END TIME UTC | 1/4/2018 1:21:00 PM |

Remediation steps

[Continue investigation](#) | [Run playbooks](#)

The type of alert can vary, read [Understanding security alerts in Azure Security Center](#) for more details about the type of alert, and potential remediation steps. For alerts that can be safely dismissed, you can right click on the alert and select the option **Dismiss**:



- If the root cause and scope of the malicious activity is unknown, proceed to the next step to investigate further.

Investigate an alert or incident

- On the **Security alert** page, click **Start investigation** button (if you already started, the name changes to **Continue investigation**).

The screenshot shows the Microsoft Security Center Investigation Dashboard. At the top, it displays a 'Security incident detected' alert with a 'High Priority' status. Below the header, there's a timeline from October 13, 2017, to November 6, 2017, spanning 24 days. A central graph illustrates the connections between various entities: 'Security incident detected' is at the center, connected to 'Successful RDP brute force...', 'Suspicious SVHOST process', and 'Multiple Domain Accounts Qu...'. Each entity has its own icon and a brief description. To the right of the graph, there are two expandable sections: 'General Information' and 'Remediation Steps'. The 'General Information' section contains details like the alert description ('The alert has no log data in this time interval'), alert ID ('2518942547722139231_77a4630c-be6e-4957-ad81-5920c3a3f1b8'), and time generated ('10/15/2017 2:25:41.000 AM'). The 'Remediation Steps' section is currently collapsed. On the far right, a sidebar lists navigation options: Info, Entities, Search, Exploration, Playbooks, Comments, and Audit.

The investigation map is a graphical representation of the entities that are connected to this security alert or incident. By clicking on an entity in the map, the information about that entity will show new entities, and the map expands. The entity that is selected in the map has its properties highlighted in the pane on the right side of the page. The information available on each tab will vary according to the selected entity. During the investigation process, review all relevant information to better understand the attacker's movement.

- If you need more evidence, or must further investigate entities that were found during the investigation, proceed to the next step.

Search data for investigation

You can use search capabilities in Security Center to find more evidence of compromised systems, and more details about the entities that are part of the investigation.

To perform a search open the **Security Center** dashboard, click **Search** in the left navigation pane, select the workspace that contains the entities that you want to search, type the search query, and click the search button.

Clean up resources

Other quickstarts and tutorials in this collection build upon this quickstart. If you plan to continue on to work with subsequent quickstarts and tutorials, continue running the Standard tier and keep automatic provisioning enabled. If you do not plan to continue or wish to return to the Free tier:

- Return to the Security Center main menu and select **Security Policy**.
- Select the subscription or policy that you want to return to Free. **Security policy** opens.
- Under **POLICY COMPONENTS**, select **Pricing tier**.
- Select **Free** to change subscription from Standard tier to Free tier.
- Select **Save**.

If you wish to disable automatic provisioning:

1. Return to the Security Center main menu and select **Security policy**.
2. Select the subscription that you wish to disable automatic provisioning.
3. Under **Security policy – Data Collection**, select **Off** under **Onboarding** to disable automatic provisioning.
4. Select **Save**.

NOTE

Disabling automatic provisioning does not remove the Microsoft Monitoring Agent from Azure VMs where the agent has been provisioned. Disabling automatic provisioning limits security monitoring for your resources.

Next steps

In this tutorial, you learned about Security Center features to be used when responding to a security incident, such as:

- Security incident which is an aggregation of related alerts for a resource
- Investigation map which is a graphical representation of the entities connected to a security alert or incident
- Search capabilities to find more evidence of compromised systems

To learn more about Security Center's investigation feature see:

[Investigate incidents and alerts](#)

Tutorial: Improve your regulatory compliance

2/25/2020 • 4 minutes to read • [Edit Online](#)

Azure Security Center helps streamline the process for meeting regulatory compliance requirements, using the **regulatory compliance dashboard**. In the dashboard, Security Center provides insights into your compliance posture based on continuous assessments of your Azure environment. Security Center analyzes risk factors in your hybrid cloud environment according to security best practices. These assessments are mapped to compliance controls from a supported set of standards. In the Regulatory compliance dashboard, you can see the status of all the assessments within your environment in the context of a particular standard or regulation. As you act on the recommendations and reduce risk factors in your environment, your compliance posture improves.

In this tutorial, you will learn how to:

- Evaluate your regulatory compliance using the Regulatory compliance dashboard
- Improve your compliance posture by taking action on recommendations

If you don't have an Azure subscription, create a [free account](#) before you begin.

Prerequisites

To step through the features covered in this tutorial, you must have Security Center's Standard pricing tier. You can try Security Center Standard at no cost. To learn more, see the [pricing page](#). The quickstart [Onboard your Azure subscription to Security Center Standard](#) walks you through how to upgrade to Standard.

Assess your regulatory compliance

Security Center continuously assesses the configuration of your resources to identify security issues and vulnerabilities. These assessments are presented as recommendations, which focus on improving your security hygiene. In the Regulatory compliance dashboard, you can view a set of compliance standards with all their requirements, where supported requirements are mapped to applicable security assessments. This enables you to view your compliance posture with respect to the standard, based on the status of these assessments.

The regulatory compliance dashboard view can help focus your attention on the gaps in compliance with a standard or regulation that is important to you. This focused view also enables you to continuously monitor your compliance score over time within dynamic cloud and hybrid environments.

NOTE

By default, Security Center supports the following regulatory standards: Azure CIS, PCI DSS 3.2, ISO 27001, and SOC TSP.

The [dynamic compliance packages \(preview\)](#) feature allows you to upgrade the standards shown in your regulatory compliance dashboard to the new *dynamic* packages. You can also use the same preview feature to add new compliance packages and monitor your compliance with additional standards.

1. In the Security Center main menu, under **POLICY & COMPLIANCE** select **Regulatory compliance**.

At the top of the screen, you see a dashboard with an overview of your compliance status with the set of supported compliance regulations. You can see your overall compliance score, and the number of passing vs. failing assessments associated with each standard.

The screenshot shows the Azure Security Center - Regulatory compliance dashboard. On the left, there's a navigation sidebar with sections like Events, Search, POLICY & COMPLIANCE (Coverage, Secure score, Security policy, Regulatory compliance), RESOURCE SECURITY HYGIENE (Recommendations, Compute & apps, IoT hubs & resources, Networking, Data & storage, Identity & access (Preview), Security solutions), ADVANCED CLOUD DEFENSE (Adaptive application controls, Just in time VM access, File Integrity Monitoring), and THREAT PROTECTION (Security alerts, Custom alert rules (Preview)).

The main area displays a "Regulatory compliance assessment" section with a pie chart showing 347 total items, 145 Failed, 201 Passed, and 1 Skipped. Below this are "Regulatory standards compliance status" cards for Azure CIS 1.0.0 (13 of 22 passed controls), PCI DSS 3.2 (4 of 33 passed controls), ISO 27001 (3 of 22 passed controls), and SOC TSP (0 of 13 passed controls). A "Regulatory compliance" panel on the right provides a summary of compliance posture relative to standards and regulations, with a "Learn more" link.

Under the Azure CIS 1.0.0 card, there are tabs for All, PCI DSS 3.2, ISO 27001, and SOC TSP. The All tab is selected, showing a list of controls under "Identity and Access Management", "Security Center", and "Storage Accounts". The "Storage Accounts" section is expanded, showing a specific control: "3.1. Ensure that 'Secure transfer required' is set to 'Enabled'". Below this is a table:

| ASSESSMENT | RESOURCE TYPE | FAILED RESOURCES |
|--|------------------|------------------|
| Require secure transfer to storage account | Storage accounts | 166 of 198 |

Other controls listed include "3.2. Ensure that 'Storage service encryption' is set to Enabled for Blob Service".

2. Select a tab for a compliance standard that is relevant to you. You will see the list of all controls for that standard. For the applicable controls, you can view the details of passing and failing assessments associated with that control. Some controls are grayed out. These controls don't have any Security Center assessments associated with them. Check the requirements for these and assess them in your environment on your own. Some of these may be process-related and not technical.

This screenshot shows the same dashboard but with the PCI DSS 3.2 tab selected under the Azure CIS card. The overall compliance status is 313 total items, 42 Failed, and 271 Passed. The "Regulatory standards compliance status" section now shows PCI DSS 3.2 (7 of 21 passed rules) as the selected standard.

The "Regulatory compliance" panel remains the same, providing a summary of compliance posture relative to standards and regulations, with a "Learn more" link.

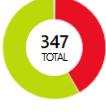
The "PCI DSS 3.2" tab is selected, showing a list of controls under "Install and maintain a firewall configuration to protect cardholder data". The "1.2. Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment" section is expanded, showing two sub-controls: "1.2.1. Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment, and specifically deny all other traffic." and "1.2.2. Secure and synchronize router configuration files.". The "1.2.3. Install perimeter firewalls between all wireless networks and the cardholder data environment, and configure these firewalls to deny or, if traffic is necessary for business purposes, permit only authorized traffic between the wireless environment and the cardholder data environment." control is also listed. The "1.3. Prohibit direct public access between the Internet and any system component in the cardholder data environment." control is listed under the "1.3. Prohibit direct public access between the Internet and any system component in the cardholder data environment." section.

3. To generate and download a PDF report summarizing your current compliance status for a particular standard, click **Download report**.

The report provides a high-level summary of your compliance status for the selected standard based on Security Center assessments data, and is organized according to the controls of that particular standard. The report can be shared with relevant stakeholders, and may serve to provide evidence to internal and external auditors.

[Download report](#)

Regulatory compliance assessment



| Status | Count |
|---------|-------|
| Failed | 145 |
| Passed | 201 |
| Skipped | 1 |

Regulatory standards compliance status

| Standard | Passed Controls | Total Controls |
|-----------------|-----------------|----------------|
| Azure CIS 1.0.0 | 13 | 22 |
| PCI DSS 3.2 | 4 | 33 |
| ISO 27001 | 3 | 22 |
| SOC TSP | 0 | 13 |

Azure CIS 1.0.0
PCI DSS 3.2
ISO 27001
SOC TSP
All

Under each applicable compliance control is the set of assessments run by Security Center that are associated with that currently passing: this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular standard are listed here.

Expand all compliance controls

- ✓ A5. Information security policies
- ✗ A6. Organization of information security
- ✓ A7. Human resources security
- ✗ A8. Asset management
- ✗ A9. Access control
- ✗ A10. Cryptography
- ✓ A11. Physical and environmental security
- ✗ A12. Operations security

Improve your compliance posture

Given the information in the Regulatory compliance dashboard, you can improve your compliance posture by resolving recommendations directly within the dashboard.

1. Click through any of the failing assessments that appear in the dashboard to view the details for that recommendation. Each recommendation includes a set of remediation steps that should be followed to resolve the issue.
2. You can select a particular resource to view more details and resolve the recommendation for that resource. For example, in the **Azure CIS standard** tab, you can click on the recommendation **Require secure transfer to storage account**.

Dashboard > Security Center - Regulatory Compliance (Preview) > Require secure transfer to storage account (Preview)

Require secure transfer to storage account (Preview)

Description

Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking.

General Information

| | |
|-----------------------|------|
| RECOMMENDATION SCORE | 2/20 |
| RECOMMENDATION IMPACT | +18 |
| USER IMPACT | Low |
| IMPLEMENTATION COST | Low |

Threats

- Data exfiltration
- Data spillage
- Threat resistance

Remediation steps

To enable secure transfer required:

- In your storage account, go to the 'Configuration' page.
- Enable 'Secure transfer required'.

Unhealthy resources: 141 Healthy resources: 17

LEARN MORE [Learn more about recommendations](#)

Unhealthy resources (141) Healthy resources (17) Unscanned resources (0)

Search storage accounts

| NAME | SUBSCRIPTION |
|-----------------|------------------------------|
| contosostorage1 | abcd1234abcd1234abcd1234 |
| contosostorage2 | 1234abcd1234abcd1234abcd1234 |

- As you click through to the recommendation information and select an unhealthy resource, it leads you directly to the experience of enabling **secure storage transfer** within the Azure portal.

For more information about how to apply recommendations, see [Implementing security recommendations in Azure Security Center](#).

Dashboard > Security Center - Regulatory Compliance (Preview) > Require secure transfer to storage account (Preview) > contosostorage1 - Configuration

contosostorage1 - Configuration

Storage account

Search (Ctrl+ /)

Save Discard

The cost of your storage account depends on the usage and the options you choose below. [Learn more](#)

Account kind: Storage (general purpose v1)

This account can be upgraded to a General Purpose v2 account with additional features. Upgrading is permanent and will result in billing changes. Learn more.

Upgrade

Performance: Standard Premium

* Secure transfer required Enabled Disabled

Replication: Locally-redundant storage (LRS)

Data Lake Storage Gen2 (preview): Hierarchical namespace Enabled Disabled

- After you take action to resolve recommendations, you will see the impact in the compliance dashboard report because your compliance score improves.

NOTE

Assessments are run approximately every 12 hours, so you will see the impact on your compliance data only after the assessments run.

Next steps

In this tutorial, you learned about using Security Center's Regulatory compliance dashboard to:

- View and monitor your compliance posture, relative to the standards and regulations that are important to you.
- Improve your compliance status by resolving relevant recommendations and watching the compliance score improve.

The Regulatory compliance dashboard can greatly simplify the compliance process, and significantly cut the time required for gathering compliance evidence for your Azure and hybrid environment.

To learn more see:

- [Update to dynamic compliance packages in your Regulatory compliance dashboard \(Preview\)](#) - Learn about this preview feature which allows you to update the standards shown in your regulatory compliance dashboard to the new *dynamic* packages. You can also use the same preview feature to add new compliance packages and monitor your compliance with additional standards.
- [Security health monitoring in Azure Security Center](#) - Learn how to monitor the health of your Azure resources.
- [Managing security recommendations in Azure Security Center](#) - Learn how to use recommendations in Azure Security Center to help protect your Azure resources.
- [Improve your Secure Score in Azure Security Center](#) - Learn how to prioritize vulnerabilities and security recommendations to most improve your security posture.

Improve your Secure Score in Azure Security Center

2/25/2020 • 3 minutes to read • [Edit Online](#)

NOTE

There is an enhanced Secure Score available in preview. The enhanced Secure Score will eventually replace the existing Secure Score, but for a while they will be running side-by-side to ease the transition.

For details of the benefits of the enhanced Secure Score, see [here](#).

To take part in the preview, open Azure Portal, launch Azure Security Center, and select Secure Score. From there, you will see a banner at the top of the page offering the new Secure Score experience. Alternatively, click [here](#).

With so many services offering security benefits, it's often hard to know what steps to take first to secure and harden your workload. The Secure Score reviews your security recommendations and prioritizes them for you, so you know which recommendations to perform first. This helps you find the most serious security vulnerabilities so you can prioritize investigation. Secure Score is a tool that helps you assess your workload security posture.

Secure Score calculation

Security Center mimics the work of a security analyst, reviewing your security recommendations, and applying advanced algorithms to determine how crucial each recommendation is. Azure Security center constantly reviews your active recommendations and calculates your Secure Score based on them, the score of a recommendation is derived from its severity and security best practices that will affect your workload security the most.

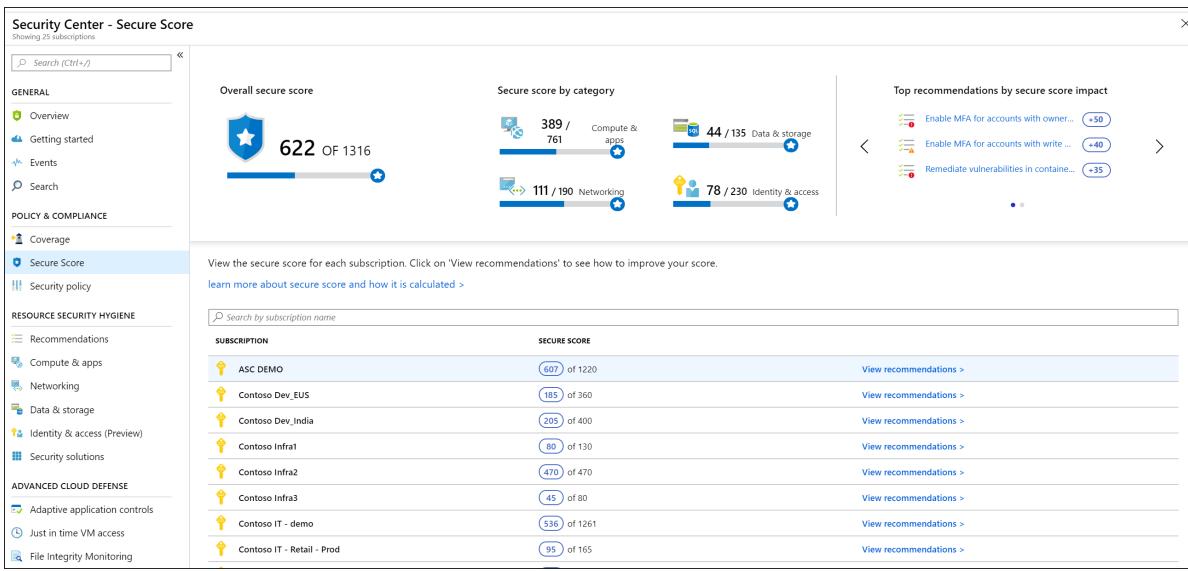
Security Center also provides you with an **Overall Secure Score**.

Overall Secure Score is an accumulation of all your recommendation scores. You can view your overall Secure Score across your subscriptions or management groups, depending on what you select. The score will vary based on subscription selected and the active recommendations on these subscriptions.

To check which recommendations impact your Secure Score most, you can view the top three most impactful recommendations in the Security Center dashboard or you can sort the recommendations in the recommendations list blade using the **Secure Score impact** column.

To view your overall Secure Score:

1. In the Azure dashboard, click **Security Center** and then click **Secure Score**.
2. At the top you can see Secure Score highlights:
 - The **Overall Secure Score** represents the score per policies, per selected subscription
 - **Secure Score by category** shows you which resources need the most attention
 - **Top recommendations by Secure Score impact** provides you with a list of the recommendations that will improve your Secure Score the most if you implement them.

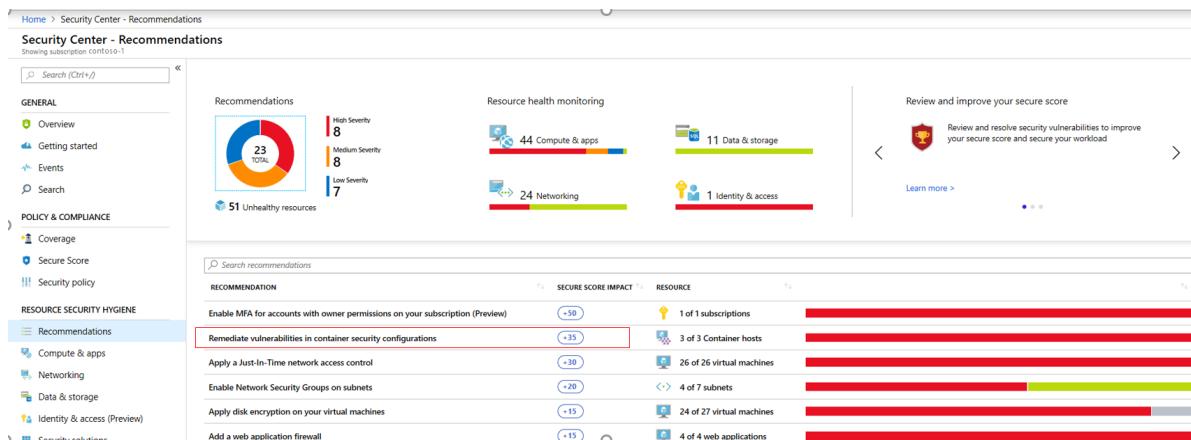


3. In the table below you can see each of your subscriptions and the overall Secure Score for each.

NOTE

The sum of the Secure Score of each subscription does not equal the overall Secure Score. The Secure Score is a calculation based on the ratio between your healthy resources and your total resources per recommendation, not a sum of Secure Scores across your subscriptions.

4. Click **View recommendations** to see the recommendations for that subscription that you can remediate to improve your Secure Score.
5. In the list of recommendations, you can see that for each recommendation there is a column that represents the **Secure Score impact**. This number represents how much your overall Secure Score will improve if you follow the recommendations. For example, in the screen below, if you **Remediate vulnerabilities in container security configurations**, your Secure Score will increase by 35 points.



Individual Secure Score

In addition, to view individual Secure Scores, you can find these within the individual recommendation blade.

The **Recommendation Secure Score** is a calculation based on the ratio between your healthy resources and your total resources. If the number of healthy resources is equal to the total number of resources, you get the maximum Secure Score of the recommendation of 50. To try to get your Secure Score closer to the max score, fix the unhealthy resources by following the recommendations.

The **Recommendation impact** lets you know how much your Secure Score improves if you apply the recommendation steps. For example, if your Secure Score is 42 and the **Recommendation impact** is +3,

performing the steps outlined in the recommendation improve your score to become 45.

The recommendation shows which threats your workload is exposed to if the remediation steps are not taken.

Home > Security Center - Recommendations > Recommendations > Remediate vulnerabilities in container security configurations

Remediate vulnerabilities in container security configurations

Description

Remediate vulnerabilities in security configuration on machines with Docker installed to protect them from attacks.

General Information

| | |
|-----------------------|----------|
| RECOMMENDATION SCORE | 0/35 |
| RECOMMENDATION IMPACT | +35 |
| USER IMPACT | Moderate |
| IMPLEMENTATION COST | Moderate |

Threats

- Data exfiltration
- Data spillage
- Account breach

Remediation steps

To Remediate vulnerabilities in the container security configurations:

1. Review the list of failed rules.
2. Fix each rule according to the specified instructions.

Unhealthy resources **2** Healthy resources **0**

LEARN MORE [Learn more about recommendations](#)

Next steps

This article showed you how to improve your security posture using **Secure Score** in Azure Security Center. To learn more about Security Center, see:

- [Azure Security Center FAQ](#)--Find frequently asked questions about the service and Secure Score.
- [Security health monitoring in Azure Security Center](#)--Learn how to monitor the health of your Azure resources.
- [Secure Score - enhanced](#)--Learn about the benefits of the enhanced Secure Score currently in preview.

The enhanced Secure Score (Preview)

2/25/2020 • 12 minutes to read • [Edit Online](#)

This article introduces the enhanced Secure Score (currently in preview), the accompanying Security Controls, and the advantages they bring. It also explains how your score is calculated.

Introduction to Secure Score

Azure Security Center has two main goals: to help you understand your current security situation, and to help you efficiently and effectively improve your security. The central aspect of Security Center that enables you to achieve those goals is Secure Score.

Security Center continually assesses your resources, subscriptions, and organization for security issues. It then aggregates all the findings into a single score so that you can tell, at a glance, your current security situation: the higher the score, the lower the identified risk level. Use the score to track security efforts and projects in your organization.

The *enhanced* Secure Score (currently in preview) is **attack surface focused** and brings three benefits:

- **Security Controls** - Security recommendations are now grouped into logical sets that better reflect your vulnerable attack surfaces. For more information, see [How the Secure Score is calculated](#) below.
- **Overall score better reflects the overall posture** - Points were awarded at the recommendation level. With this enhancement, your score will only improve when you remediate *all* of the recommendations for a single resource within a control. That means that your score only improves when the security of a resource improves.
- **Security status of individual attack surfaces is more visible** - By showing the score per Security Control, the Secure Score page becomes the place where you can get a granular view of how well your organization is securing each individual attack surface.

The enhanced Secure Score is shown as a percentage, as shown in the following screenshot:

Overall secure score
38% 22 of 58

| Subscription | Secure score | Action |
|--------------|------------------|---|
| Be | ★ 39% (22 of 58) | View recommendations > |
| ASC DEMO | ★ 38% (22 of 58) | View recommendations > |

Locating your Secure Score

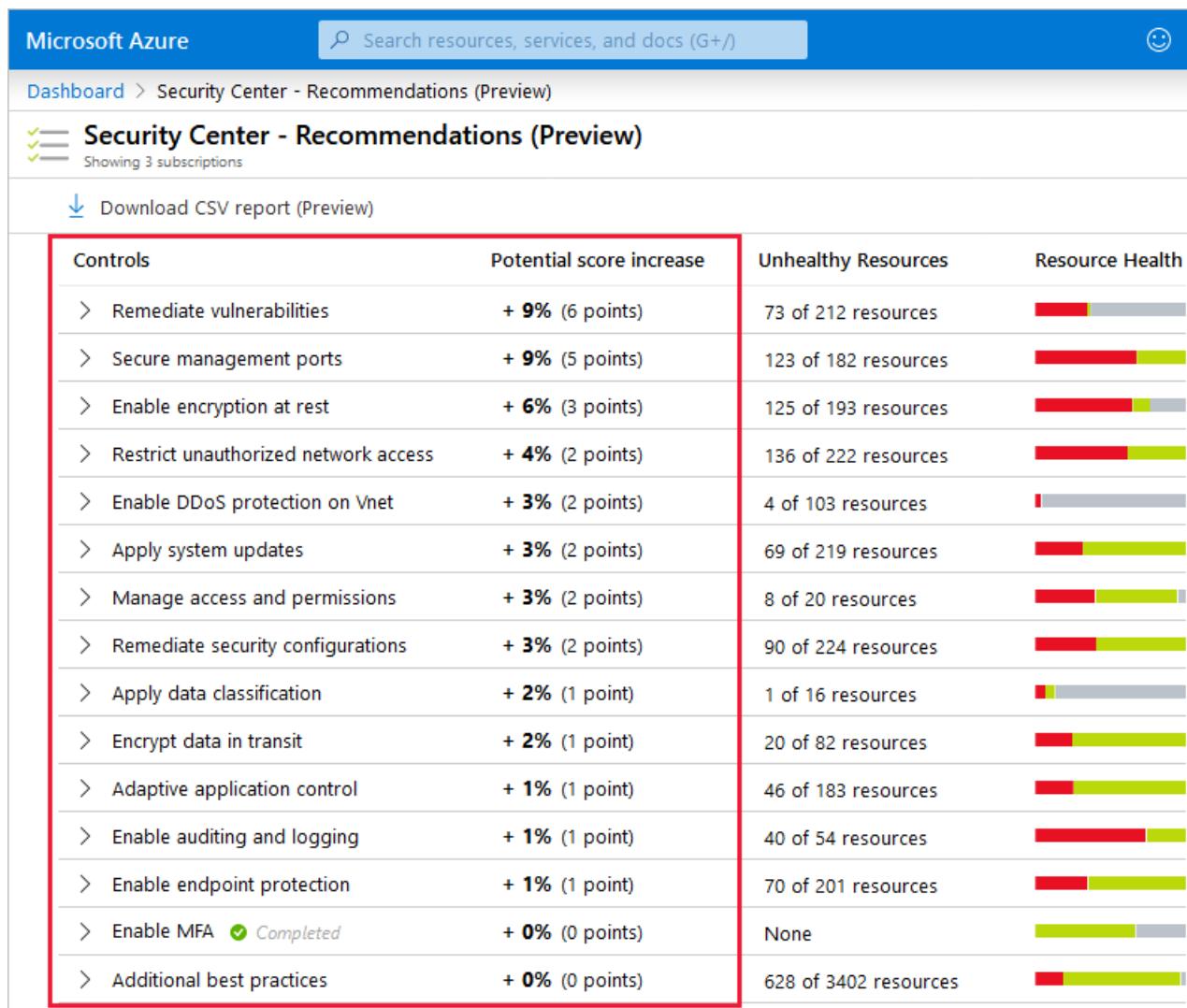
Security Center displays your score prominently: it's the first thing shown in the Overview page. If you click through to the dedicated Secure Score page, you'll see the score broken down by subscription. Click a single subscription to see the detailed list of prioritized recommendations and the potential impact that remediating them will have on the subscription's score.

How the Secure Score is calculated

Before this preview, Security Center considered each recommendation individually and assigned a value to it based on its severity. Security teams working to improve their security posture had to prioritize responses to Security Center recommendations based on the full list of findings. Every time you remediated a recommendation for a single resource, your Secure Score improved.

As part of the enhancements to the Secure Score, recommendations are now grouped into **Security Controls**. A control is a set of security recommendations and the instructions that help you implement those recommendations. Controls are logical groupings of related recommendations. Points are no longer awarded at the recommendation level. Instead, your score will only improve when you remediate *all* of the recommendations for a single resource within a control.

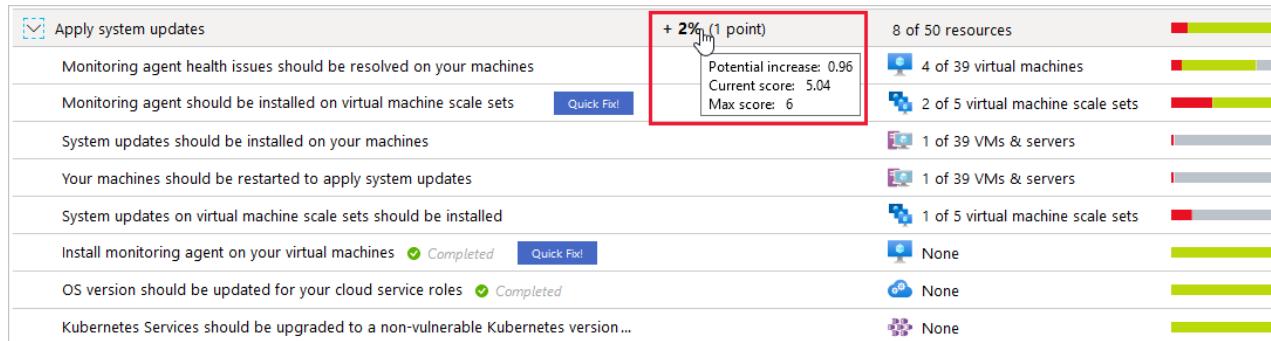
The contribution of each Security Control towards the overall Secure Score is shown clearly on the recommendations page.



To get all the possible points for a Security Control, all your resources must comply with all of the security recommendations within the Security Control. For example, Security Center has multiple recommendations regarding how to secure your management ports. In the past, you could remediate some of those related and

interdependent recommendations while leaving others unsolved, and your Secure Score would improve. When looked at objectively, it's easy to argue that your security hadn't improved until you had resolved them all. Now, you must remediate them all to make a difference to your Secure Score.

For example, the Security Control called "Apply system updates" has a maximum score of six points, which you can see in the tooltip on the potential increase value of the control:



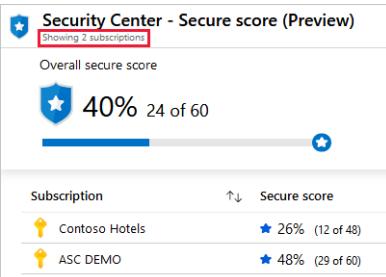
The potential for the Security Control "Apply system updates" in the screenshot above shows "2% (1 Point)". That means that if you remediate all the recommendations in this control, your score will increase by 2% (in this case, one point). For simplicity, values in the recommendations list's "Potential increase" column are rounded to whole numbers. The tooltips show the precise values:

- Max score** - The maximum number of points you can gain by completing all recommendations within a control. The maximum score for a control indicates the relative significance of that control. Use the max score values to triage which issues to work on first.
- Potential increase** - The remaining points available to you within the control. To get these points added to your Secure Score, remediate all of the control's recommendations. In the example above, the one point shown for the control is actually 0.96 points.
- Current score** - The current score for this control. Each control contributes towards the total score. In this example, the control is contributing 5.04 points to the total.

Calculations - understanding your score

| Metric | Formula and Example |
|---|---|
| Security Control's current score | $\text{Current score} = \frac{\text{Max score}}{\text{Healthy} + \text{Unhealthy}} \times \text{Healthy}$ <p>Each individual Security Control contributes towards the Security Score. Each resource affected by a recommendation within the control, contributes towards the control's current score. The current score for each control is a measure of the status of the resources <i>within</i> the control.</p> <p>In this example, the max score of 6 would be divided by 78 because that's the sum of the healthy and unhealthy resources. $6 / 78 = 0.0769$ Multiplying that by the number of healthy resources (4) results in the current score: $0.0769 * 4 = 0.31$</p> |

| METRIC | FORMULA AND EXAMPLE | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|--|--------------|--------------|----------|------------------|----------|--------------------------|-----------------------------|-----------------|---------------------------|-----------------|-----------------------------|-----------------|--|-----------------|----------------------------------|-----------------|------------------------|-----------------|---------------------------------|-----------------|-------------------------------------|-----------------|-----------------------------|----------------|---------------------------|----------------|--------------------------------|----------------|-------------------------------|----------------|------------------------------|----------------|---|-----------------|-----------------------------|-----------------|
| <p>Secure Score Single subscription</p> | <p><i>Secure Score = $\frac{\sum \text{Security Controls' current scores}}{\sum \text{Security Controls' maximum scores}} \times 100$</i></p> <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th>Subscription</th> <th>Secure score</th> </tr> </thead> <tbody> <tr> <td>ASC DEMO</td> <td>★ 47% (28 of 60)</td> </tr> </tbody> </table> <p>In this example, there is a single subscription with all Security Controls available (a potential maximum score of 60 points). The score shows 28 points out of a possible 60 and the remaining 32 points are reflected in the "Potential score increase" figures of the Security Controls.</p> <table border="1" style="width: 100%; border-collapse: collapse; text-align: center;"> <thead> <tr> <th>Controls</th> <th>Potential score increase</th> </tr> </thead> <tbody> <tr> <td>> Remediate vulnerabilities</td> <td>+ 9% (6 points)</td> </tr> <tr> <td>> Secure management ports</td> <td>+ 9% (5 points)</td> </tr> <tr> <td>> Enable encryption at rest</td> <td>+ 6% (3 points)</td> </tr> <tr> <td>> Restrict unauthorized network access</td> <td>+ 4% (2 points)</td> </tr> <tr> <td>> Enable DDoS protection on Vnet</td> <td>+ 3% (2 points)</td> </tr> <tr> <td>> Apply system updates</td> <td>+ 3% (2 points)</td> </tr> <tr> <td>> Manage access and permissions</td> <td>+ 3% (2 points)</td> </tr> <tr> <td>> Remediate security configurations</td> <td>+ 3% (2 points)</td> </tr> <tr> <td>> Apply data classification</td> <td>+ 2% (1 point)</td> </tr> <tr> <td>> Encrypt data in transit</td> <td>+ 2% (1 point)</td> </tr> <tr> <td>> Adaptive application control</td> <td>+ 1% (1 point)</td> </tr> <tr> <td>> Enable auditing and logging</td> <td>+ 1% (1 point)</td> </tr> <tr> <td>> Enable endpoint protection</td> <td>+ 1% (1 point)</td> </tr> <tr> <td>> Enable MFA Completed</td> <td>+ 0% (0 points)</td> </tr> <tr> <td>> Additional best practices</td> <td>+ 0% (0 points)</td> </tr> </tbody> </table> | Subscription | Secure score | ASC DEMO | ★ 47% (28 of 60) | Controls | Potential score increase | > Remediate vulnerabilities | + 9% (6 points) | > Secure management ports | + 9% (5 points) | > Enable encryption at rest | + 6% (3 points) | > Restrict unauthorized network access | + 4% (2 points) | > Enable DDoS protection on Vnet | + 3% (2 points) | > Apply system updates | + 3% (2 points) | > Manage access and permissions | + 3% (2 points) | > Remediate security configurations | + 3% (2 points) | > Apply data classification | + 2% (1 point) | > Encrypt data in transit | + 2% (1 point) | > Adaptive application control | + 1% (1 point) | > Enable auditing and logging | + 1% (1 point) | > Enable endpoint protection | + 1% (1 point) | > Enable MFA Completed | + 0% (0 points) | > Additional best practices | + 0% (0 points) |
| Subscription | Secure score | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ASC DEMO | ★ 47% (28 of 60) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Controls | Potential score increase | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > Remediate vulnerabilities | + 9% (6 points) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > Secure management ports | + 9% (5 points) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > Enable encryption at rest | + 6% (3 points) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > Restrict unauthorized network access | + 4% (2 points) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > Enable DDoS protection on Vnet | + 3% (2 points) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > Apply system updates | + 3% (2 points) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > Manage access and permissions | + 3% (2 points) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > Remediate security configurations | + 3% (2 points) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > Apply data classification | + 2% (1 point) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > Encrypt data in transit | + 2% (1 point) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > Adaptive application control | + 1% (1 point) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > Enable auditing and logging | + 1% (1 point) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > Enable endpoint protection | + 1% (1 point) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > Enable MFA Completed | + 0% (0 points) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > Additional best practices | + 0% (0 points) | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| METRIC | FORMULA AND EXAMPLE |
|---|--|
| Secure Score Multiple subscriptions | <p>The current score for all resources across all subscriptions are added and the calculation is then the same as for a single subscription</p> <p>When viewing multiple subscriptions, Secure Score evaluates all resources within all enabled policies and groups their combined impact on each Security Control's maximum score.</p>  <p>The combined score is not an average; rather it's the evaluated posture of the status of all resources across all subscriptions.</p> <p>Here too, if you go to the recommendations page and add up the potential points available, you will find that it's the difference between the current score (24) and the maximum score available (60).</p> |

Improving your Secure Score

To improve your Secure Score, remediate security recommendations from your recommendations list. You can remediate each recommendation manually for each resource, or by using the **Quick Fix!** option (when available) to apply a remediation for a recommendation to a group of resources quickly. For more information, see [Remediate recommendations](#).

Only built-in recommendations have an impact on the Secure Score.

Security Controls and their recommendations

The table below lists the Security Controls in Azure Security Center. For each control, you can see the maximum number of points you can add to your Secure Score if you remediate *all* of the recommendations listed in the control, for *all* of your resources.

| TIP |
|--|
| If you'd like to filter or sort this list differently, copy and paste it into Excel. |

| SECURITY CONTROL | MAXIMUM SECURE SCORE POINTS | RECOMMENDATIONS |
|------------------|-----------------------------|-----------------|
| | | |

| SECURITY CONTROL | MAXIMUM SECURE SCORE POINTS | RECOMMENDATIONS |
|----------------------------------|-----------------------------|--|
| Enable MFA | 10 | <ul style="list-style-type: none"> - MFA should be enabled on accounts with owner permissions on your subscription - MFA should be enabled on accounts with read permissions on your subscription - MFA should be enabled accounts with write permissions on your subscription |
| Secure management ports | 8 | <ul style="list-style-type: none"> - Just-In-Time network access control should be applied on virtual machines - Virtual machines should be associated with a Network Security Group - Management ports should be closed on your virtual machines |
| Apply system updates | 6 | <ul style="list-style-type: none"> - Monitoring agent health issues should be resolved on your machines - Monitoring agent should be installed on virtual machine scale sets - Monitoring agent should be installed on your machines - OS version should be updated for your cloud service roles - System updates on virtual machine scale sets should be installed - System updates should be installed on your machines - Your machines should be restarted to apply system updates - Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version - Monitoring agent should be installed on your virtual machines |
| Remediate vulnerabilities | 6 | <ul style="list-style-type: none"> - Advanced data security should be enabled on your SQL servers - Vulnerabilities in Azure Container Registry images should be remediated (Preview) - Vulnerabilities on your SQL databases should be remediated - Vulnerabilities should be remediated by a Vulnerability Assessment solution - Vulnerability assessment should be enabled on your SQL managed instances - Vulnerability assessment should be enabled on your SQL servers - Vulnerability assessment solution should be installed on your virtual machines |

| SECURITY CONTROL | MAXIMUM SECURE SCORE POINTS | RECOMMENDATIONS |
|--------------------------------------|-----------------------------|--|
| Enable encryption at rest | 4 | <ul style="list-style-type: none"> - Disk encryption should be applied on virtual machines - Transparent Data Encryption on SQL databases should be enabled - Automation account variables should be encrypted - Service Fabric clusters should have the ClusterProtectionLevel property set to EncryptAndSign - SQL server TDE protector should be encrypted with your own key |
| Encrypt data in transit | 4 | <ul style="list-style-type: none"> - API App should only be accessible over HTTPS - Function App should only be accessible over HTTPS - Only secure connections to your Redis Cache should be enabled - Secure transfer to storage accounts should be enabled - Web Application should only be accessible over HTTPS |
| Manage access and permissions | 4 | <ul style="list-style-type: none"> - A maximum of 3 owners should be designated for your subscription - Deprecated accounts should be removed from your subscription (Preview) - Deprecated accounts with owner permissions should be removed from your subscription (Preview) - External accounts with owner permissions should be removed from your subscription (Preview) - External accounts with read permissions should be removed from your subscription - External accounts with write permissions should be removed from your subscription (Preview) - There should be more than one owner assigned to your subscription - Role-Based Access Control (RBAC) should be used on Kubernetes Services (Preview) - Service Fabric clusters should only use Azure Active Directory for client authentication |

| SECURITY CONTROL | MAXIMUM SECURE SCORE POINTS | RECOMMENDATIONS |
|---|-----------------------------|--|
| Remediate security configurations | 4 | <ul style="list-style-type: none"> - Pod Security Policies should be defined on Kubernetes Services (Preview) - Vulnerabilities in container security configurations should be remediated - Vulnerabilities in security configuration on your machines should be remediated - Vulnerabilities in security configuration on your virtual machine scale sets should be remediated - Monitoring agent should be installed on your virtual machines - Monitoring agent should be installed on your machines - Monitoring agent should be installed on virtual machine scale sets - Monitoring agent health issues should be resolved on your machines |
| Restrict unauthorized network access | 4 | <ul style="list-style-type: none"> - IP forwarding on your virtual machine should be disabled - Authorized IP ranges should be defined on Kubernetes Services (Preview) - (DEPRECATED) Access to App Services should be restricted (Preview) - (DEPRECATED) The rules for web applications on IaaS NSGs should be hardened - Virtual machines should be associated with a Network Security Group - CORS should not allow every resource to access your API App - CORS should not allow every resource to access your Function App - CORS should not allow every resource to access your Web Application - Remote debugging should be turned off for API App - Remote debugging should be turned off for Function App - Remote debugging should be turned off for Web Application - Access should be restricted for permissive Network Security Groups with Internet-facing VMs - Network Security Group Rules for Internet facing virtual machines should be hardened |
| Apply adaptive application control | 3 | <ul style="list-style-type: none"> - Adaptive Application Controls should be enabled on virtual machines - Monitoring agent should be installed on your virtual machines - Monitoring agent should be installed on your machines - Monitoring agent health issues should be resolved on your machines |

| SECURITY CONTROL | MAXIMUM SECURE SCORE POINTS | RECOMMENDATIONS |
|--|-----------------------------|--|
| Apply data classification | 2 | <ul style="list-style-type: none"> - Sensitive data in your SQL databases should be classified (Preview) |
| Protect applications against DDoS attacks | 2 | <ul style="list-style-type: none"> - DDoS Protection Standard should be enabled |
| Enable endpoint protection | 2 | <ul style="list-style-type: none"> - Endpoint protection health failures should be remediated on virtual machine scale sets - Endpoint protection health issues should be resolved on your machines - Endpoint protection solution should be installed on virtual machine scale sets - Install endpoint protection solution on virtual machines - Monitoring agent health issues should be resolved on your machines - Monitoring agent should be installed on virtual machine scale sets - Monitoring agent should be installed on your machines - Monitoring agent should be installed on your virtual machines - Install endpoint protection solution on your machines |

| SECURITY CONTROL | MAXIMUM SECURE SCORE POINTS | RECOMMENDATIONS |
|------------------------------------|-----------------------------|---|
| Enable auditing and logging | 1 | <ul style="list-style-type: none"> - Auditing on SQL server should be enabled - Diagnostic logs in App Services should be enabled - Diagnostic logs in Azure Data Lake Store should be enabled - Diagnostic logs in Azure Stream Analytics should be enabled - Diagnostic logs in Batch accounts should be enabled - Diagnostic logs in Data Lake Analytics should be enabled - Diagnostic logs in Event Hub should be enabled - Diagnostic logs in IoT Hub should be enabled - Diagnostic logs in Key Vault should be enabled - Diagnostic logs in Logic Apps should be enabled - Diagnostic logs in Search service should be enabled - Diagnostic logs in Service Bus should be enabled - Diagnostic logs in Virtual Machine Scale Sets should be enabled - Metric alert rules should be configured on Batch accounts - SQL Auditing settings should have Action-Groups configured to capture critical activities - SQL servers should be configured with auditing retention days greater than 90 days. |

| SECURITY CONTROL | MAXIMUM SECURE SCORE POINTS | RECOMMENDATIONS |
|--|-----------------------------|--|
| Implement security best practices | 0 | <ul style="list-style-type: none"> - Access to storage accounts with firewall and virtual network configurations should be restricted - All authorization rules except RootManageSharedAccessKey should be removed from Event Hub namespace - An Azure Active Directory administrator should be provisioned for SQL servers - Authorization rules on the Event Hub instance should be defined - Storage accounts should be migrated to new Azure Resource Manager resources - Virtual machines should be migrated to new Azure Resource Manager resources - Advanced data security settings for SQL server should contain an email address to receive security alerts - Advanced data security should be enabled on your managed instances - All advanced threat protection types should be enabled in SQL managed instance advanced data security settings - Email notifications to admins and subscription owners should be enabled in SQL server advanced data security settings - Advanced Threat Protection types should be set to 'All' in SQL server Advanced Data Security settings - Subnets should be associated with a Network Security Group - All advanced threat protection types should be enabled in SQL server advanced data security settings |
| | | |

Secure Score FAQ

Why has my Secure Score gone down?

With the changes introduced in this enhanced Secure Score, you must solve all recommendation for a resource to receive points. The scores also changed to a scale of 0-10.

If I address only three out of four recommendations in a Security Control, will my Secure Score change?

No; it won't change until you remediate all of the recommendations for a single resource. To get the maximum score for a control, you must remediate all recommendations, for all resources.

Will this enhanced Secure Score replace the existing Secure Score?

Yes, but for a while they'll be running side by side to ease the transition.

If a recommendation isn't applicable to me, and I disable it in the policy, will my Security Control be fulfilled and my Secure Score updated?

Yes. We recommend disabling recommendations when they're inapplicable in your environment. For instructions

on how to disable a specific recommendation, see [Disable security policies](#).

If a Security Control offers me zero points towards my Secure Score, should I ignore it?

In some cases you'll see a control max score greater than zero, but the impact is zero. When the incremental score for fixing resources is negligible, it's rounded to zero. Don't ignore these recommendations as they still bring security improvements. The only exception is the "Additional Best Practice" control. Remediating these recommendations won't increase your score, but it will enhance your overall security.

Next steps

This article described the enhanced Secure Score and the new Security Controls it introduces. For related material, see the following articles:

- [Learn about the different elements of a recommendation](#)
- [Learn how to remediate recommendations](#)

Permissions in Azure Security Center

2/27/2020 • 2 minutes to read • [Edit Online](#)

Azure Security Center uses [Role-Based Access Control \(RBAC\)](#), which provides [built-in roles](#) that can be assigned to users, groups, and services in Azure.

Security Center assesses the configuration of your resources to identify security issues and vulnerabilities. In Security Center, you only see information related to a resource when you are assigned the role of Owner, Contributor, or Reader for the subscription or resource group that a resource belongs to.

In addition to these roles, there are two specific Security Center roles:

- **Security Reader:** A user that belongs to this role has viewing rights to Security Center. The user can view recommendations, alerts, a security policy, and security states, but cannot make changes.
- **Security Administrator:** A user that belongs to this role has the same rights as the Security Reader and can also update the security policy and dismiss alerts and recommendations.

NOTE

The security roles, Security Reader and Security Administrator, have access only in Security Center. The security roles do not have access to other service areas of Azure such as Storage, Web & Mobile, or Internet of Things.

Roles and allowed actions

The following table displays roles and allowed actions in Security Center.

| ROLE | EDIT SECURITY POLICY | APPLY SECURITY RECOMMENDATIONS FOR A RESOURCE (INCLUDING WITH 'QUICK FIX!') | DISMISS ALERTS AND RECOMMENDATIONS | VIEW ALERTS AND RECOMMENDATIONS |
|----------------------------|----------------------|---|------------------------------------|---------------------------------|
| Subscription Owner | ✓ | ✓ | ✓ | ✓ |
| Subscription Contributor | -- | ✓ | ✓ | ✓ |
| Resource Group Owner | -- | ✓ | -- | ✓ |
| Resource Group Contributor | -- | ✓ | -- | ✓ |
| Reader | -- | -- | -- | ✓ |
| Security Administrator | ✓ | -- | ✓ | ✓ |
| Security Reader | -- | -- | -- | ✓ |

NOTE

We recommend that you assign the least permissive role needed for users to complete their tasks. For example, assign the Reader role to users who only need to view information about the security health of a resource but not take action, such as applying recommendations or editing policies.

Next steps

This article explained how Security Center uses RBAC to assign permissions to users and identified the allowed actions for each role. Now that you're familiar with the role assignments needed to monitor the security state of your subscription, edit security policies, and apply recommendations, learn how to:

- [Set security policies in Security Center](#)
- [Manage security recommendations in Security Center](#)
- [Monitor the security health of your Azure resources](#)
- [Manage and respond to security alerts in Security Center](#)
- [Monitor partner security solutions](#)

Azure Security Center Data Security

2/25/2020 • 4 minutes to read • [Edit Online](#)

To help customers prevent, detect, and respond to threats, Azure Security Center collects and processes security-related data, including configuration information, metadata, event logs, crash dump files, and more. Microsoft adheres to strict compliance and security guidelines—from coding to operating a service.

This article explains how data is managed and safeguarded in Azure Security Center.

Data sources

Azure Security Center analyzes data from the following sources to provide visibility into your security state, identify vulnerabilities and recommend mitigations, and detect active threats:

- **Azure Services:** Uses information about the configuration of Azure services you have deployed by communicating with that service's resource provider.
- **Network Traffic:** Uses sampled network traffic metadata from Microsoft's infrastructure, such as source/destination IP/port, packet size, and network protocol.
- **Partner Solutions:** Uses security alerts from integrated partner solutions, such as firewalls and antimalware solutions.
- **Your Virtual Machines and Servers:** Uses configuration information and information about security events, such as Windows event and audit logs, IIS logs, syslog messages, and crash dump files from your virtual machines. In addition, when an alert is created, Azure Security Center may generate a snapshot of the VM disk affected and extract machine artifacts related to the alert from the VM disk, such as a registry file, for forensics purposes.

Data protection

Data segregation: Data is kept logically separate on each component throughout the service. All data is tagged per organization. This tagging persists throughout the data lifecycle, and it is enforced at each layer of the service.

Data access: In order to provide security recommendations and investigate potential security threats, Microsoft personnel may access information collected or analyzed by Azure services, including crash dump files, process creation events, VM disk snapshots and artifacts, which may unintentionally include Customer Data or personal data from your virtual machines. We adhere to the [Microsoft Online Services Terms and Privacy Statement](#), which state that Microsoft will not use Customer Data or derive information from it for any advertising or similar commercial purposes. We only use Customer Data as needed to provide you with Azure services, including purposes compatible with providing those services. You retain all rights to Customer Data.

Data use: Microsoft uses patterns and threat intelligence seen across multiple tenants to enhance our prevention and detection capabilities; we do so in accordance with the privacy commitments described in our [Privacy Statement](#).

Data location

Your Workspace(s): A workspace is specified for the following Geos, and data collected from your Azure virtual machines, including crash dumps, and some types of alert data, are stored in the nearest workspace.

| VM GEO | WORKSPACE GEO |
|---|----------------|
| United States, Brazil, South Africa | United States |
| Canada | Canada |
| Europe (Excluding United Kingdom) | Europe |
| United Kingdom | United Kingdom |
| Asia (Excluding India, Japan, Korea, China) | Asia Pacific |
| Korea | Asia Pacific |
| India | India |
| Japan | Japan |
| China | China |
| Australia | Australia |

VM disk snapshots are stored in the same storage account as the VM disk.

For virtual machines and servers running in other environments, e.g. on-premises, you can specify the workspace and region where collected data is stored.

Azure Security Center Storage: Information about security alerts, including partner alerts, is stored regionally according to the location of the related Azure resource, whereas information about security health status and recommendation is stored centrally in either the United States or Europe according to customer's location. Azure Security Center collects ephemeral copies of your crash dump files and analyzes them for evidence of exploit attempts and successful compromises. Azure Security Center performs this analysis within the same Geo as the workspace, and deletes the ephemeral copies when analysis is complete.

Machine artifacts are stored centrally in the same region as the VM.

Managing data collection from virtual machines

When you enable Security Center in Azure, data collection is turned on for each of your Azure subscriptions. You can also turn on data collection for your subscriptions in the Security Policy section of Azure Security Center.

When Data collection is turned on, Azure Security Center provisions the Microsoft Monitoring Agent on all existing supported Azure virtual machines and any new ones that are created. The Microsoft Monitoring agent scans for various security-related configurations and events it into [Event Tracing for Windows](#) (ETW) traces. In addition, the operating system will raise event log events during the course of running the machine. Examples of such data are: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, logged in user, and tenant ID. The Microsoft Monitoring Agent reads event log entries and ETW traces and copies them to your workspace(s) for analysis. The Microsoft Monitoring Agent also copies crash dump files to your workspace(s), enable process creation events, and enable command line auditing.

If you are using Azure Security Center Free, you can also disable data collection from virtual machines in the Security Policy. Data Collection is required for subscriptions on the Standard tier. VM disk snapshots and artifact collection will still be enabled even if data collection has been disabled.

Data Consumption

Customers can consume Security Center related data from different data streams, as shown below:

- **Azure Activity**: all security alerts, approved Security Center [Just-in-time](#) requests, and all alerts generated by adaptive application controls.
- **Azure Monitor logs**: all security alerts.

NOTE

Security recommendations can be also consumed via REST API. Read [Security Resource Provider REST API Reference](#) for more information.

See also

In this document, you learned how data is managed and safeguarded in Azure Security Center. To learn more about Azure Security Center, see:

- [Azure Security Center Planning and Operations Guide](#) — Learn how to plan and understand the design considerations to adopt Azure Security Center.
- [Security health monitoring in Azure Security Center](#) — Learn how to monitor the health of your Azure resources
- [Managing and responding to security alerts in Azure Security Center](#) — Learn how to manage and respond to security alerts
- [Monitoring partner solutions with Azure Security Center](#) — Learn how to monitor the health status of your partner solutions.
- [Azure Security Blog](#) — Find blog posts about Azure security and compliance

Use Azure Security Center recommendations to enhance security

2/25/2020 • 3 minutes to read • [Edit Online](#)

You can reduce the chances of a significant security event by configuring a security policy and then implementing the recommendations provided by Azure Security Center. This article shows you how to use security policies and recommendations in Security Center to help mitigate a security attack.

Security Center automatically runs continuous scans to analyze the security state of your Azure resources. When Security Center identifies potential security vulnerabilities, it creates recommendations that guide you through the process of configuring the needed security controls. Security Center updates its recommendations within 24 hours, with the following exceptions:

- Operating system security configuration recommendations are updated within 48 hours
- Endpoint Protection issues recommendations are updated within 8 hours

Scenario

This scenario shows you how to use Security Center to help reduce the chances of a security incident by monitoring Security Center recommendations and taking action. The scenario uses the fictitious company, Contoso, and roles presented in the Security Center [planning and operations guide](#). In this scenario, we're focusing on the roles of the following personas:



Jeff Cloud Workload Owner

Manages a cloud workload and its related resources (often in a DevOps role)

Responsible for implementing and maintaining protections in accordance with the company security policy

In small orgs, also defines policy and monitor alerts



David IT Security

Sets company security policies to ensure the appropriate protections are in place

Monitors compliance with policies

Generates reports for leadership or auditors

Contoso recently migrated some of their on-premises resources to Azure. Contoso wants to protect their resources and reduce vulnerability of their resources in the cloud.

Use Azure Security Center

David, from Contoso's IT security, has already chosen to onboard Security Center on Contoso's subscriptions to Azure Security Center to prevent and detect security vulnerabilities.

Security Center automatically analyzes the security state of Contoso's Azure resources and applies default security policies. When Security Center identifies potential security vulnerabilities, it creates **recommendations** based on the controls set in the security policy.

David runs Azure Security standard tier, across all their subscriptions to get the full suite of recommendations and security features available. Jeff also onboards all their existing on-premises servers that haven't yet been migrated to the cloud so that they can take advantage of Security Center's hybrid support across their [Windows](#) and [Linux](#) servers.

Jeff is a cloud workload owner. Jeff is responsible for applying security controls in accordance with Contoso's security policies.

Jeff performs the following tasks:

- Monitor security recommendations provided by Security Center
- Evaluate security recommendations and decide if they should apply or dismiss the recommendations.
- Apply security recommendations

Remediate threats using recommendations

As part of their daily monitoring activities, Jeff signs in to Azure and opens Security Center.

1. Jeff selects the workload's subscriptions.
2. Jeff checks the **Secure Score** to get an overall picture of how secure the subscriptions are and sees that the score is 548.
3. Jeff has to decide which recommendations to handle first. So Jeff clicks Secure Score and starts to handle recommendations based on how much it improves his **Secure Score impact**.
4. Because Jeff has lots of connected VMs and servers, Jeff decides to focus on **Compute and apps**.
5. When Jeff clicks **Compute and apps**, they see a list of recommendations and handles them according to the Secure Score impact.
6. Jeff has numerous Internet facing VMs, and because their ports are exposed, they're worried that an attacker could gain control over the servers. So Jeff chooses to use **just-in-time VM access**.

Jeff continues to move through the high priority and medium priority recommendations, and makes decisions on implementation. For each recommendation, Jeff looks at the detailed information provided by Security Center to understand which resources are impacted, what the Secure Score impact is, what each recommendation means and remediation steps for how to mitigate each issue.

Conclusion

Monitoring recommendations in Security Center helps you eliminate security vulnerabilities before an attack occurs. When you remediate recommendations, your Secure Score and your workloads' security posture improve. Security Center automatically discovers new resources you deploy, assesses them against your security policy and provides new recommendations for securing them.

Next steps

Make sure you have a monitoring process in place, in which you regularly check the recommendations in Security Center so that you can make sure to keep your resources secure over time.

This scenario showed you how to use security policies and recommendations in Security Center to help mitigate a security attack.

Learn how to respond to threats with [Managing and responding to security alerts](#).

Cross-tenant management in Security Center

2/27/2020 • 2 minutes to read • [Edit Online](#)

Cross-tenant management enables you to view and manage the security posture of multiple tenants in Security Center by leveraging [Azure delegated resource management](#). Manage multiple tenants efficiently, from a single view, without having to sign in to each tenant's directory.

- Service providers can manage the security posture of resources, for multiple customers, from within their own tenant.
- Security teams of organizations with multiple tenants can view and manage their security posture from a single location.

Set up cross-tenant management

Set up cross-tenant management by delegating access to resources of managed tenants to your own tenant using [Azure delegated resource management](#).

NOTE

Azure delegated resource management is one of the key components of Azure Lighthouse.

How does cross-tenant management work in Security Center

You are able to review and manage subscriptions across multiple tenants in the same way that you manage multiple subscriptions in a single tenant.

From the top menu bar, click the filter icon, and select the subscriptions, from each tenant's directory, you'd like to view.



The views and actions are basically the same. Here are some examples:

- **Manage security policies:** From one view, manage the security posture of many resources with [policies](#), take actions with security recommendations, and collect and manage security-related data.
- **Improve Secure Score and compliance posture:** Cross-tenant visibility enables you to view the overall security posture of all your tenants and where and how to best improve the [Secure Score](#) and [compliance posture](#) for each of them.
- **Remediate recommendations:** Monitor and remediate a [recommendation](#) for many resources from various tenants at one time. You can then immediately tackle the vulnerabilities that present the highest risk across all tenants.
- **Manage Alerts:** Detect [alerts](#) throughout the different tenants. Take action on resources that are out of compliance with actionable [remediation steps](#).
- **Manage advanced cloud defense features and more:** Manage the various threat protection services,

such as [just-in-time \(JIT\) VM access](#), [Adaptive Network Hardening](#), [adaptive application controls](#), and more.

Next steps

This article explains how cross-tenant management works in Security Center. To learn more about Security Center, see the following:

- [Strengthen your security posture with Azure Security Center](#) - Learn how to monitor the health of your Azure resources.
- [Azure Security Center FAQ](#) - Find frequently asked questions about using the service.
- [Learn about Azure Lighthouse in enterprise scenarios](#) - Discover how Azure Lighthouse can simplify cross-tenant management within an enterprise which uses multiple Azure AD tenants.

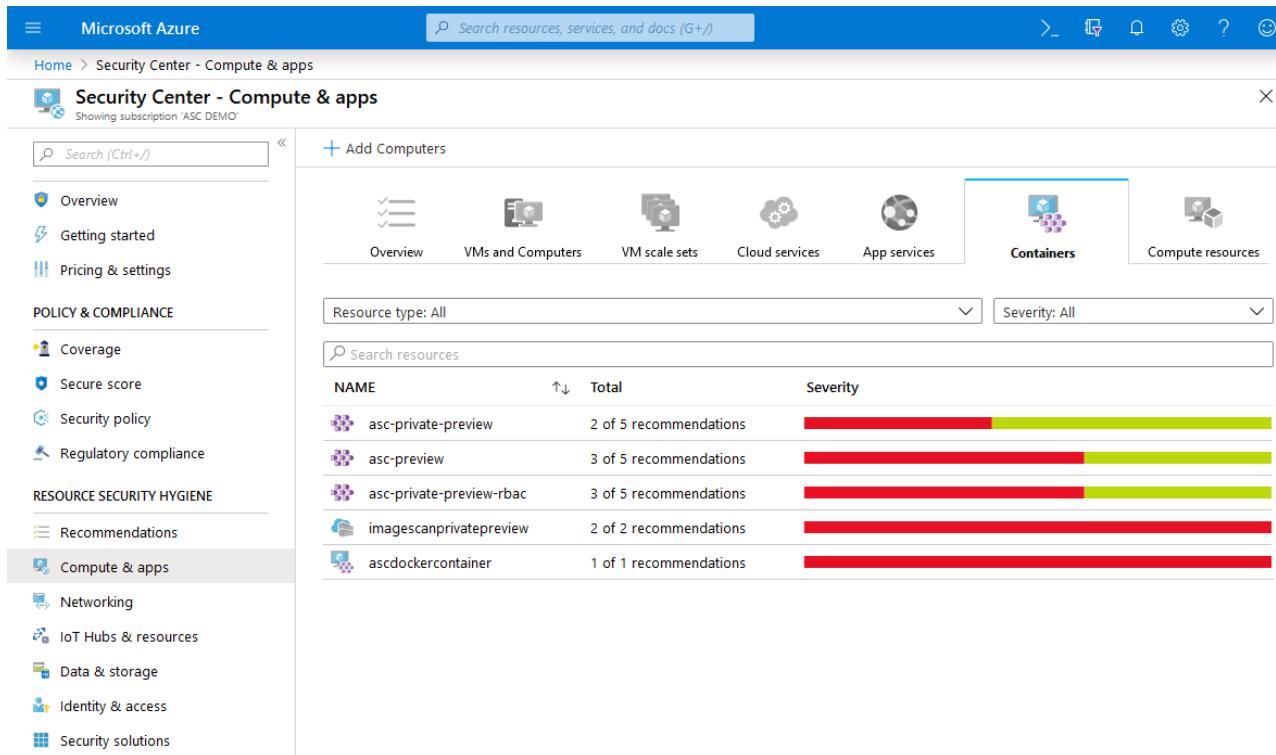
Container security in Security Center

2/27/2020 • 3 minutes to read • [Edit Online](#)

Azure Security Center is the Azure-native solution for container security. Security Center is also the optimal single pane of glass experience for the security of your cloud workloads, VMs, servers, and containers.

This article describes how Security Center helps you improve, monitor, and maintain the security of your containers and their apps. You'll learn how Security Center helps with these core aspects of container security:

- Vulnerability management
- Hardening of the container's environment
- Runtime protection



The screenshot shows the Azure Security Center interface for Compute & apps. On the left, there's a sidebar with navigation links like Overview, Getting started, Pricing & settings, Policy & Compliance (Coverage, Secure score, Security policy, Regulatory compliance), Resource Security Hygiene (Recommendations, Compute & apps selected), Networking, IoT Hubs & resources, Data & storage, Identity & access, and Security solutions. The main area has a search bar and a 'Add Computers' button. Below that, there are tabs for Overview, VMs and Computers, VM scale sets, Cloud services, App services, Containers (which is selected and highlighted in blue), and Compute resources. A filter bar allows setting Resource type (All) and Severity (All). A table below lists recommendations for various container images:

| NAME | Total | Severity |
|--------------------------|------------------------|---|
| asc-private-preview | 2 of 5 recommendations | <div style="width: 40%; background-color: red;"></div> <div style="width: 60%; background-color: green;"></div> |
| asc-preview | 3 of 5 recommendations | <div style="width: 60%; background-color: red;"></div> <div style="width: 40%; background-color: green;"></div> |
| asc-private-preview-rbac | 3 of 5 recommendations | <div style="width: 40%; background-color: red;"></div> <div style="width: 60%; background-color: green;"></div> |
| imagescanprivatepreview | 2 of 2 recommendations | <div style="width: 100%; background-color: red;"></div> |
| ascdockerccontainer | 1 of 1 recommendations | <div style="width: 100%; background-color: red;"></div> |

For instructions on how to use these features, see [Monitoring the security of your containers](#).

Vulnerability management - scanning container images (Preview)

To monitor your ARM-based Azure Container Registry, ensure you're on Security Center's standard tier (see [pricing](#)). Then enable the optional Container Registries bundle. When a new image is pushed, Security Center scans the image using a scanner from the industry-leading vulnerability scanning vendor, Qualys.

When issues are found – by Qualys or Security Center – you'll get notified in the Security Center dashboard. For every vulnerability, Security Center provides actionable recommendations, along with a severity classification, and guidance for how to remediate the issue. For details of Security Center's recommendations for containers, see the [reference list of recommendations](#).

Environment hardening

Continuous monitoring of your Docker configuration

Azure Security Center identifies unmanaged containers hosted on IaaS Linux VMs, or other Linux machines

running Docker containers. Security Center continuously assesses the configurations of these containers. It then compares them with the [Center for Internet Security \(CIS\) Docker Benchmark](#).

Security Center includes the entire ruleset of the CIS Docker Benchmark and alerts you if your containers don't satisfy any of the controls. When it finds misconfigurations, Security Center generates security recommendations. Use the **recommendations page** to view recommendations and remediate issues. You'll also see the recommendations on the **Containers** tab that displays all virtual machines deployed with Docker.

For details of the relevant Security Center recommendations that might appear for this feature, see the [container section](#) of the recommendations reference table.

When you're exploring the security issues of a VM, Security Center provides additional information about the containers on the machine. Such information includes the Docker version and the number of images running on the host.

NOTE

These CIS benchmark checks will not run on AKS-managed instances or Databricks-managed VMs.

Continuous monitoring of your Kubernetes clusters (Preview)

Security Center works together with Azure Kubernetes Service (AKS), Microsoft's managed container orchestration service for developing, deploying, and managing containerized applications.

AKS provides security controls and visibility into the security posture of your clusters. Security Center uses these features to:

- Constantly monitor the configuration of your AKS clusters
- Generate security recommendations aligned with industry standards

For details of the relevant Security Center recommendations that might appear for this feature, see the [container section](#) of the recommendations reference table.

Run-time protection - Real-time threat protection

Security Center provides real-time threat protection for your containerized environments and generates alerts for suspicious activities. You can use this information to quickly remediate security issues and improve the security of your containers.

We detect threats at the host and AKS cluster level. For full details, see [threat protection for Azure containers](#).

Container security FAQ

What types of images can Azure Security Center scan?

Security Center scans Linux OS based images which provide shell access.

The Qualys scanner doesn't support super minimalist images such as [Docker scratch](#) images, or "Distroless" images which only contain your application and its runtime dependencies (without a package manager, shell, or OS).

How does we scan Azure Security Center scan an image?

The image is extracted from the registry. It's then run in an isolated sandbox with the Qualys scanner which extracts a list of known vulnerabilities.

How often does Azure Security Center scan my images?

Image scans are triggered on every push.

Can I get the scan results via REST API?

Yes. The results are under [Sub-Assessments Rest API](#). In addition, you can use Azure Resource Graph (ARG), the Kusto-like API for all of your resources: a query can fetch a specific scan.

Next steps

To learn more about container security in Azure Security Center, see these related articles:

- To view the security posture of your container-related resources, see the containers section of [Protect your machines and applications](#).
- Details of the [integration with Azure Kubernetes Service](#)
- Details of the [integration with Azure Container Registry](#)

Azure Container Registry integration with Security Center (Preview)

2/18/2020 • 2 minutes to read • [Edit Online](#)

Azure Container Registry (ACR) is a managed, private Docker registry service that stores and manages your container images for Azure deployments in a central registry. It's based on the open-source Docker Registry 2.0.

If you're on Azure Security Center's standard tier, you can add the Container Registries bundle. This optional feature brings deeper visibility into the vulnerabilities of the images in your ARM-based registries. Enable or disable the bundle at the subscription level to cover all registries in a subscription. This feature is charged per image, as shown on the [pricing page](#). Enabling the Container Registries bundle, ensures that Security Center is ready to scan images that get pushed to the registry.

Whenever an image is pushed to your registry, Security Center automatically scans that image. To trigger the scan of an image, push it to your repository.

When the scan completes (typically after approximately 10 minutes), findings are available in Security Center recommendations like this:

The screenshot shows the Microsoft Azure Security Center interface. A prominent recommendation card is displayed, titled "Vulnerabilities in Azure Container Registry images should be remediated (powered by Qualys) - (Preview)". The card includes the following details:

- Unhealthy registries:** 1 / 1
- Severity:** High
- Total vulnerabilities:** 10 (with a red X icon)
- Vulnerabilities by severity:** High (1), Medium (9), Low (0)
- Registries with most vulnerabilities:** imagescanprivatepreview (10)
- Total vulnerable images:** 2 (with a red X icon)
Out of 3

Below the card, several sections are expanded:

- General Information:** Includes a recommendation score of 0/30, impact of +30, user impact of Low, and implementation effort of Moderate.
- Threats:** Lists Data exfiltration, Data spillage, Account breach, and Elevation of privilege.
- Remediation steps:** Provides instructions for manual remediation, including steps to resolve container image vulnerabilities.
- Affected resources:** Shows 1 unhealthy resource (imagescanprivatepreview) and 0 healthy resources.
- Security Checks:** Lists findings for the affected resource, including the ID 176750 and security check "Debian Security Update for apache2 (DSA 4422-1)".

To the right of the card, a detailed view of a specific finding is shown:

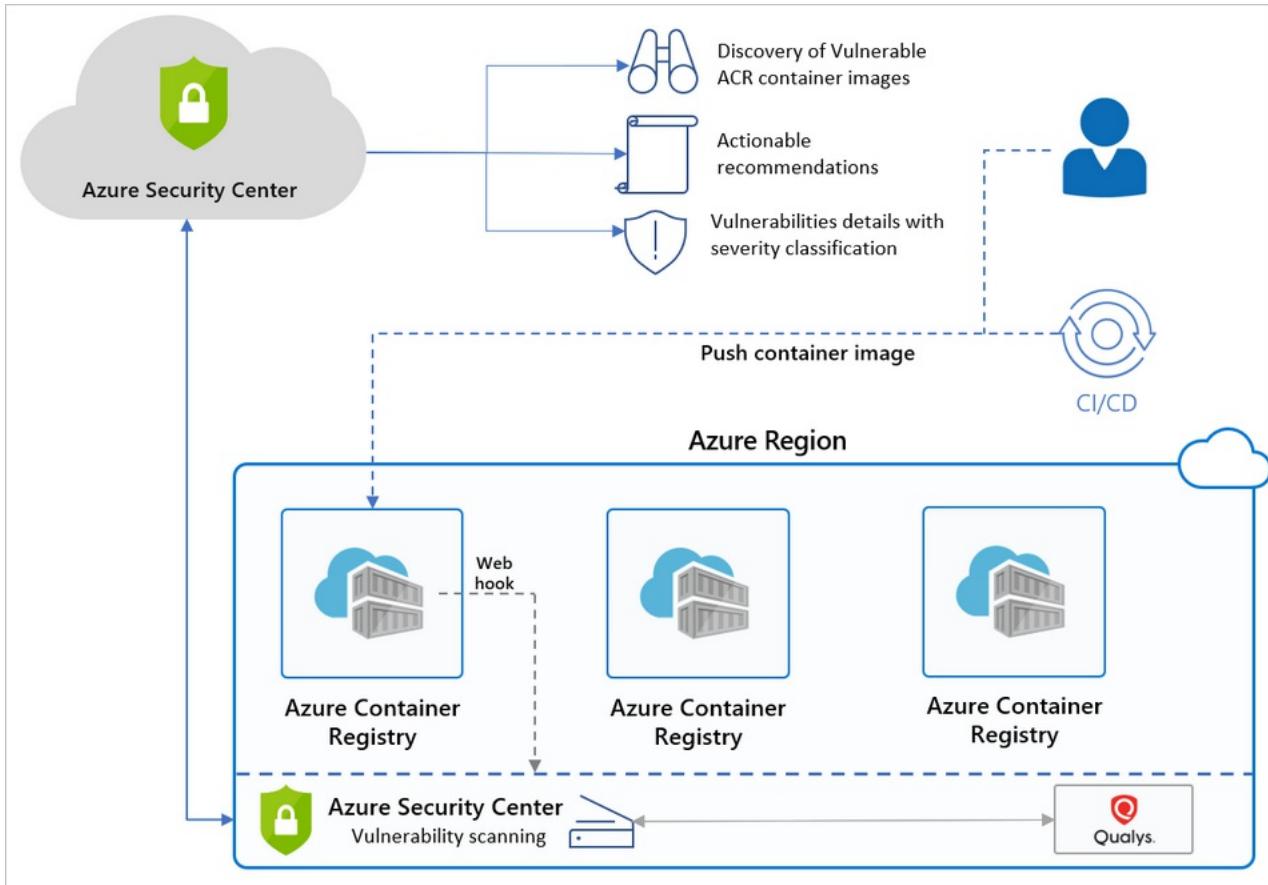
- Description:** Debian has released security update for apache2 to fix the vulnerabilities.
- General information:** Includes fields for ID (176750), Severity (High), Type (Vulnerability), Published (4/4/2019, 1:52 PM GMT+3), Patchable (Yes), and CVEs (CVE-2018-17189, CVE-2018-17199, CVE-2019-0196, CVE-2019-0211, CVE-2019-0217, CVE-2019-0220).
- Remediation:** Provides links to the Debian security advisory DSA 4422-1 for further details and download patches.
- Additional information:** Shows vendor references to DSA 4422-1.
- Affected resources:** Lists the affected resource imagescanprivatepreview.

Benefits of integration

Security Center identifies ARM-based ACR registries in your subscription and seamlessly provides:

- **Azure-native vulnerability scanning** for all pushed Linux images. Security Center scans the image using a scanner from the industry-leading vulnerability scanning vendor, Qualys. This native solution is seamlessly integrated by default.
- **Security recommendations** for Linux images with known vulnerabilities. Security Center provides details of each reported vulnerability and a severity classification. Additionally, it gives guidance for how to

remediate the specific vulnerabilities found on each image pushed to registry.



Next steps

To learn more about Security Center's container security features, see:

- [Azure Security Center and container security](#)
- [Integration with Azure Kubernetes Service](#)
- [Virtual Machine protection](#) - Describes Security Center's recommendations

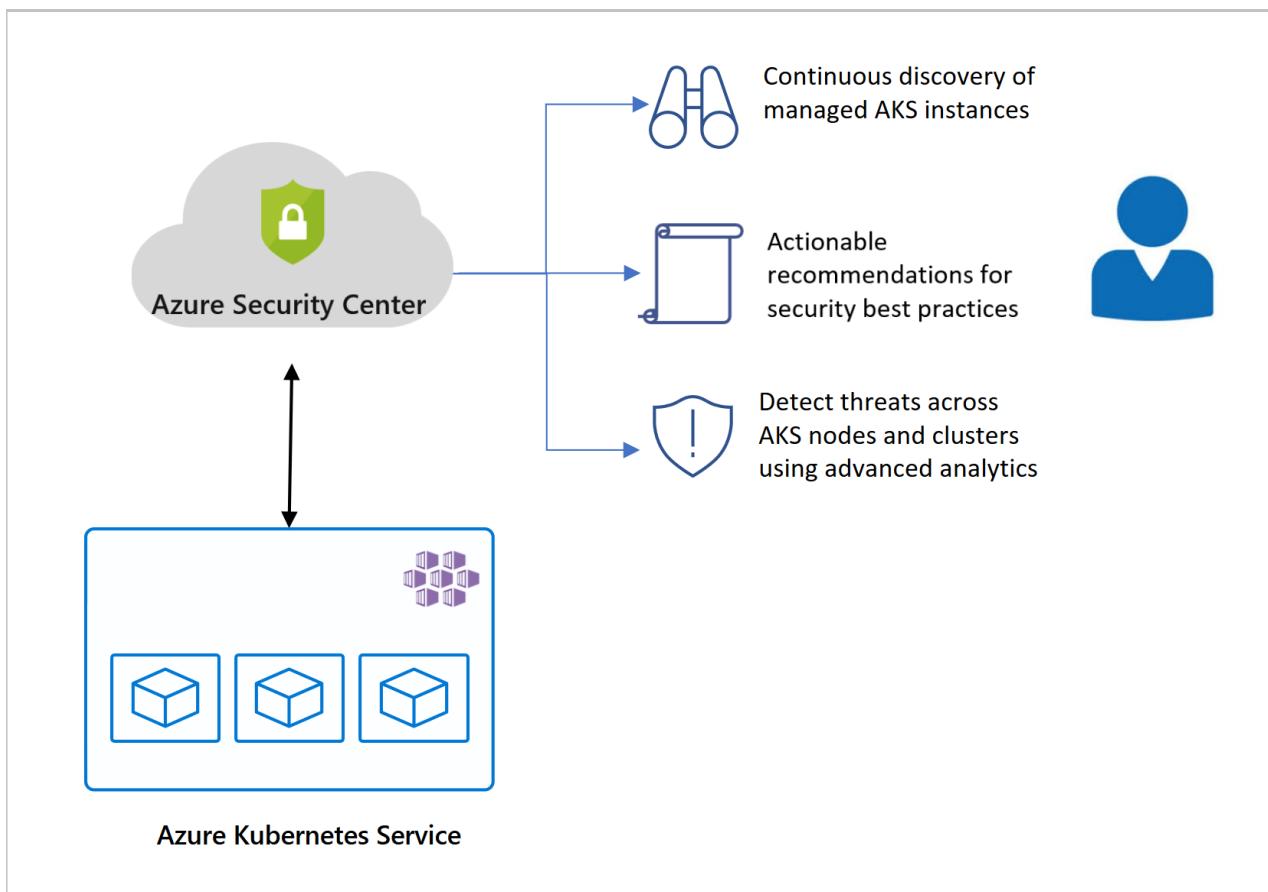
Azure Kubernetes Services integration with Security Center (Preview)

2/25/2020 • 2 minutes to read • [Edit Online](#)

Azure Kubernetes Service (AKS) is Microsoft's managed service for developing, deploying, and managing containerized applications.

Use AKS together with Azure Security Center's standard tier (see [pricing](#)) to gain deeper visibility to your AKS nodes, cloud traffic, and security controls.

Security Center brings security benefits to your AKS clusters using data already gathered by the AKS master node.



Together, these two tools form the best cloud-native Kubernetes security offering.

Benefits of integration

Using the two services together provides:

- **Security recommendations** - Security Center identifies your AKS resources and categorizes them: from clusters to individual virtual machines. You can then view security recommendations per resource. For more information, see the containers recommendations in the [reference list of recommendations](#).

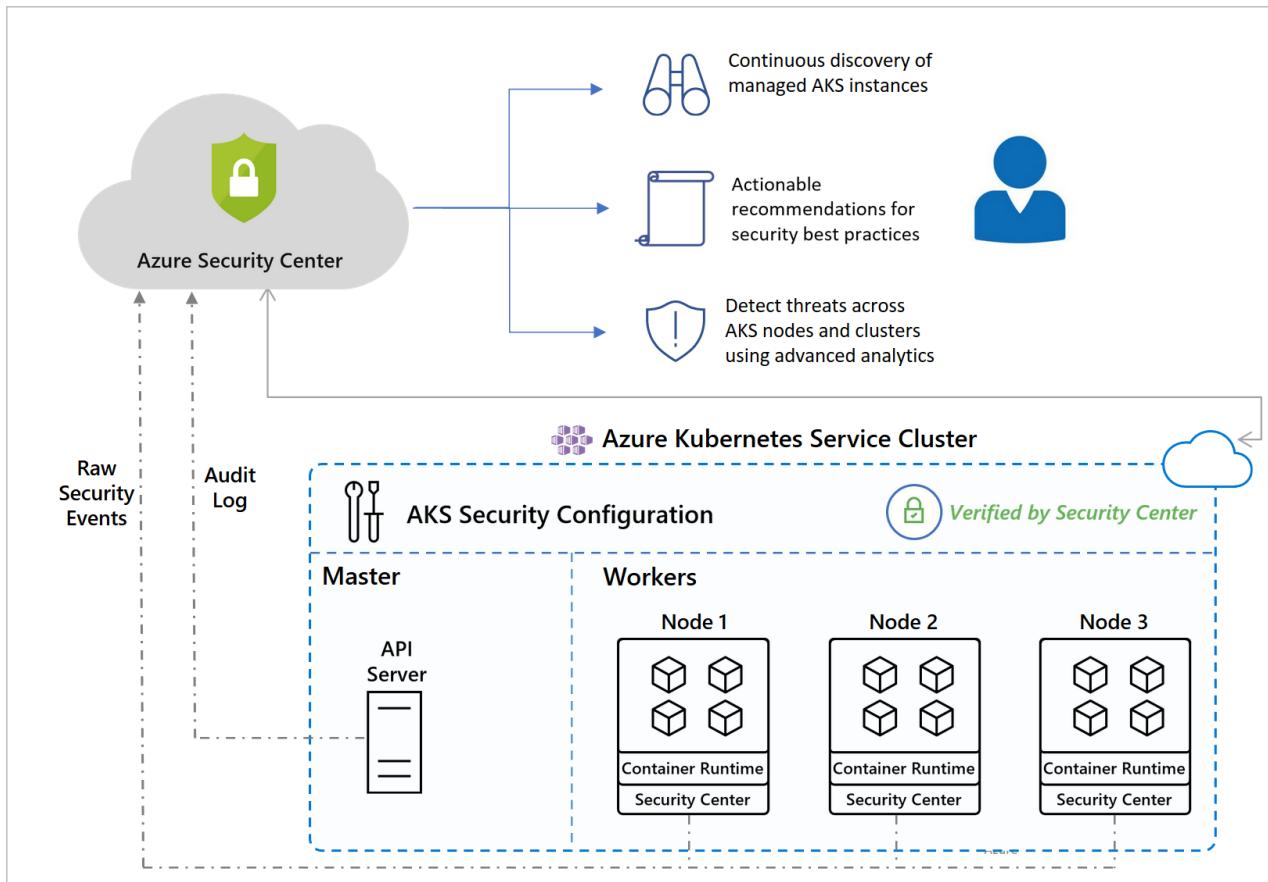
NOTE

If the name of a Security Center recommendation ends with a "(Preview)" tag, it's referring to the preview nature of the recommendation, not the feature.

- **Environment hardening** - Security Center constantly monitors the configuration of your Kubernetes clusters and Docker configurations. It then generates security recommendations that reflect industry standards.
- **Run-time protection** - Through continuous analysis of the following AKS sources, Security Center alerts you to threats and malicious activity detected at the host *and* AKS cluster level:
 - Raw security events, such as network data and process creation
 - The Kubernetes audit log

For more information, see [threat protection for Azure containers](#)

For the list of possible alerts, see these sections in the alerts reference table: [AKS cluster level alerts](#) and [Container host level alerts](#).



NOTE

Some of the data scanned by Azure Security Center from your Kubernetes environment may contain sensitive information.

Next steps

To learn more about Security Center's container security features, see:

- [Azure Security Center and container security](#)
- [Integration with Azure Container Registry](#)

- [Data management at Microsoft](#) - Describes the data policies of Microsoft services (including Azure, Intune, and Office 365), details of Microsoft's data management, and the retention policies that affect your data

Security alerts in Azure Security Center

2/25/2020 • 8 minutes to read • [Edit Online](#)

In Azure Security Center, there are a variety of alerts for many different resource types. Security Center generates alerts for resources deployed on Azure, and also for resources deployed on on-premises and hybrid cloud environments.

Security alerts are triggered by advanced detections and are available only in the Standard Tier of Azure Security Center. A free trial is available. You can upgrade from the Pricing Tier selection in the [Security Policy](#). Visit [Security Center page](#) to learn more about pricing.

Responding to today's threats

There have been significant changes in the threat landscape over the last 20 years. In the past, companies typically only had to worry about web site defacement by individual attackers who were mostly interested in seeing "what they could do". Today's attackers are much more sophisticated and organized. They often have specific financial and strategic goals. They also have more resources available to them, as they may be funded by nation states or organized crime.

These changing realities have led to an unprecedented level of professionalism in the attacker ranks. No longer are they interested in web defacement. They are now interested in stealing information, financial accounts, and private data – all of which they can use to generate cash on the open market or to leverage a particular business, political, or military position. Even more concerning than those attackers with a financial objective are the attackers who breach networks to do harm to infrastructure and people.

In response, organizations often deploy various point solutions, which focus on defending either the enterprise perimeter or endpoints by looking for known attack signatures. These solutions tend to generate a high volume of low fidelity alerts, which require a security analyst to triage and investigate. Most organizations lack the time and expertise required to respond to these alerts – so many go unaddressed.

In addition, attackers have evolved their methods to subvert many signature-based defenses and [adapt to cloud environments](#). New approaches are required to more quickly identify emerging threats and expedite detection and response.

What are security alerts?

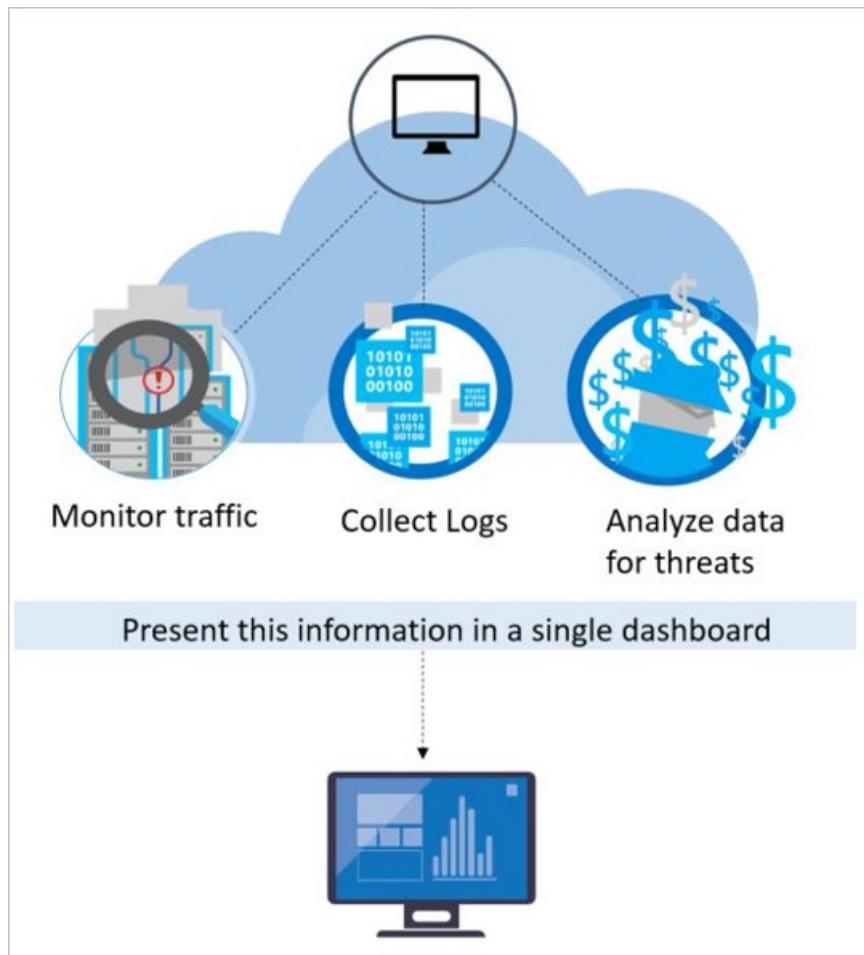
Alerts are the notifications that Security Center generates when it detects threats on your resources. Security Center prioritizes and lists the alerts, along with the information needed for you to quickly investigate the problem. Security Center also provides recommendations for how you can remediate an attack.

How does Security Center detect threats?

Microsoft security researchers are constantly on the lookout for threats. Because of Microsoft's global presence in the cloud and on-premises, they have access to an expansive set of telemetry. The wide-reaching and diverse collection of datasets enables the discovering of new attack patterns and trends across its on-premises consumer and enterprise products, as well as its online services. As a result, Security Center can rapidly update its detection algorithms as attackers release new and increasingly sophisticated exploits. This approach helps you keep pace with a fast moving threat environment.

To detect real threats and reduce false positives, Security Center collects, analyzes, and integrates log data from your Azure resources and the network. It also works with connected partner solutions, like firewall and endpoint

protection solutions. Security Center analyzes this information, often correlating information from multiple sources, to identify threats.



Security Center employs advanced security analytics, which go far beyond signature-based approaches. Breakthroughs in big data and [machine learning](#) technologies are leveraged to evaluate events across the entire cloud fabric – detecting threats that would be impossible to identify using manual approaches and predicting the evolution of attacks. These security analytics include:

- **Integrated threat intelligence:** Looks for known bad actors by leveraging global threat intelligence from Microsoft products and services, the Microsoft Digital Crimes Unit (DCU), the Microsoft Security Response Center (MSRC), and external feeds.
- **Behavioral analytics:** Applies known patterns to discover malicious behavior.
- **Anomaly detection:** Uses statistical profiling to build a historical baseline. It alerts on deviations from established baselines that conform to a potential attack vector.

The sections below discuss each of these analytics in further detail.

Integrated threat intelligence

Microsoft has an immense amount of global threat intelligence. Telemetry flows in from multiple sources, such as Azure, Office 365, Microsoft CRM online, Microsoft Dynamics AX, outlook.com, MSN.com, the Microsoft Digital Crimes Unit (DCU), and Microsoft Security Response Center (MSRC). Researchers also receive threat intelligence information that is shared among major cloud service providers and feeds from other third parties. Azure Security Center can use this information to alert you to threats from known bad actors.

Behavioral analytics

Behavioral analytics is a technique that analyzes and compares data to a collection of known patterns. However, these patterns are not simple signatures. They are determined through complex machine learning algorithms that are applied to massive datasets. They are also determined through careful analysis of malicious behaviors by expert analysts. Azure Security Center can use behavioral analytics to identify compromised resources based on

analysis of virtual machine logs, virtual network device logs, fabric logs, crash dumps, and other sources.

In addition, there's correlation with other signals to check for supporting evidence of a widespread campaign. This correlation helps to identify events that are consistent with established indicators of compromise.

Anomaly detection

Azure Security Center also uses anomaly detection to identify threats. In contrast to behavioral analytics (which depends on known patterns derived from large data sets), anomaly detection is more "personalized" and focuses on baselines that are specific to your deployments. Machine learning is applied to determine normal activity for your deployments and then rules are generated to define outlier conditions that could represent a security event.

How are alerts classified?

Security Center assigns a severity to alerts, to help you prioritize the order in which you attend to each alert, so that when a resource is compromised, you can get to it right away. The severity is based on how confident Security Center is in the finding or the analytic used to issue the alert as well as the confidence level that there was malicious intent behind the activity that led to the alert.

NOTE

Alert severity is displayed differently in the portal and versions of the REST API that predate 01-01-2019. If you're using an older version of the API, upgrade for the consistent experience described below.

- **High:** There is a high probability that your resource is compromised. You should look into it right away. Security Center has high confidence in both the malicious intent and in the findings used to issue the alert. For example, an alert that detects the execution of a known malicious tool such as Mimikatz, a common tool used for credential theft.
- **Medium:** This is probably a suspicious activity may indicate that a resource is compromised. Security Center's confidence in the analytic or finding is medium and the confidence of the malicious intent is medium to high. These would usually be machine learning or anomaly-based detections. For example, a sign-in attempt from an anomalous location.
- **Low:** This might be a benign positive or a blocked attack.
 - Security Center is not confident enough that the intent is malicious and the activity may be innocent. For example, log clear is an action that may happen when an attacker tries to hide their tracks, but in many cases is a routine operation performed by admins.
 - Security Center doesn't usually tell you when attacks were blocked, unless it's an interesting case that we suggest you look into.
- **Informational:** You will only see informational alerts when you drill down into a security incident, or if you use the REST API with a specific alert ID. An incident is typically made up of a number of alerts, some of which may appear on their own to be only informational, but in the context of the other alerts may be worthy of a closer look.

Continuous monitoring and assessments

Azure Security Center benefits from having security research and data science teams throughout Microsoft who continuously monitor for changes in the threat landscape. This includes the following initiatives:

- **Threat intelligence monitoring:** Threat intelligence includes mechanisms, indicators, implications, and actionable advice about existing or emerging threats. This information is shared in the security community and Microsoft continuously monitors threat intelligence feeds from internal and external sources.
- **Signal sharing:** Insights from security teams across Microsoft's broad portfolio of cloud and on-premises services, servers, and client endpoint devices are shared and analyzed.
- **Microsoft security specialists:** Ongoing engagement with teams across Microsoft that work in specialized

security fields, like forensics and web attack detection.

- **Detection tuning:** Algorithms are run against real customer data sets and security researchers work with customers to validate the results. True and false positives are used to refine machine learning algorithms.

These combined efforts culminate in new and improved detections, which you can benefit from instantly – there's no action for you to take.

Security alert types

The following topics guide you through the different alerts, according to resource types:

- [Alerts for IaaS Windows machines](#)
- [Alerts for IaaS Linux machines](#)
- [Alerts for Azure App Service](#)
- [Alerts for Azure containers](#)
- [Alerts for SQL Database and SQL Data Warehouse](#)
- [Alerts for Azure Storage](#)
- [Alerts for Cosmos DB](#)

The following topics explain how Security Center uses the different telemetry that it collects from integrating with the Azure infrastructure, in order to apply additional protection layers for resources deployed on Azure:

- [Alerts for Azure management layer \(Azure Resource Manager\) \(Preview\)](#)
- [Alerts for Azure Key Vault \(Preview\)](#)
- [Alerts for Azure network layer](#)
- [Alerts from other services](#)

What are security incidents?

A security incident is a collection of related alerts, instead of listing each alert individually. Security Center uses [Cloud Smart Alert Correlation](#) to correlate different alerts and low fidelity signals into security incidents.

Using incidents, Security Center provides you with a single view of an attack campaign and all of the related alerts. This view enables you to quickly understand what actions the attacker took, and what resources were affected. For more information, see [Cloud smart alert correlation](#).

Security alerts in Azure Activity Log

In addition to being available in the Azure portal or programmatically, Security alerts and incidents are audited as events in [Azure Activity Log](#). For more information on the event schema, see [Security Alerts in Azure Activity log](#).

Next steps

In this article, you learned about the different types of alerts available in Security Center. For more information, see:

- [Azure Security Center planning and operations guide](#)
- [Azure Security Center FAQ](#)

Security alerts - a reference guide

2/27/2020 • 71 minutes to read • [Edit Online](#)

This article lists the security alerts you might see in Azure Security Center's Threat Protection module. The alerts shown in your environment depend on the resources and services you're protecting, as well as your customized configuration.

To learn about how to respond to these alerts, see [Manage and respond to security alerts in Azure Security Center](#).

To learn about how to export alerts (and recommendations) see [Export security alerts and recommendations \(Preview\)](#).

Below the alerts tables is a table describing the Azure Security Center kill chain that is used to categorize the intents of these alerts.

Alerts for Windows machines

[Further details and notes](#)

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|---|---------------------|
| A logon from a malicious IP has been detected | A successful remote authentication for the account 'tristan.schleining' and process 'Advapi' occurred, however the logon IP address [IP address] has previously been reported as malicious or highly unusual. A successful attack has probably occurred. | - |
| A logon from a malicious IP has been detected. [seen multiple times] | A successful remote authentication for the account 'IUSR_10001' and process 'Advapi' occurred, however the logon IP address [IP address] has previously been reported as malicious or highly unusual. A successful attack has probably occurred. Files with the .scr extensions are screen saver files and are normally reside and execute from the Windows system directory. | - |
| Addition of Guest account to Local Administrators group | Analysis of host data has detected the addition of the built in Guest account to the Local Administrators group on % {Compromised Host}, which is strongly associated with attacker activity. | - |
| An event log was cleared | Machine logs indicate a suspicious event log clearing operation by user: '% {user name}' in Machine: '% {CompromisedEntity}'. The %{log channel} log was cleared. | - |
| Detected actions indicative of disabling and deleting IIS log files | Analysis of host data detected actions that show IIS log files being disabled and/or deleted. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|---|---------------------|
| Detected anomalous mix of upper and lower case characters in command line | Analysis of host data on % {Compromised Host} detected a command line with anomalous mix of upper and lower case characters. This kind of pattern, while possibly benign, is also typical of attackers trying to hide from case-sensitive or hash-based rule matching when performing administrative tasks on a compromised host. | - |
| Detected change to a registry key that can be abused to bypass UAC | Analysis of host data on % {Compromised Host} detected that a registry key that can be abused to bypass UAC (User Account Control) was changed. This kind of configuration, while possibly benign, is also typical of attacker activity when trying to move from unprivileged (standard user) to privileged (for example administrator) access on a compromised host. | - |
| Detected decoding of an executable using built-in certutil.exe tool | Analysis of host data on % {Compromised Host} detected that certutil.exe, a built-in administrator utility, was being used to decode an executable instead of its mainstream purpose that relates to manipulating certificates and certificate data. Attackers are known to abuse functionality of legitimate administrator tools to perform malicious actions, for example using a tool such as certutil.exe to decode a malicious executable that will then be subsequently executed. | - |
| Detected enabling of the WDigest UseLogonCredential registry key | Analysis of host data detected a change in the registry key HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest\ "UseLogonCredential". Specifically this key has been updated to allow logon credentials to be stored in clear text in LSA memory. Once enabled an attacker can dump clear text passwords from LSA memory with credential harvesting tools such as Mimikatz. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|---|---------------------|
| Detected encoded executable in command line data | Analysis of host data on %{Compromised Host} detected a base-64 encoded executable. This has previously been associated with attackers attempting to construct executables on-the-fly through a sequence of commands, and attempting to evade intrusion detection systems by ensuring that no individual command would trigger an alert. This could be legitimate activity, or an indication of a compromised host. | - |
| Detected obfuscated command line | Attackers use increasingly complex obfuscation techniques to evade detections that run against the underlying data. Analysis of host data on %{Compromised Host} detected suspicious indicators of obfuscation on the commandline. | - |
| Detected Petya ransomware indicators | Analysis of host data on %{Compromised Host} detected indicators associated with Petya ransomware. See https://blogs.technet.microsoft.com/mmpc/2017/06/27/new-ransomware-old-techniques-petya-adds-worm-capabilities/ for more information. Review the commandline associated in this alert and escalate this alert to your security team. | - |
| Detected possible execution of keygen executable | Analysis of host data on %{Compromised Host} detected execution of a process whose name is indicative of a keygen tool; such tools are typically used to defeat software licensing mechanisms but their download is often bundled with other malicious software. Activity group GOLD has been known to make use of such keygens to covertly gain back door access to hosts that they compromise. | - |
| Detected possible execution of malware dropper | Analysis of host data on %{Compromised Host} detected a filename that has previously been associated with one of activity group GOLD's methods of installing malware on a victim host. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|--|---------------------|
| Detected possible local reconnaissance activity | Analysis of host data on % {Compromised Host} detected a combination of systeminfo commands that has previously been associated with one of activity group GOLD's methods of performing reconnaissance activity. While 'systeminfo.exe' is a legitimate Windows tool, executing it twice in succession in the way that has occurred here is rare. | - |
| Detected potentially suspicious use of Telegram tool | Analysis of host data shows installation of Telegram, a free cloud-based instant messaging service that exists both for mobile and desktop system. Attackers are known to abuse this service to transfer malicious binaries to any other computer, phone, or tablet. | - |
| Detected suppression of legal notice displayed to users at logon | Analysis of host data on % {Compromised Host} detected changes to the registry key that controls whether a legal notice is displayed to users when they log on. Microsoft security analysis has determined that this is a common activity undertaken by attackers after having compromised a host. | - |
| Detected suspicious combination of HTA and PowerShell | mshta.exe (Microsoft HTML Application Host) which is a signed Microsoft binary is being used by the attackers to launch malicious PowerShell commands. Attackers often resort to having a HTA file with inline VBScript. When a victim browses to the HTA file and chooses to run it, the PowerShell commands and scripts that it contains are executed. Analysis of host data on % {Compromised Host} detected mshta.exe launching PowerShell commands. | - |
| Detected suspicious commandline arguments | Analysis of host data on % {Compromised Host} detected suspicious commandline arguments that have been used in conjunction with a reverse shell used by activity group HYDROGEN. | - |
| Detected suspicious commandline used to start all executables in a directory | Analysis of host data has detected a suspicious process running on % {Compromised Host}. The commandline indicates an attempt to start all executables (*.exe) that may reside in a directory. This could be an indication of a compromised host. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|--|---------------------|
| Detected suspicious credentials in commandline | Analysis of host data on % {Compromised Host} detected a suspicious password being used to execute a file by activity group BORON. This activity group has been known to use this password to execute Pirpi malware on a victim host. | - |
| Detected suspicious document credentials | Analysis of host data on % {Compromised Host} detected a suspicious, common precomputed password hash used by malware being used to execute a file. Activity group HYDROGEN has been known to use this password to execute malware on a victim host. | - |
| Detected suspicious execution of VBScript.Encode command | Analysis of host data on % {Compromised Host} detected the execution of VBScript.Encode command. This encodes the scripts into unreadable text, making it more difficult for users to examine the code. Microsoft threat research shows that attackers often use encoded VBscript files as part of their attack to evade detection systems. This could be legitimate activity, or an indication of a compromised host. | - |
| Detected suspicious execution via rundll32.exe | Analysis of host data on % {Compromised Host} detected rundll32.exe being used to execute a process with an uncommon name, consistent with the process naming scheme previously seen used by activity group GOLD when installing their first stage implant on a compromised host. | - |
| Detected suspicious file cleanup commands | Analysis of host data on % {Compromised Host} detected a combination of systeminfo commands that has previously been associated with one of activity group GOLD's methods of performing post-compromise self-cleanup activity. While 'systeminfo.exe' is a legitimate Windows tool, executing it twice in succession, followed by a delete command in the way that has occurred here is rare. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|---|---------------------|
| Detected suspicious file creation | <p>Analysis of host data on %{Compromised Host} detected creation or execution of a process which has previously indicated post-compromise action taken on a victim host by activity group BARIUM. This activity group has been known to use this technique to download additional malware to a compromised host after an attachment in a phishing doc has been opened.</p> | - |
| Detected suspicious named pipe communications | <p>Analysis of host data on %{Compromised Host} detected data being written to a local named pipe from a Windows console command. Named pipes are known to be a channel used by attackers to task and communicate with a malicious implant. This could be legitimate activity, or an indication of a compromised host.</p> | - |
| Detected suspicious network activity | <p>Analysis of network traffic from %{Compromised Host} detected suspicious network activity. Such traffic, while possibly benign, is typically used by an attacker to communicate with malicious servers for downloading of tools, command-and-control and exfiltration of data. Typical related attacker activity includes copying remote administration tools to a compromised host and exfiltrating user data from it.</p> | - |
| Detected suspicious new firewall rule | <p>Analysis of host data detected a new Firewall rule has been added via netsh.exe to allow traffic from an executable in a suspicious location.</p> | - |
| Detected suspicious use of Cacls to lower the security state of the system | <p>Attackers use myriad ways like brute force, spear phishing etc. to achieve initial compromise and get a foothold on the network . Once initial compromise is achieved they often take steps to lower the security settings of a system. Cacls—short for change access control list is Microsoft Windows native command line utility often used for modifying the security permission on folders and files. A lot of time the binary is used by the attackers to lower the security settings of a system. This is done by giving Everyone full access to some of the system binaries like ftp.exe, net.exe, wscript.exe etc. Analysis of host data on %{Compromised Host} detected suspicious use of Cacls to lower the security of a system.</p> | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|---|---------------------|
| Detected suspicious use of FTP -s Switch | Analysis of process creation data from the %{Compromised Host} detected the use of FTP's "-s:filename" switch. This switch is used to specify an FTP script file for the client to run. Malware or malicious processes are known to use this FTP switch (-s:filename) to point to a script file which is configured to connect to a remote FTP server and download additional malicious binaries. | - |
| Detected suspicious use of Pcalua.exe to launch executable code | Analysis of host data on %{Compromised Host} detected the use of pcalua.exe to launch executable code. Pcalua.exe is component of the Microsoft Windows "Program Compatibility Assistant" which detects compatibility issues during the installation or execution of a program. Attackers are known to abuse functionality of legitimate Windows system tools to perform malicious actions, for example using pcalua.exe with the -a switch to launch malicious executables either locally or from remote shares. | - |
| Detected the disabling of critical services | The analysis of host data on %{Compromised Host} detected execution of "net.exe stop" command being used to stop critical services like SharedAccess or Windows Security Center. The stopping of either of these service can be indication of a malicious behavior. | - |
| Digital currency mining related behavior detected | Analysis of host data on %{Compromised Host} detected the execution of a process or command normally associated with digital currency mining. | - |
| Dynamic PS script construction | Analysis of host data on %{Compromised Host} detected a PowerShell script being constructed dynamically. Attackers sometimes use this approach of progressively building up a script in order to evade IDS systems. This could be legitimate activity, or an indication that one of your machines has been compromised. | - |
| Executable found running from a suspicious location | Analysis of host data detected an executable file on %{Compromised Host} that is running from a location in common with known suspicious files. This executable could either be legitimate activity, or an indication of a compromised host. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|---|---------------------|
| High risk software detected | Analysis of host data from % {Compromised Host} detected the usage of software that has been associated with the installation of malware in the past. A common technique utilized in the distribution of malicious software is to package it within otherwise benign tools such as the one seen in this alert. Upon using these tools, the malware can be silently installed in the background. | - |
| Local Administrators group members were enumerated | Machine logs indicate a successful enumeration on group %{Enumerated Group Domain Name}%{Enumerated Group Name}. Specifically, % {Enumerating User Domain Name}% {Enumerating User Name} remotely enumerated the members of the % {Enumerated Group Domain Name}% {Enumerated Group Name} group. This activity could either be legitimate activity, or an indication that a machine in your organization has been compromised and used to reconnaissance %{vmname}. | - |
| Malicious firewall rule created by ZINC server implant [seen multiple times] | A firewall rule was created using techniques that match a known actor, ZINC. The rule was possibly used to open a port on % {Compromised Host} to allow for Command & Control communications. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Malicious SQL activity | Machine logs indicate that '%{process name}' was executed by account: %{user name}. This activity is considered malicious. | - |
| Masquerading Windows Module Detected | Crash dump analysis detected the presence of a 3rd party module impersonating a Windows module within a crash dump from the process identified in this alert. This occurrence may indicate a system compromise. | - |
| Multiple Domain Accounts Queried | Analysis of host data has determined that an unusual number of distinct domain accounts are being queried within a short time period from % {Compromised Host}. This kind of activity could be legitimate, but can also be an indication of compromise. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|--|---------------------|
| Possible credential dumping detected [seen multiple times] | Analysis of host data has detected use of native windows tool(e.g. sqldumper.exe) being used in a way that allows to extract credentials from memory. Often times attackers use these techniques to extract credentials that they then further use for lateral movement and privilege escalation. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Potential attempt to bypass AppLocker detected | Analysis of host data on %{Compromised Host} detected a potential attempt to bypass AppLocker restrictions. AppLocker can be configured to implement a policy that limits what executables are allowed to run on a Windows system. The command line pattern similar to that identified in this alert has been previously associated with attacker attempts to circumvent AppLocker policy by using trusted executables (allowed by AppLocker policy) to execute untrusted code. This could be legitimate activity, or an indication of a compromised host. | - |
| PsExec execution detected | Analysis of host data indicates that the process %{Process Name} was executed by PsExec utility. PsExec can be used for running processes remotely. This technique might be used for malicious purposes. | - |
| Ransomware indicators detected | Analysis of host data indicates suspicious activity traditionally associated with lock-screen and encryption ransomware. Lock screen ransomware displays a full-screen message preventing interactive use of the host and access to its files. Encryption ransomware prevents access by encrypting data files. In both cases a ransom message is typically displayed, requesting payment in order to restore file access. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|---|---------------------|
| Ransomware indicators detected [seen multiple times] | <p>Analysis of host data indicates suspicious activity traditionally associated with lock-screen and encryption ransomware. Lock screen ransomware displays a full-screen message preventing interactive use of the host and access to its files.</p> <p>Encryption ransomware prevents access by encrypting data files. In both cases a ransom message is typically displayed, requesting payment in order to restore file access. This behavior was seen [x] times today on the following machines: [Machine names]</p> | - |
| Rare SVCHOST service group executed | <p>The system process SVCHOST was observed running a rare service group. Malware often use SVCHOST to masquerade its malicious activity.</p> | - |
| Sticky keys attack detected | <p>Analysis of host data indicates that an attacker may be subverting an accessibility binary (for example sticky keys, onscreen keyboard, narrator) in order to provide backdoor access to the host %(Compromised Host).</p> | - |
| Successful brute force attack | <p>Multiple failed authentication attempts originating from the same source were detected across multiple hosts in Azure subscriptions . This resembles a password spray attack, in which an attacker performs numerous authentication attempts spread across multiple hosts. Some of the authentication attempts successfully signed in to a host in this subscription.</p> | - |
| Suspect integrity level indicative of RDP hijacking | <p>Analysis of host data has detected the tscon.exe running with SYSTEM privileges - this can be indicative of an attacker abusing this binary in order to switch context to any other logged on user on this host; it is a known attacker technique to compromise additional user accounts and move laterally across a network.</p> | - |
| Suspect service installation | <p>Analysis of host data has detected the installation of tscon.exe as a service: this binary being started as a service potentially allows an attacker to trivially switch to any other logged on user on this host by hijacking RDP connections; it is a known attacker technique to compromise additional user accounts and move laterally across a network.</p> | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|--|---------------------|
| Suspected Kerberos Golden Ticket attack parameters observed | Analysis of host data detected commandline parameters consistent with a Kerberos Golden Ticket attack. | - |
| Suspicious Account Creation Detected | Analysis of host data on %{Compromised Host} detected creation or use of a local account %{Suspicious account name} : this account name closely resembles a standard Windows account or group name '%{Similar To Account Name}'. This is potentially a rogue account created by an attacker, so named in order to avoid being noticed by a human administrator. | - |
| Suspicious Activity Detected | Analysis of host data has detected a sequence of one or more processes running on %{machine name} that have historically been associated with malicious activity. While individual commands may appear benign the alert is scored based on an aggregation of these commands. This could either be legitimate activity, or an indication of a compromised host. | - |
| Suspicious authentication activity | Although none of them succeeded, some of them used accounts were recognized by the host. This resembles a dictionary attack, in which an attacker performs numerous authentication attempts using a dictionary of predefined account names and passwords in order to find valid credentials to access the host. This indicates that some of your host account names might exist in a well-known account name dictionary. | - |
| Suspicious command execution | Machine logs indicate a suspicious command line execution by user %{user name}. | - |
| Suspicious double extension file executed | Analysis of host data indicates an execution of a process with a suspicious double extension. This extension may trick users into thinking files are safe to be opened and might indicate the presence of malware on the system. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|--|---------------------|
| Suspicious download using Certutil detected | <p>Analysis of host data on % {Compromised Host} detected the use of certutil.exe, a built-in administrator utility, for the download of a binary instead of its mainstream purpose that relates to manipulating certificates and certificate data. Attackers are known to abuse functionality of legitimate administrator tools to perform malicious actions, for example using certutil.exe to download and decode a malicious executable that will then be subsequently executed.</p> | - |
| Suspicious download using Certutil detected [seen multiple times] | <p>Analysis of host data on % {Compromised Host} detected the use of certutil.exe, a built-in administrator utility, for the download of a binary instead of its mainstream purpose that relates to manipulating certificates and certificate data. Attackers are known to abuse functionality of legitimate administrator tools to perform malicious actions, for example using certutil.exe to download and decode a malicious executable that will then be subsequently executed. This behavior was seen [x] times today on the following machines: [Machine names]</p> | - |
| Suspicious PowerShell Activity Detected | <p>Analysis of host data detected a PowerShell script running on % {Compromised Host} that has features in common with known suspicious scripts. This script could either be legitimate activity, or an indication of a compromised host.</p> | - |
| Suspicious PowerShell cmdlets executed | <p>Analysis of host data indicates execution of known malicious PowerShell PowerSploit cmdlets.</p> | - |
| Suspicious process executed | <p>Machine logs indicate that the suspicious process: '{Suspicious Process}' was running on the machine, often associated with attacker attempts to access credentials.'</p> | - |
| Suspicious process executed [seen multiple times] | <p>Machine logs indicate that the suspicious process: '{Suspicious Process}' was running on the machine, often associated with attacker attempts to access credentials. This behavior was seen [x] times today on the following machines: [Machine names]</p> | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|--|---------------------|
| Suspicious process name detected | Analysis of host data on %{Compromised Host} detected a process whose name is suspicious, for example corresponding to a known attacker tool or named in a way that is suggestive of attacker tools that try to hide in plain sight. This process could be legitimate activity, or an indication that one of your machines has been compromised. | - |
| Suspicious process name detected [seen multiple times] | Analysis of host data on %{Compromised Host} detected a process whose name is suspicious, for example corresponding to a known attacker tool or named in a way that is suggestive of attacker tools that try to hide in plain sight. This process could be legitimate activity, or an indication that one of your machines has been compromised. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Suspicious process termination burst | Analysis of host data indicates a suspicious process termination burst in %{Machine Name}. Specifically, %{NumberOfCommands} processes were killed between %{Begin} and %{Ending}. | - |
| Suspicious Screensaver process executed | The process '%{process name}' was observed executing from an uncommon location. Files with the .scr extensions are screen saver files and are normally reside and execute from the Windows system directory. | - |
| Suspicious SQL activity | Machine logs indicate that '%{process name}' was executed by account: %{user name}. This activity is uncommon with this account. | - |
| Suspicious SVCHOST process executed | The system process SVCHOST was observed running in an abnormal context. Malware often use SVCHOST to masquerade its malicious activity. | - |
| Suspicious system file execution | Analysis of host data detected an executable file on %{Compromised Host} that is running from an unusual location. This executable could either be legitimate activity, or an indication of a compromised host. | - |
| Suspicious system process executed | The system process %{process name} was observed running in an abnormal context. Malware often use this process name to masquerade its malicious activity. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|--|---------------------|
| Suspicious Volume Shadow Copy Activity | Analysis of host data has detected a shadow copy deletion activity on the resource. Volume Shadow Copy (VSC) is an important artifact that stores data snapshots. Some malware and specifically Ransomware, targets VSC to sabotage backup strategies. | - |
| Suspicious WindowPosition registry value detected | Analysis of host data on % {Compromised Host} detected an attempted WindowPosition registry configuration change that could be indicative of hiding application windows in non-visible sections of the desktop. This could be legitimate activity, or an indication of a compromised machine: this type of activity has been previously associated with known adware (or unwanted software) such as Win32/OneSystemCare and Win32/SystemHealer and malware such as Win32/Creprote. When the WindowPosition value is set to 201329664, (Hex: 0x0c00 0c00), corresponding to X-axis=0c00 and the Y-axis=0c00) this places the console app's window in a non-visible section of the user's screen in an area that is hidden from view below the visible start menu/taskbar. Known suspect Hex value includes, but not limited to c000c000 | - |
| Suspiciously named process detected | Analysis of host data on % {Compromised Host} detected a process whose name is very similar to but different from a very commonly run process (%{Similar To Process Name}). While this process could be benign attackers are known to sometimes hide in plain sight by naming their malicious tools to resemble legitimate process names. | - |
| Unusual process execution detected | Analysis of host data on % {Compromised Host} detected the execution of a process by %{User Name} that was unusual. Accounts such as % {User Name} tend to perform a limited set of operations, this execution was determined to be out of character and may be suspicious. | - |
| VBScript HTTP object allocation detected | Creation of a VBScript file using Command Prompt has been detected. The following script contains HTTP object allocation command. This action can be used to download malicious files. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|--|----------------------------|
| Windows registry persistence method detected | Analysis of host data has detected an attempt to persist an executable in the Windows registry. Malware often uses such a technique to survive a boot. | - |
| Code injection discovered | <p>Code injection is the insertion of executable modules into running processes or threads. This technique is used by malware to access data, while successfully hiding itself to prevent being found and removed.</p> <p>This alert indicates that an injected module is present in the crash dump. To differentiate between malicious and non-malicious injected modules, Security Center checks whether the injected module conforms to a profile of suspicious behavior.</p> | - |
| Suspicious code segment detected | Indicates that a code segment has been allocated by using non-standard methods, such as reflective injection and process hollowing. The alert provides additional characteristics of the code segment that have been processed to provide context for the capabilities and behaviors of the reported code segment. | - |
| Shellcode discovered | <p>Shellcode is the payload that is run after malware exploits a software vulnerability.</p> <p>This alert indicates that crash dump analysis has detected executable code that exhibits behavior commonly performed by malicious payloads.</p> <p>Although non-malicious software can also perform this behavior, it isn't typical of normal software development practices.</p> | - |
| Fileless attack technique detected | The memory of the process specified contains a fileless attack toolkit: [toolkit name]. Fileless attack toolkits typically don't have a presence on the file system, making detection by traditional antivirus software difficult. | DefenseEvasion / Execution |
| | | |

Alerts for Linux machines

[Further details and notes](#)

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|---|----------------------------------|
| Process seen accessing the SSH authorized keys file in an unusual way | An SSH authorized keys file has been accessed in a method similar to known malware campaigns. This access can indicate that an attacker is attempting to gain persistent access to a machine. | - |
| Detected Persistence Attempt | Host data analysis has detected that a startup script for single-user mode has been installed. Because it's rare that any legitimate process would be required to run in that mode, this might indicate that an attacker has added a malicious process to every run-level to guarantee persistence. | Persistence |
| Suspicious file timestamp modification | Host data analysis detected a suspicious timestamp modification. Attackers often copy timestamps from existing, legitimate files to new tools to avoid detection of these newly dropped files. | Persistence / DefenseEvasion |
| A new user was added to the sudoers group | Host data analysis detected that a user was added to the sudoers group, which enables its members to run commands with high privileges. | PrivilegeEscalation |
| Process associated with digital currency mining detected | Host data analysis detected the execution of a process that is normally associated with digital currency mining. | Exploitation / Execution |
| Potential port forwarding to external IP address | Host data analysis detected the initiation of port forwarding to an external IP address. | Exfiltration / CommandAndControl |
| A kernel module was loaded | A kernel module was loaded in the host %{compromised host} using the command %{Command used} by the user %{user}. | - |
| A kernel module was removed | A kernel module was removed in the host %{compromised host} using the command %{Command used} by the user %{user}. | - |
| Access of htaccess file detected | Analysis of host data on % {Compromised Host} detected possible manipulation of a htaccess file. Htaccess is a powerful configuration file that allows you to make multiple changes to a web server running the Apache Web software including basic redirect functionality, or for more advanced functions such as basic password protection. Attackers will often modify htaccess files on machines they have compromised to gain persistence. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|--|---------------------|
| An history file has been cleared | Analysis of host data indicates that the command history log file has been cleared. Attackers may do this to cover their traces. The operation was performed by user: '{user name}'. | - |
| Attempt to stop apt-daily-upgrade.timer service detected | Analysis of host data on % {Compromised Host} detected an attempt to stop apt-daily-upgrade.timer service. In some recent attacks ,its been observed attackers stopping this service ,to download malicious files and granting execution privileges for their attack | - |
| Attempt to stop apt-daily-upgrade.timer service detected [seen multiple times] | Analysis of host data on % {Compromised Host} detected an attempt to stop apt-daily-upgrade.timer service. In some recent attacks ,its been observed attackers stopping this service ,to download malicious files and granting execution privileges for their attack. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Behavior similar to common Linux bots detected | Analysis of host data on % {Compromised Host} detected the execution of a process normally associated with common Linux botnets. | - |
| Behavior similar to common Linux bots detected [seen multiple times] | Analysis of host data on % {Compromised Host} detected the execution of a process normally associated with common Linux botnets. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Behavior similar to Fairware ransomware detected | Analysis of host data on % {Compromised Host} detected the execution of rm -rf commands applied to suspicious locations. As rm -rf will recursively delete files, it is normally used on discrete folders. In this case, it is being used in a location that could remove a lot of data. Fairware ransomware is known to execute rm -rf commands in this folder. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|---|---------------------|
| Behavior similar to Fairware ransomware detected [seen multiple times] | Analysis of host data on %{Compromised Host} detected the execution of rm -rf commands applied to suspicious locations. As rm -rf will recursively delete files, it is normally used on discrete folders. In this case, it is being used in a location that could remove a lot of data. Fairware ransomware is known to execute rm -rf commands in this folder. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Behavior similar to ransomware detected [seen multiple times] | Analysis of host data on %{Compromised Host} detected the execution of files that have resemblance of known ransomware that can prevents users from accessing their system or personal files and demands ransom payment in order to regain access. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Container with a miner image detected | Machine logs indicate execution of a Docker container that run an image associated with a digital currency mining. This behavior can possibly indicate that your resources are abused by an attacker. | - |
| Detected anomalous mix of upper and lower case characters in command line | Analysis of host data on %{Compromised Host} detected a command line with anomalous mix of upper and lower case characters. This kind of pattern, while possibly benign, is also typical of attackers trying to hide from case-sensitive or hash-based rule matching when performing administrative tasks on a compromised host. | - |
| Detected file download from a known malicious source | Analysis of host data has detected the download of a file from a known malware source on %{Compromised Host}. | - |
| Detected file download from a known malicious source [seen multiple times] | Analysis of host data has detected the download of a file from a known malware source on %{Compromised Host}. This behavior was seen over [x] times today on the following machines: [Machine names] | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|--|---------------------|
| Detected Persistence Attempt [seen multiple times] | Analysis of host data on % {Compromised Host} has detected installation of a startup script for single-user mode. It is extremely rare than any legitimate process has any requirement to execute in that mode so may indicate an attacker has added a malicious process to every run-level to guarantee persistence. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Detected suspicious file download | Analysis of host data has detected suspicious download of remote file on % {Compromised Host}. | - |
| Detected suspicious file download [seen multiple times] | Analysis of host data has detected suspicious download of remote file on % {Compromised Host}. This behavior was seen 10 times today on the following machines: [Machine name] | - |
| Detected suspicious network activity | Analysis of network traffic from % {Compromised Host} detected suspicious network activity. Such traffic, while possibly benign, is typically used by an attacker to communicate with malicious servers for downloading of tools, command-and-control and exfiltration of data. Typical related attacker activity includes copying remote administration tools to a compromised host and exfiltrating user data from it. | - |
| Detected suspicious use of the nohup command | Analysis of host data has detected suspicious use of the nohup command on %(Compromised Host). Attackers have been seen running the command nohup from a temporary directory to allow their executables to run in the background. It is not normal to see this command run on files located in a temporary directory. | - |
| Detected suspicious use of the nohup command [seen multiple times] | Analysis of host data has detected suspicious use of the nohup command on %(Compromised Host). Attackers have been seen running the command nohup from a temporary directory to allow their executables to run in the background. It is not normal to see this command run on files located in a temporary directory. This behavior was seen [x] times today on the following machines: [Machine names] | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|--|---------------------|
| Detected suspicious use of the useradd command | Analysis of host data has detected suspicious use of the useradd command on %{Compromised Host}. | - |
| Detected suspicious use of the useradd command [seen multiple times] | Analysis of host data has detected suspicious use of the useradd command on %{Compromised Host}. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Digital currency mining related behavior detected | Analysis of host data on %{Compromised Host} detected the execution of a process or command normally associated with digital currency mining. | - |
| Disabling of auditd logging [seen multiple times] | The Linux Audit system provides a way to track security-relevant information on the system. It records as much information about the events that are happening on your system as possible. Disabling auditd logging could hamper discovering violations of security policies used on the system. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Executable found running from a suspicious location | Analysis of host data detected an executable file on %{Compromised Host} that is running from a location in common with known suspicious files. This executable could either be legitimate activity, or an indication of a compromised host. | - |
| Exploitation of Xorg vulnerability [seen multiple times] | Analysis of host data on %{Compromised Host} detected the user of Xorg with suspicious arguments. Attackers may use this technique in privilege escalation attempts. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Exposed Docker daemon detected | Machine logs indicate that your Docker daemon (dockerd) exposes a TCP socket. By default, Docker configuration, does not use encryption or authentication when a TCP socket is enabled. This enables full access to the Docker daemon, by anyone with access to the relevant port. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|---|---------------------|
| Failed SSH brute force attack | Failed brute force attacks were detected from the following attackers: % {Attackers}. Attackers were trying to access the host with the following user names: %{Accounts used on failed sign in to host attempts}. | - |
| Hidden file execution detected | Analysis of host data indicates that a hidden file was execute by %{user name}. This activity could either be legitimate activity, or an indication of a compromised host. | - |
| Indicators associated with DDOS toolkit detected | Analysis of host data on % {Compromised Host} detected file names that are part of a toolkit associated with malware capable of launching DDoS attacks, opening ports and services and taking full control over the infected system. This could also possibly be legitimate activity. | - |
| Indicators associated with DDOS toolkit detected [seen multiple times] | Analysis of host data on % {Compromised Host} detected file names that are part of a toolkit associated with malware capable of launching DDoS attacks, opening ports and services and taking full control over the infected system. This could also possibly be legitimate activity. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Local host reconnaissance detected | Analysis of host data on % {Compromised Host} detected the execution of a command normally associated with common Linux bot reconnaissance. | - |
| Local host reconnaissance detected [seen multiple times] | Analysis of host data on % {Compromised Host} detected the execution of a command normally associated with common Linux bot reconnaissance. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Manipulation of host firewall detected | Analysis of host data on % {Compromised Host} detected possible manipulation of the on-host firewall. Attackers will often disable this to exfiltrate data. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|---|---------------------|
| Manipulation of host firewall detected [seen multiple times] | Analysis of host data on % {Compromised Host} detected possible manipulation of the on-host firewall. Attackers will often disable this to exfiltrate data. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| New SSH key added | A new SSH key was added to the authorized keys file | - |
| New SSH key added [seen multiple times] | A new SSH key was added to the authorized keys file. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Possible attack tool detected | Machine logs indicate that the suspicious process: '%{Suspicious Process}' was running on % {Compromised Host}. This tool is often associated with malicious users attacking other machines in some way. | - |
| Possible attack tool detected [seen multiple times] | Machine logs indicate that the suspicious process: '%{Suspicious Process}' was running on % {Compromised Host}. This tool is often associated with malicious users attacking other machines in some way. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Possible backdoor detected [seen multiple times] | Analysis of host data has detected a suspicious file being downloaded then run on % {Compromised Host} in your subscription. This activity has previously been associated with installation of a backdoor. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Possible credential access tool detected | Machine logs indicate a possible known credential access tool was running on % {Compromised Host} launched by process: '%{Suspicious Process}'. This tool is often associated with attacker attempts to access credentials. | - |
| Possible credential access tool detected [seen multiple times] | Machine logs indicate a possible known credential access tool was running on % {Compromised Host} launched by process: '%{Suspicious Process}'. This tool is often associated with attacker attempts to access credentials. This behavior was seen [x] times today on the following machines: [Machine names] | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|--|---------------------|
| Possible exploitation of Hadoop Yarn | Analysis of host data on % {Compromised Host} detected the possible exploitation of the Hadoop Yarn service. | - |
| Possible Log Tampering Activity Detected | Analysis of host data on % {Compromised Host} detected possible removal of files that tracks user's activity during the course of its operation. Attackers often try to evade detection and leave no trace of malicious activities by deleting such log files. | - |
| Possible Log Tampering Activity Detected [seen multiple times] | Analysis of host data on % {Compromised Host} detected possible removal of files that tracks user's activity during the course of its operation. Attackers often try to evade detection and leave no trace of malicious activities by deleting such log files. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Possible loss of data detected | Analysis of host data on % {Compromised Host} detected a possible data egress condition. Attackers will often egress data from machines they have compromised. | - |
| Possible loss of data detected [seen multiple times] | Analysis of host data on % {Compromised Host} detected a possible data egress condition. Attackers will often egress data from machines they have compromised. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Possible malicious web shell detected | Analysis of host data on % {Compromised Host} detected a possible web shell. Attackers will often upload a web shell to a machine they have compromised to gain persistence or for further exploitation. | - |
| Possible malicious web shell detected [seen multiple times] | Analysis of host data on % {Compromised Host} detected a possible web shell. Attackers will often upload a web shell to a machine they have compromised to gain persistence or for further exploitation. This behavior was seen [x] times today on the following machines: [Machine names] | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|---|---------------------|
| Possible password change using crypt-method detected [seen multiple times] | Analysis of host data on %{Compromised Host} detected password change using crypt method. Attackers can make this change to continue access and gaining persistence after compromise. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Potential overriding of common files | Analysis of host data has detected common executables being overwritten on %{Compromised Host}. Attackers will overwrite common files as a way to obfuscate their actions or for persistence. | - |
| Potential overriding of common files [seen multiple times] | Analysis of host data has detected common executables being overwritten on %{Compromised Host}. Attackers will overwrite common files as a way to obfuscate their actions or for persistence. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Potential port forwarding to external IP address [seen multiple times] | Analysis of host data on %{Compromised Host} detected the initiation of port forwarding to an external IP address. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Potential reverse shell detected | Analysis of host data on %{Compromised Host} detected a potential reverse shell. These are used to get a compromised machine to call back into a machine an attacker owns. | - |
| Potential reverse shell detected [seen multiple times] | Analysis of host data on %{Compromised Host} detected a potential reverse shell. These are used to get a compromised machine to call back into a machine an attacker owns. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Privileged command run in container | Machine logs indicate that a privileged command was run in a Docker container. A privileged command has extended privileges on the host machine. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|---|---------------------|
| Privileged Container Detected | Machine logs indicate that a privileged Docker container is running. A privileged container has a full access to the host's resources. If compromised, an attacker can use the privileged container to gain access to the host machine. | - |
| Process associated with digital currency mining detected [seen multiple times] | Analysis of host data on % {Compromised Host} detected the execution of a process normally associated with digital currency mining. This behavior was seen over 100 times today on the following machines: [Machine name] | - |
| Python encoded downloader detected [seen multiple times] | Analysis of host data on % {Compromised Host} detected the execution of encoded Python that downloads and runs code from a remote location. This may be an indication of malicious activity. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Screenshot taken on host [seen multiple times] | Analysis of host data on % {Compromised Host} detected the user of a screen capture tool. Attackers may use these tools to access private data. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Script extension mismatch detected | Analysis of host data on % {Compromised Host} detected a mismatch between the script interpreter and the extension of the script file provided as input. This has frequently been associated with attacker script executions. | - |
| Script extension mismatch detected [seen multiple times] | Analysis of host data on % {Compromised Host} detected a mismatch between the script interpreter and the extension of the script file provided as input. This has frequently been associated with attacker script executions. This behavior was seen [x] times today on the following machines: [Machine names] | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|--|---------------------|
| Shellcode detected [seen multiple times] | <p>Analysis of host data on %{Compromised Host} detected shellcode being generated from the command line. This process could be legitimate activity, or an indication that one of your machines has been compromised. This behavior was seen [x] times today on the following machines: [Machine names]</p> | - |
| SSH server is running inside a container | <p>Machine logs indicate that an SSH server is running inside a Docker container. While this behavior can be intentional, it frequently indicates that a container is misconfigured or breached.</p> | - |
| Successful SSH brute force attack | <p>Analysis of host data has detected a successful brute force attack. The IP %{Attacker source IP} was seen making multiple login attempts. Successful logins were made from that IP with the following user(s): %{Accounts used to successfully sign in to host}. This means that the host may be compromised and controlled by a malicious actor.</p> | - |
| Suspicious Account Creation Detected | <p>Analysis of host data on %{Compromised Host} detected creation or use of a local account %{Suspicious account name} : this account name closely resembles a standard Windows account or group name '%{Similar To Account Name}'. This is potentially a rogue account created by an attacker, so named in order to avoid being noticed by a human administrator.</p> | - |
| Suspicious compilation detected | <p>Analysis of host data on %{Compromised Host} detected suspicious compilation. Attackers will often compile exploits on a machine they have compromised to escalate privileges.</p> | - |
| Suspicious compilation detected [seen multiple times] | <p>Analysis of host data on %{Compromised Host} detected suspicious compilation. Attackers will often compile exploits on a machine they have compromised to escalate privileges. This behavior was seen [x] times today on the following machines: [Machine names]</p> | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|---|---------------------|
| Suspicious kernel module detected [seen multiple times] | Analysis of host data on %{Compromised Host} detected a shared object file being loaded as a kernel module. This could be legitimate activity, or an indication that one of your machines has been compromised. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Suspicious password access | Analysis of host data has detected suspicious access to encrypted user passwords on %{Compromised Host}. | - |
| Suspicious password access [seen multiple times] | Analysis of host data has detected suspicious access to encrypted user passwords on %{Compromised Host}. This behavior was seen [x] times today on the following machines: [Machine names] | - |
| Suspicious PHP execution detected | Machine logs indicate a that a suspicious PHP process is running. The action included an attempt to run OS commands or PHP code from the command line using the PHP process. While this behavior can be legitimate, in web applications this behavior is also observed in malicious activities such as attempts to infect websites with web shells. | - |
| Suspicious request to Kubernetes API | Machine logs indicate that a suspicious request was made to the Kubernetes API. The request was sent from a Kubernetes node, possibly from one of the containers running in the node. Although this behavior can be intentional, it might indicate that the node is running a compromised container. | - |
| | | |

Alerts for Azure App Service

[Further details and notes](#)

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|---|---------------------|
| An attempt to run Linux commands on a Windows App Service | Analysis of App Service processes detected an attempt to run a Linux command on a Windows App Service. This action was running by the web application. This behavior is often seen during campaigns that exploit a vulnerability in a common web application. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|--|---------------------|
| An IP that connected to your Azure App Service FTP Interface was found in Threat Intelligence | App Service FTP logs analysis has detected a connection from a source address that was found in the threat intelligence feed. During this connection, a user accessed the pages listed. | - |
| Anomalous requests pattern detected | The Azure App Service activity log indicates an anomalous HTTP activity to the App Service from %(Source IP). This activity resembles a pattern of Fuzzing \ Brute force activity. | - |
| Attempt to run high privilege command detected | Analysis of App Service processes has detected an attempt to run a command that requires high privileges. The command ran in the web application context. While this behavior can be legitimate, in web applications this behavior might indicate malicious activities. | - |
| Connection to web page from anomalous IP address detected | The Azure App Service activity log indicates a connection to a sensitive web page from a source IP address (% {Source IP Address}) that has never connected to it before. This might indicate that someone is attempting a brute force attack into your web app administration pages. It might also be the result of a new IP address being used by a legitimate user. | - |
| Raw data download detected | Analysis of App Service processes detected an attempt to download code from raw-data websites such as Pastebin. This action was run by a PHP process. This behavior is associated with attempts to download web shells or other malicious components to the App Service. | - |
| Phishing content hosted on Azure Webapps | URL used for phishing attack found on the Azure AppServices website. This URL was part of a phishing attack sent to O365 customers. The content typically lures visitors into entering their corporate credentials or financial information into a legitimate looking website. | Collection |
| PHP file in upload folder | The Azure App Service activity log indicates an access to a suspicious PHP page located in the upload folder. This type of folder does not usually contain PHP files. The existence of this type of file might indicate an exploitation taking advantage of arbitrary file upload vulnerabilities. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|---|---------------------|
| Saving curl output to disk detected | Analysis of App Service processes detected the running of a curl command in which the output was saved to the disk. While this behavior can be legitimate, in web applications this behavior is also observed in malicious activities such as attempts to infect websites with web shells. | - |
| Spam folder referrer detected | Azure App Service activity log indicates web activity that was identified as originating from a web site associated with SPAM activity. This could occur if your web site is compromised and used for spam activity. | - |
| Suspicious access to possibly vulnerable web page detected | The App Service activity log indicates that a web page that seems to be sensitive was accessed. This suspicious activity originated from a source address whose access pattern resembles that of a web scanner. This kind of activity is often associated with an attempt by an attacker to scan your network to try to gain access to sensitive or vulnerable web pages. | - |
| Suspicious PHP execution detected | Machine logs indicate that a suspicious PHP process is running. The action included an attempt to run operating system commands or PHP code from the command line, by using the PHP process. While this behavior can be legitimate, in web applications this behavior might indicate malicious activities, such as attempts to infect websites with web shells. | Execution |
| Suspicious User Agent detected | Azure App Service activity log indicates requests with suspicious user agent. This behavior can indicate on attempts to exploit a vulnerability in your App Service application. | - |
| Suspicious WordPress theme invocation detected | The App Service activity log indicates a possible code injection activity on your App Service resource. This suspicious activity resembles activity that manipulates a WordPress theme to support server-side execution of code, followed by a direct web request to invoke the manipulated theme file. This type of activity can be part of an attack campaign over WordPress. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|--|---------------------|
| Vulnerability scanner detected (Joomla/WordPress/CMS) | The Azure App Service activity log indicates that a possible vulnerability scanner was used on your App Service resource. The suspicious activity detected resembles that of tools targeting Joomla applications / WordPress applications / a content management system (CMS). | - |
| Web fingerprinting detected (NMAP / Blind Elephant) | The App Service activity log indicates a possible web fingerprinting activity on your App Service resource. This suspicious activity is associated with a tool called Blind Elephant. The tool fingerprints web servers and tries to detect the installed applications and their versions. Attackers often use this tool for probing the web applications to find vulnerabilities. | - |
| | | |

Alerts for containers - Azure Kubernetes Service clusters

Further details and notes

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|---|---------------------|
| PREVIEW - Role binding to the cluster-admin role detected | Kubernetes audit log analysis detected a new binding to the cluster-admin role resulting in administrator privileges. Unnecessarily providing administrator privileges might result in privilege escalation issues in the cluster. | Persistence |
| PREVIEW - Exposed Kubernetes dashboard detected | Kubernetes audit log analysis detected exposure of the Kubernetes Dashboard by a LoadBalancer service. Exposed dashboards allow unauthenticated access to the cluster management and pose a security threat. | Persistence |
| PREVIEW - New high privileges role detected | Kubernetes audit log analysis detected a new role with high privileges. A binding to a role with high privileges gives the user/group elevated privileges in the cluster. Unnecessarily providing elevated privileges might result in privilege escalation issues in the cluster. | Persistence |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|---|---------------------|
| PREVIEW - New container in the kube-system namespace detected | Kubernetes audit log analysis detected a new container in the kube-system namespace that isn't among the containers that normally run in this namespace. The kube-system namespaces shouldn't contain user resources. Attackers can use this namespace to hide malicious components. | Persistence |
| PREVIEW - Digital currency mining container detected | Kubernetes audit log analysis detected a container that has an image associated with a digital currency mining tool. | Execution |
| PREVIEW - Privileged container detected | Kubernetes audit log analysis detected a new privileged container. A privileged container has access to the node's resources and breaks the isolation between containers. If compromised, an attacker can use the privileged container to gain access to the node. | PrivilegeEscalation |
| PREVIEW - Container with a sensitive volume mount detected | Kubernetes audit log analysis detected a new container with a sensitive volume mount. The volume that was detected is a hostPath type that mounts a sensitive file or folder from the node to the container. If the container gets compromised, the attacker can use this mount to gain access to the node. | PrivilegeEscalation |
| | | |

Alerts for containers - host level

[Further details and notes](#)

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|---|---------------------------------|
| Privileged Container Detected | Machine logs indicate that a privileged Docker container is running. A privileged container has full access to the host's resources. If compromised, an attacker can use the privileged container to gain access to the host machine. | PrivilegeEscalation / Execution |
| Privileged command run in container | Machine logs indicate that a privileged command was run in a Docker container. A privileged command has extended privileges on the host machine. | PrivilegeEscalation |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|--|--------------------------|
| Exposed Docker daemon detected | Machine logs indicate that your Docker daemon (dockerd) exposes a TCP socket. By default, Docker configuration doesn't use encryption or authentication when a TCP socket is enabled. Anyone with access to the relevant port can then get full access to the Docker daemon. | Exploitation / Execution |
| SSH server is running inside a container | Machine logs indicate that an SSH server is running inside a Docker container. While this behavior can be intentional, it frequently indicates that a container is misconfigured or breached. | Execution |
| Container with a miner image detected | Machine logs indicate execution of a Docker container running an image associated with digital currency mining. This behavior can possibly indicate that your resources are being abused. | Execution |
| Suspicious request to Kubernetes API | Machine logs indicate that a suspicious request was made to the Kubernetes API. The request was sent from a Kubernetes node, possibly from one of the containers running in the node. Although this behavior can be intentional, it might indicate that the node is running a compromised container. | Execution |
| Suspicious request to the Kubernetes Dashboard | Machine logs indicate that a suspicious request was made to the Kubernetes Dashboard. The request was sent from a Kubernetes node, possibly from one of the containers running in the node. Although this behavior can be intentional, it might indicate that the node is running a compromised container. | - |
| | | |

Alerts for SQL Database and SQL Data Warehouse

[Further details and notes](#)

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|-------|-------------|---------------------|
| | | |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|--|---------------------|
| A possible vulnerability to SQL Injection | <p>An application has generated a faulty SQL statement in the database. This can indicate a possible vulnerability to SQL injection attacks. There are two possible reasons for a faulty statement. A defect in application code might have constructed the faulty SQL statement. Or, application code or stored procedures didn't sanitize user input when constructing the faulty SQL statement, which can be exploited for SQL injection.</p> | - |
| Attempted logon by a potentially harmful application | <p>A potentially harmful application has been used to access the database. In some cases, the alert detects penetration testing in action. In other cases, the alert detects an attack that uses common tools.</p> | Probing |
| Logon from an unusual location | <p>There has been a change in the access pattern to SQL Server, where someone has signed in to the server from an unusual geographical location. In some cases, the alert detects a legitimate action (a new application or developer maintenance). In other cases, the alert detects a malicious action (a former employee or external attacker).</p> | Exploitation |
| Logon by an unfamiliar principal | <p>There has been a change in the access pattern to SQL Server. Someone has signed in to the server by using an unusual principal (user). In some cases, the alert detects a legitimate action (a new application or developer maintenance). In other cases, the alert detects a malicious action (a former employee or external attacker).</p> | Exploitation |
| Potential SQL Brute Force attempt | <p>An abnormally high number of failed sign-ins with different credentials have occurred. In some cases, the alert detects penetration testing in action. In other cases, the alert detects a brute force attack.</p> | Probing |
| Potential SQL injection | <p>An active exploit has occurred against an identified application vulnerable to SQL injection. This means an attacker is trying to inject malicious SQL statements by using the vulnerable application code or stored procedures.</p> | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|---|---------------------|
| Logon from an unusual Azure Data Center | There has been a change in the access pattern to an SQL Server, where someone has signed in to the server from an unusual Azure Data Center. In some cases, the alert detects a legitimate action (a new application or Azure service). In other cases, the alert detects a malicious action (attacker operating from breached resource in Azure). | Probing |
| Potentially Unsafe Action | High privileged SQL command which is commonly used in malicious sessions has been executed in an SQL Server. Those commands are recommended to be disabled by default. In some cases, the alert detects a legitimate action (admin script running). In other cases, the alert detects a malicious action (attacker using SQL trusts to breach Windows layer). | Execution |
| Unusual export location | There has been a change in the export storage destination for a SQL import and export operation. In some cases, the alert detects a legitimate change (new backup destination). In other cases, the alert detects a malicious action (attacker easily exfiltrated data to a file). | Exfiltration |
| | | |

Alerts for Azure Storage

[Further details and notes](#)

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|---|---------------------|
| PREVIEW - Potential malware uploaded to a storage account | Indicates that a blob containing potential malware has been uploaded to a storage account. Potential causes may include an intentional malware upload by an attacker or an unintentional upload, of a potentially malicious blob, by a legitimate user. | LateralMovement |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|---|------------------------|
| Access from a Tor exit node to a storage account | Indicates that this account has been accessed successfully from an IP address that is known as an active exit node of Tor (an anonymizing proxy). The severity of this alert considers the authentication type used (if any), and whether this is the first case of such access. Potential causes can be an attacker who has accessed your storage account by using Tor, or a legitimate user who has accessed your storage account by using Tor. | Probing / Exploitation |
| Access from an unusual location to a storage account | Indicates that there was a change in the access pattern to an Azure Storage account. Someone has accessed this account from an IP address considered unfamiliar when compared with recent activity. Either an attacker has gained access to the account, or a legitimate user has connected from a new or unusual geographic location. An example of the latter is remote maintenance from a new application or developer. | Exploitation |
| Anonymous access to a storage account | Indicates that there's a change in the access pattern to a storage account. For instance, the account has been accessed anonymously (without any authentication), which is unexpected compared to the recent access pattern on this account. A potential cause is that an attacker has exploited public read access to a container that holds blob storage. | Exploitation |
| Unusual access inspection in a storage account | Indicates that the access permissions of a storage account have been inspected in an unusual way, compared to recent activity on this account. A potential cause is that an attacker has performed reconnaissance for a future attack. | Collection |
| Unusual amount of data extracted from a storage account | Indicates that an unusually large amount of data has been extracted compared to recent activity on this storage container. A potential cause is that an attacker has extracted a large amount of data from a container that holds blob storage. | Exfiltration |
| Unusual application accessed a storage account | Indicates that an unusual application has accessed this storage account. A potential cause is that an attacker has accessed your storage account by using a new application. | Exploitation |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|--|-----------------------------|
| Unusual change of access permissions in a storage account | Indicates that the access permissions of this storage container have been changed in an unusual way. A potential cause is that an attacker has changed container permissions to weaken its security posture or to gain persistence. | Persistence |
| Unusual data exploration in a storage account | Indicates that blobs or containers in a storage account have been enumerated in an abnormal way, compared to recent activity on this account. A potential cause is that an attacker has performed reconnaissance for a future attack. | Collection |
| Unusual deletion in a storage account | Indicates that one or more unexpected delete operations has occurred in a storage account, compared to recent activity on this account. A potential cause is that an attacker has deleted data from your storage account. | Exfiltration |
| Unusual upload of .cspkg to a storage account | Indicates that an Azure Cloud Services package (.cspkg file) has been uploaded to a storage account in an unusual way, compared to recent activity on this account. A potential cause is that an attacker has been preparing to deploy malicious code from your storage account to an Azure cloud service. | LateralMovement / Execution |
| Unusual upload of .exe to a storage account | Indicates that an .exe file has been uploaded to a storage account in an unusual way, compared to recent activity on this account. A potential cause is that an attacker has uploaded a malicious executable file to your storage account, or that a legitimate user has uploaded an executable file. | LateralMovement / Execution |
| | | |

Alerts for Azure Cosmos DB (Preview)

Further details and notes

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|--|---------------------|
| Access from an unusual location to a Cosmos DB account | Indicates that there was a change in the access pattern to an Azure Cosmos DB account. Someone has accessed this account from an unfamiliar IP address, compared to recent activity. Either an attacker has accessed the account, or a legitimate user has accessed it from a new and unusual geographical location. An example of the latter is remote maintenance from a new application or developer. | Exploitation |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|---|---------------------|
| Unusual amount of data extracted from a Cosmos DB account | <p>Indicates that there was a change in the data extraction pattern from an Azure Cosmos DB account. Someone has extracted an unusual amount of data compared to recent activity. An attacker might have extracted a large amount of data from an Azure Cosmos DB database (for example, data exfiltration or leakage, or an unauthorized transfer of data). Or, a legitimate user or application might have extracted an unusual amount of data from a container (for example, for maintenance backup activity).</p> | Exfiltration |
| | | |

Alerts for Azure network layer

[Further details and notes](#)

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|--|---------------------|
| Network communication with a malicious machine detected | <p>Network traffic analysis indicates that your machine (IP %{Victim IP}) has communicated with what is possibly a Command and Control center. When the compromised resource is a load balancer or an application gateway, the suspected activity might indicate that one or more of the resources in the backend pool (of the load balancer or application gateway) has communicated with what is possibly a Command and Control center.</p> | - |
| Possible compromised machine detected | <p>Threat intelligence indicates that your machine (at IP %{Machine IP}) may have been compromised by a malware of type Conficker. Conficker was a computer worm that targets the Microsoft Windows operating system and was first detected in November 2008. Conficker infected millions of computers including government, business and home computers in over 200 countries, making it the largest known computer worm infection since the 2003 Welchia worm.</p> | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|---|---------------------|
| Possible incoming %{Service Name} brute force attempts detected | <p>Network traffic analysis detected incoming %{Service Name} communication to %{Victim IP}, associated with your resource % {Compromised Host} from %{Attacker IP}. When the compromised resource is a load balancer or an application gateway, the suspected incoming traffic has been forwarded to one or more of the resources in the backend pool (of the load balancer or application gateway). Specifically, sampled network data shows suspicious activity between %{Start Time} and %{End Time} on port %{Victim Port}. This activity is consistent with brute force attempts against %{Service Name} servers.</p> | - |
| Possible incoming SQL brute force attempts detected | <p>Network traffic analysis detected incoming SQL communication to % {Victim IP}, associated with your resource %{Compromised Host}, from % {Attacker IP}. When the compromised resource is a load balancer or an application gateway, the suspected incoming traffic has been forwarded to one or more of the resources in the backend pool (of the load balancer or application gateway). Specifically, sampled network data shows suspicious activity between %{Start Time} and % {End Time} on port %{Port Number} (% {SQL Service Type}). This activity is consistent with brute force attempts against SQL servers.</p> | - |
| Possible outgoing denial-of-service attack detected | <p>Network traffic analysis detected anomalous outgoing activity originating from %{Compromised Host}, a resource in your deployment. This activity may indicate that your resource was compromised and is now engaged in denial-of-service attacks against external endpoints. When the compromised resource is a load balancer or an application gateway, the suspected activity might indicate that one or more of the resources in the backend pool (of the load balancer or application gateway) was compromised. Based on the volume of connections, we believe that the following IPs are possibly the targets of the DOS attack: %{Possible Victims}. Note that it is possible that the communication to some of these IPs is legitimate.</p> | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|--|---------------------|
| Possible outgoing port scanning activity detected | <p>Network traffic analysis detected suspicious outgoing traffic from % {Compromised Host}. This traffic may be a result of a port scanning activity. When the compromised resource is a load balancer or an application gateway, the suspected outgoing traffic has been originated from one or more of the resources in the backend pool (of the load balancer or application gateway). If this behavior is intentional, please note that performing port scanning is against Azure Terms of service. If this behavior is unintentional, it may mean your resource has been compromised.</p> | - |
| Suspicious incoming RDP network activity | <p>Network traffic analysis detected anomalous incoming Remote Desktop Protocol (RDP) communication to % {Victim IP}, associated with your resource %{Compromised Host}, from % {Attacker IP}. When the compromised resource is a load balancer or an application gateway, the suspected incoming traffic has been forwarded to one or more of the resources in the backend pool (of the load balancer or application gateway). Specifically, sampled network data shows % {Number of Connections} incoming connections to your resource, which is considered abnormal for this environment. This activity may indicate an attempt to brute force your RDP end point</p> | - |
| Suspicious incoming RDP network activity from multiple sources | <p>Network traffic analysis detected anomalous incoming Remote Desktop Protocol (RDP) communication to % {Victim IP}, associated with your resource %{Compromised Host}, from multiple sources. When the compromised resource is a load balancer or an application gateway, the suspected incoming traffic has been forwarded to one or more of the resources in the backend pool (of the load balancer or application gateway). Specifically, sampled network data shows %{Number of Attacking IPs} unique IPs connecting to your resource, which is considered abnormal for this environment. This activity may indicate an attempt to brute force your RDP end point from multiple hosts (Botnet)</p> | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|---|---------------------|
| Suspicious incoming SSH network activity | <p>Network traffic analysis detected anomalous incoming SSH communication to %{Victim IP}, associated with your resource % {Compromised Host}, from %{Attacker IP}. When the compromised resource is a load balancer or an application gateway, the suspected incoming traffic has been forwarded to one or more of the resources in the backend pool (of the load balancer or application gateway). Specifically, sampled network data shows %{Number of Connections} incoming connections to your resource, which is considered abnormal for this environment. This activity may indicate an attempt to brute force your SSH end point</p> | - |
| Suspicious incoming SSH network activity from multiple sources | <p>Network traffic analysis detected anomalous incoming SSH communication to %{Victim IP}, associated with your resource % {Compromised Host}, from multiple sources. When the compromised resource is a load balancer or an application gateway, the suspected incoming traffic has been forwarded to one or more of the resources in the backend pool (of the load balancer or application gateway). Specifically, sampled network data shows % {Number of Attacking IPs} unique IPs connecting to your resource, which is considered abnormal for this environment. This activity may indicate an attempt to brute force your SSH end point from multiple hosts (Botnet)</p> | - |
| Suspicious outgoing %{Attacked Protocol} traffic detected | <p>Network traffic analysis detected suspicious outgoing traffic from % {Compromised Host} to destination port %{Most Common Port}. When the compromised resource is a load balancer or an application gateway, the suspected outgoing traffic has been originated from to one or more of the resources in the backend pool (of the load balancer or application gateway). This behavior may indicate that your resource is taking part in %{Attacked Protocol} brute force attempts or port sweeping attacks.</p> | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|--|---------------------|
| Suspicious outgoing RDP network activity | <p>Network traffic analysis detected anomalous outgoing Remote Desktop Protocol (RDP) communication to % {Victim IP} originating from % {Compromised Host} (%{Attacker IP}), a resource in your deployment. When the compromised resource is a load balancer or an application gateway, the suspected outgoing traffic has been originated from to one or more of the resources in the backend pool (of the load balancer or application gateway). Specifically, sampled network data shows %{Number of Connections} outgoing connections from your resource, which is considered abnormal for this environment. This activity may indicate that your machine was compromised and is now used to brute force external RDP end points. Note that this type of activity could possibly cause your IP to be flagged as malicious by external entities.</p> | - |
| Suspicious outgoing RDP network activity to multiple destinations | <p>Network traffic analysis detected anomalous outgoing Remote Desktop Protocol (RDP) communication to multiple destinations originating from % {Compromised Host} (%{Attacker IP}), a resource in your deployment. When the compromised resource is a load balancer or an application gateway, the suspected outgoing traffic has been originated from to one or more of the resources in the backend pool (of the load balancer or application gateway). Specifically, sampled network data shows your machine connecting to % {Number of Attacked IPs} unique IPs, which is considered abnormal for this environment. This activity may indicate that your resource was compromised and is now used to brute force external RDP end points. Note that this type of activity could possibly cause your IP to be flagged as malicious by external entities.</p> | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|---|---------------------|
| Suspicious outgoing SSH network activity | <p>Network traffic analysis detected anomalous outgoing SSH communication to %{Victim IP} originating from %{Compromised Host} (%{Attacker IP}), a resource in your deployment. When the compromised resource is a load balancer or an application gateway, the suspected outgoing traffic has been originated from to one or more of the resources in the backend pool (of the load balancer or application gateway). Specifically, sampled network data shows % {Number of Connections} outgoing connections from your resource, which is considered abnormal for this environment. This activity may indicate that your resource was compromised and is now used to brute force external SSH end points. Note that this type of activity could possibly cause your IP to be flagged as malicious by external entities.</p> | - |
| Suspicious outgoing SSH network activity to multiple destinations | <p>Network traffic analysis detected anomalous outgoing SSH communication to multiple destinations originating from %{Compromised Host} (%{Attacker IP}), a resource in your deployment. When the compromised resource is a load balancer or an application gateway, the suspected outgoing traffic has been originated from to one or more of the resources in the backend pool (of the load balancer or application gateway). Specifically, sampled network data shows your resource connecting to %{Number of Attacked IPs} unique IPs, which is considered abnormal for this environment. This activity may indicate that your resource was compromised and is now used to brute force external SSH end points. Note that this type of activity could possibly cause your IP to be flagged as malicious by external entities.</p> | - |
| Traffic detected from IP addresses recommended for blocking | <p>Azure Security Center detected inbound traffic from IP addresses that are recommended to be blocked. This typically occurs when this IP address doesn't communicate regularly with this resource. Alternatively, the IP address has been flagged as malicious by Security Center's threat intelligence sources.</p> | Probing |
| | | |

Alerts for Azure Resource Manager (Preview)

[Further details and notes](#)

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|---|---------------------|
| PREVIEW - Azurite toolkit run detected | A known cloud-environment reconnaissance toolkit run has been detected in your environment. The tool Azurite can be used by an attacker (or penetration tester) to map your subscriptions' resources and identify insecure configurations. | - |
| PREVIEW – MicroBurst toolkit “Get-AzureDomainInfo” function run detected | A known cloud-environment reconnaissance toolkit run has been detected in your environment. The tool “MicroBurst” (see https://github.com/NetSPI/MicroBurst) can be used by an attacker (or penetration tester) to map your subscription(s) resources, identify insecure configurations, and leak confidential information. | - |
| PREVIEW - Suspicious management session using an inactive account detected | Subscription activity logs analysis has detected suspicious behavior. A principal not in use for a long period of time is now performing actions that can secure persistence for an attacker. | Persistence |
| PREVIEW – MicroBurst toolkit “Get-AzurePasswords” function run detected | A known cloud-environment reconnaissance toolkit run has been detected in your environment. The tool “MicroBurst” (see https://github.com/NetSPI/MicroBurst) can be used by an attacker (or penetration tester) to map your subscription(s) resources, identify insecure configurations, and leak confidential information. | - |
| PREVIEW – Suspicious management session using Azure portal detected | Analysis of your subscription activity logs has detected a suspicious behavior. A principal that doesn't regularly use the Azure portal (Ibiza) to manage the subscription environment (hasn't used Azure portal to manage for the last 45 days, or a subscription that it is actively managing), is now using the Azure portal and performing actions that can secure persistence for an attacker. | - |
| PREVIEW - Suspicious management session using PowerShell detected | Subscription activity logs analysis has detected suspicious behavior. A principal that doesn't regularly use PowerShell to manage the subscription environment is now using PowerShell, and performing actions that can secure persistence for an attacker. | Persistence |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|--|---------------------|
| Activity from anonymous IP addresses | <p>Users activity from an IP address that has been identified as an anonymous proxy IP address has been detected. These proxies are used by people who want to hide their device's IP address, and can be used for malicious intent. This detection uses a machine learning algorithm that reduces false positives, such as mis-tagged IP addresses that are widely used by users in the organization.</p> | - |
| Activity from infrequent country | <p>Activity from a location that wasn't recently or ever visited by any user in the organization has occurred. This detection considers past activity locations to determine new and infrequent locations. The anomaly detection engine stores information about previous locations used by users in the organization.</p> | - |
| Impossible travel activity | <p>Two user activities (in a single or multiple sessions) have occurred, originating from geographically distant locations. This occurs within a time period shorter than the time it would have taken the user to travel from the first location to the second. This indicates that a different user is using the same credentials. This detection uses a machine learning algorithm that ignores obvious false positives contributing to the impossible travel conditions, such as VPNs and locations regularly used by other users in the organization. The detection has an initial learning period of seven days, during which it learns a new user's activity pattern.</p> | - |
| Use of advanced Azure persistence techniques | <p>Subscription activity logs analysis has detected suspicious behavior. Customized roles have been given legitimized identity entities. This can lead the attacker to gain persistency in an Azure customer environment.</p> | - |
| | | |

Alerts for Azure Key Vault (Preview)

[Further details and notes](#)

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|-------|-------------|---------------------|
| | | |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|--|---------------------|
| Access from a TOR exit node to a Key Vault | The Key Vault has been accessed by someone using the TOR IP anonymization system to hide their location. Malicious actors often try to hide their location when attempting to gain unauthorized access to internet-connected resources. | - |
| High volume of operations in a Key Vault | A larger volume of Key Vault operations has been performed compared with historical data. Key Vault activity is typically the same over time. This may be a legitimate change inactivity. Alternatively, your infrastructure might be compromised and further investigations are necessary. | - |
| Suspicious policy change and secret query in a Key Vault | A Key Vault policy change has been made and then operations to list and/or get secrets occurred. In addition, this operation pattern isn't normally performed by the user on this vault. This is highly indicative that the Key Vault is compromised and the secrets within have been stolen by a malicious actor. | - |
| Suspicious secret listing and query in a Key Vault | A Secret List operation was followed by many Secret Get operations. Also, this operation pattern isn't normally performed by the user on this vault. This indicates that someone could be dumping the secrets stored in the Key Vault for potentially malicious purposes. | - |
| Unusual user-application pair accessed a Key Vault | The Key Vault has been accessed by a User-Application pairing that doesn't normally access it. This may be a legitimate access attempt (for example, following an infrastructure or code update). This is also a possible indication that your infrastructure is compromised and a malicious actor is trying to access your Key Vault. | - |
| Unusual application accessed a Key Vault | The Key Vault has been accessed by an Application that doesn't normally access it. This may be a legitimate access attempt (for example, following an infrastructure or code update). This is also a possible indication that your infrastructure is compromised and a malicious actor is trying to access your Key Vault. | - |

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|---|---|---------------------|
| Unusual user accessed a Key Vault | The Key Vault has been accessed by a User that doesn't normally access it. This may be a legitimate access attempt (for example, a new user needing access has joined the organization). This is also a possible indication that your infrastructure is compromised and a malicious actor is trying to access your Key Vault. | - |
| Unusual operation pattern in a Key Vault | An unusual set of Key Vault operations has been performed compared with historical data. Key Vault activity is typically the same over time. This may be a legitimate change inactivity. Alternatively, your infrastructure might be compromised and further investigations are necessary. | - |
| User accessed high volume of Key Vaults | The number of vaults that a user or application accesses has changed compared with historical data. Key Vault activity is typically the same over time. This may be a legitimate change inactivity. Alternatively, your infrastructure might be compromised and further investigations are necessary. | - |
| | | |

Alerts for Azure DDoS Protection

Further details and notes

| ALERT | DESCRIPTION | INTENT (LEARN MORE) |
|--|--|---------------------|
| DDoS Attack detected for Public IP | DDoS Attack detected for Public IP (IP address) and being mitigated. | Probing |
| DDoS Attack mitigated for Public IP | DDoS Attack mitigated for Public IP (IP address). | Probing |
| | | |

Intentions

Understanding the intention of an attack can help you investigate and report the event more easily. Azure Security Center alerts include the 'intent' field to help with these efforts.

The series of steps that describe the progression of a cyberattack from reconnaissance to data exfiltration is often referred to as a "kill chain".

Security Center's supported kill chain intents are based on the [MITRE ATT&CK™ framework](#) and described in the table below.

| INTENT | DESCRIPTION | |
|---|--|--|
| PreAttack (replaces Probing) | <p>PreAttack could be either an attempt to access a certain resource regardless of a malicious intent, or a failed attempt to gain access to a target system to gather information prior to exploitation. This step is usually detected as an attempt, originating from outside the network, to scan the target system and identify an entry point.</p> <p>Further details on the PreAttack stage can be read in MITRE's page.</p> | |
| InitialAccess (replaces Exploitation) | <p>InitialAccess is the stage where an attacker manages to get a foothold on the attacked resource. This stage is relevant for compute hosts and resources such as user accounts, certificates etc. Threat actors will often be able to control the resource after this stage.</p> | |
| Persistence | <p>Persistence is any access, action, or configuration change to a system that gives a threat actor a persistent presence on that system. Threat actors will often need to maintain access to systems through interruptions such as system restarts, loss of credentials, or other failures that would require a remote access tool to restart or provide an alternate backdoor for them to regain access.</p> | |
| PrivilegeEscalation | <p>Privilege escalation is the result of actions that allow an adversary to obtain a higher level of permissions on a system or network. Certain tools or actions require a higher level of privilege to work and are likely necessary at many points throughout an operation. User accounts with permissions to access specific systems or perform specific functions necessary for adversaries to achieve their objective may also be considered an escalation of privilege.</p> | |
| DefenseEvasion | <p>Defense evasion consists of techniques an adversary may use to evade detection or avoid other defenses. Sometimes these actions are the same as (or variations of) techniques in other categories that have the added benefit of subverting a particular defense or mitigation.</p> | |

| INTENT | DESCRIPTION | |
|-------------------------|---|--|
| CredentialAccess | <p>Credential access represents techniques resulting in access to or control over system, domain, or service credentials that are used within an enterprise environment. Adversaries will likely attempt to obtain legitimate credentials from users or administrator accounts (local system administrator or domain users with administrator access) to use within the network. With sufficient access within a network, an adversary can create accounts for later use within the environment.</p> | |
| Discovery | <p>Discovery consists of techniques that allow the adversary to gain knowledge about the system and internal network. When adversaries gain access to a new system, they must orient themselves to what they now have control of and what benefits operating from that system give to their current objective or overall goals during the intrusion. The operating system provides many native tools that aid in this post-compromise information-gathering phase.</p> | |
| LateralMovement | <p>Lateral movement consists of techniques that enable an adversary to access and control remote systems on a network and could, but does not necessarily, include execution of tools on remote systems. The lateral movement techniques could allow an adversary to gather information from a system without needing additional tools, such as a remote access tool. An adversary can use lateral movement for many purposes, including remote Execution of tools, pivoting to additional systems, access to specific information or files, access to additional credentials, or to cause an effect.</p> | |
| Execution | <p>The execution tactic represents techniques that result in execution of adversary-controlled code on a local or remote system. This tactic is often used in conjunction with lateral movement to expand access to remote systems on a network.</p> | |
| Collection | <p>Collection consists of techniques used to identify and gather information, such as sensitive files, from a target network prior to exfiltration. This category also covers locations on a system or network where the adversary may look for information to exfiltrate.</p> | |

| INTENT | DESCRIPTION | |
|--------------------------|--|--|
| Exfiltration | Exfiltration refers to techniques and attributes that result or aid in the adversary removing files and information from a target network. This category also covers locations on a system or network where the adversary may look for information to exfiltrate. | |
| CommandAndControl | The command and control tactic represents how adversaries communicate with systems under their control within a target network. | |
| Impact | Impact events primarily try to directly reduce the availability or integrity of a system, service, or network; including manipulation of data to impact a business or operational process. This would often refer to techniques such as ransomware, defacement, data manipulation, and others. | |
| | | |

Next steps

To learn more about alerts, see the following:

- [Threat protection in Azure Security Center](#)
- [Security alerts in Azure Security Center](#)
- [Manage and respond to security alerts in Azure Security Center](#)
- [Export security alerts and recommendations \(Preview\)](#)

Manage and respond to security alerts in Azure Security Center

2/27/2020 • 2 minutes to read • [Edit Online](#)

This topic shows you how to view and process the alerts that you have received in order to protect your resources.

- To learn about the different types of alerts, see [Security alert types](#).
- For an overview of how Security Center generates alerts, see [How Azure Security Center detects and responds to threats](#).

NOTE

To enable advanced detections, upgrade to Azure Security Center Standard. A free trial is available. To upgrade, select Pricing Tier in the [Security Policy](#). See [Azure Security Center pricing](#) to learn more.

What are security alerts?

Security Center automatically collects, analyzes, and integrates log data from your Azure resources, the network, and connected partner solutions, like firewall and endpoint protection solutions, to detect real threats and reduce false positives. A list of prioritized security alerts is shown in Security Center along with the information you need to quickly investigate the problem and recommendations for how to remediate an attack.

NOTE

For more information about how Security Center detection capabilities work, see [How Azure Security Center detects and responds to threats](#).

Manage your security alerts

1. From the Security Center dashboard, see the **Threat protection** tile to view and overview of the alerts.

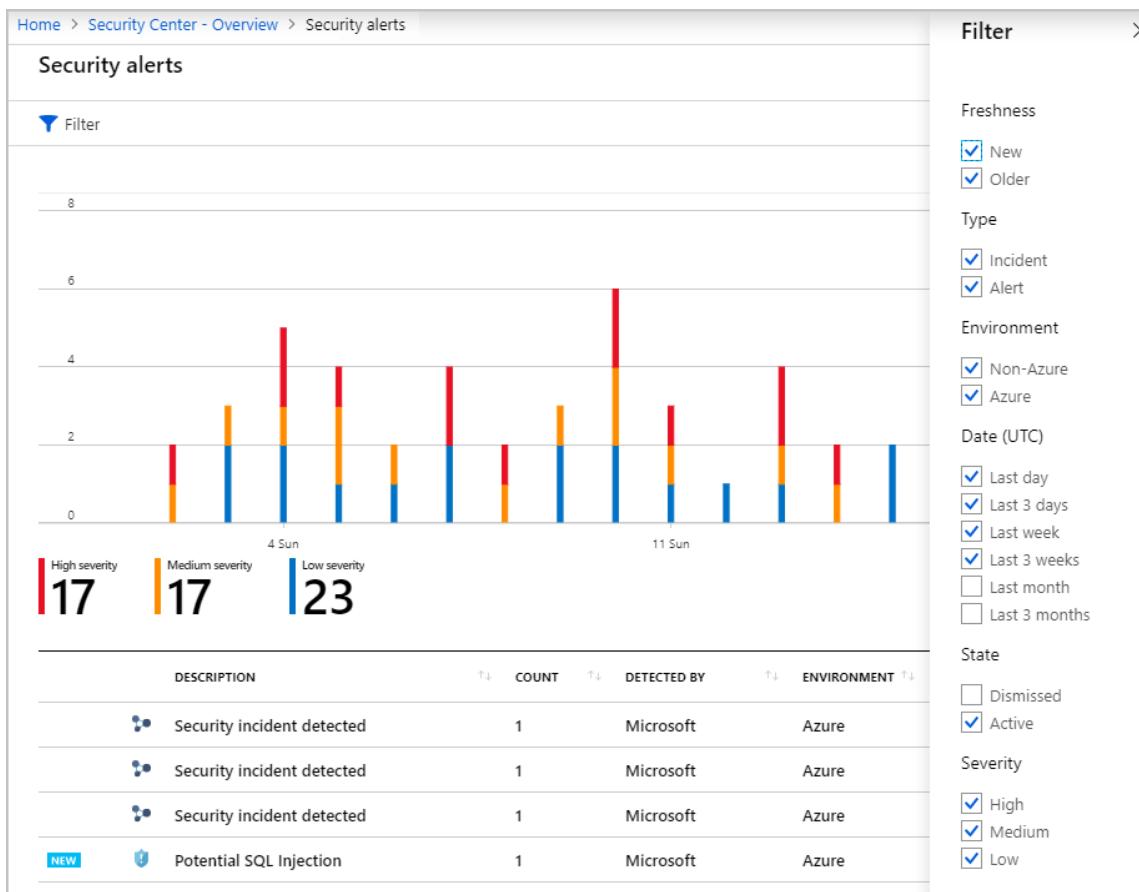
The screenshot shows the Azure Security Center Overview page. On the left, there's a navigation sidebar with sections like Overview, Policy & Compliance, Resource Security Hygiene, Advanced Cloud Defense, Threat Protection, and Automation & Orchestration. The main area has three main sections: Policy & compliance, Resource security hygiene, and Threat protection. The Threat protection section is highlighted with a red border. It contains a donut chart for security alerts by severity (High: 17, Medium: 17, Low: 23) and a bar chart for security alerts over time from 4 Sun to 18 Sun.

2. To see more details about the alerts, click the tile.

The screenshot shows the Security alerts page. At the top, it displays a summary of security alerts: 16 High severity, 17 Medium severity, and 23 Low severity. Below this is a chart showing the count of alerts per day from 4 Sun to 18 Sun. A detailed table follows, listing 10 specific security incidents with columns for Description, Count, Detected By, Environment, Date, State, and Severity.

| DESCRIPTION | COUNT | DETECTED BY | ENVIRONME... | DATE | STATE | SEVERITY |
|--|-------|-------------|--------------|----------|--------|----------|
| Security incident detected | 1 | Microsoft | Azure | 08/16/19 | Active | High |
| Security incident detected | 1 | Microsoft | Azure | 08/10/19 | Active | High |
| Security incident detected | 1 | Microsoft | Azure | 08/04/19 | Active | High |
| Potential SQL Injection | 1 | Microsoft | Azure | 08/20/19 | Active | High |
| Modified system binary discovered in du... | 1 | Microsoft | Azure | 08/17/19 | Active | High |
| Successful RDP brute force attack | 1 | Microsoft | Azure | 08/16/19 | Active | High |
| Potential SQL Injection | 1 | Microsoft | Azure | 08/14/19 | Active | High |
| Suspicious process executed | 1 | Microsoft | Azure | 08/13/19 | Active | High |
| Suspicious double extension file executed | 1 | Microsoft | Azure | 08/13/19 | Active | High |
| Modified system binary discovered in du... | 1 | Microsoft | Azure | 08/11/19 | Active | High |

3. To filter the alerts shown, click **Filter**, and from the **Filter** blade that opens, select the filter options that you want to apply. The list updates according to the selected filter. Filtering can be very helpful. For example, you might want to address security alerts that occurred in the last 24 hours because you are investigating a potential breach in the system.



Respond to security alerts

- From the **Security alerts** list, click a security alert. The resources involved and the steps you need to take to remediate an attack is shown.

Possible compromised machine detected

ATTACKED RESOURCE: vm4

COUNT: 1

ACTIVITY TIME: 08/11/19, 3:01 AM

ENVIRONMENT: Azure

STATE: Active

SEVERITY: Medium

- After reviewing the information, click a resource that was attacked.

General information

ATTACKED RESOURCE: vm4

ACTIVITY TIME: Sunday, August 11, 2019, 3:01:00 AM

SEVERITY: Medium

STATE: Active

ATTACKED RESOURCE: vm4

SUBSCRIPTION: ASC DEMO

DETECTED BY: Microsoft

ACTION TAKEN: Detected

ENVIRONMENT: Azure

RESOURCE TYPE: Virtual Machine

Remediation steps

REMEDIAL STEPS:

- Escalate the alert to the information security team.
- Make sure the machine is completely updated and has an updated Anti-Virus installed.
- Run a full anti-malware scan and verify that the threat was removed.
- Install and run Microsoft's Malicious Software Removal Tool (see <http://www.microsoft.com/security/pc-security/malware-removal.aspx>).
- Run Microsoft's Autoruns utility and try to identify unknown applications that are configured to run at login (see <https://technet.microsoft.com/en-us/sysinternals/bb963902.aspx>).
- Run Process Explorer and try to identify unknown running processes (see <https://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>).

The **General Information** section can offer an insight into what triggered the security alert. It displays information such as the target resource, source IP address (when applicable), if the alert is still active, and recommendations about how to remediate.

NOTE

In some instances, the source IP address is not available, some Windows security events logs do not include the IP address.

3. The remediation steps suggested by Security Center vary according to the security alert. Follow them for each alert.

In some cases, in order to mitigate a security alert, you may have to use other Azure controls or services to implement the recommended remediation.

The following topics guide you through the different alerts, according to resource types:

- [Alerts for IaaS Windows machines](#)
- [Alerts for IaaS Linux machines](#)
- [Alerts for Azure App Service](#)
- [Alerts for Azure containers](#)
- [Alerts for SQL Database and SQL Data Warehouse](#)
- [Alerts for Azure Storage](#)
- [Alerts for Cosmos DB](#)

The following topics explain how Security Center uses the different telemetry that it collects from integrating with the Azure infrastructure, in order to apply additional protection layers for resources deployed on Azure:

- [Alerts for Azure management layer \(Azure Resource Manager\) \(Preview\)](#)
- [Alerts for Azure Key Vault \(Preview\)](#)
- [Alerts for Azure network layer](#)
- [Alerts from other services](#)

See also

In this document, you learned how to configure security policies in Security Center. To learn more about Security Center, see the following:

- [Security alerts in Azure Security Center](#).
- [Handling security incidents](#)
- [Azure Security Center Planning and Operations Guide](#)

Manage security incidents in Azure Security Center

2/25/2020 • 2 minutes to read • [Edit Online](#)

Triage and investigating security alerts can be time consuming for even the most skilled security analysts, and for many it is hard to even know where to begin. By using [analytics](#) to connect the information between distinct [security alerts](#), Security Center can provide you with a single view of an attack campaign and all of the related alerts – you can quickly understand what actions the attacker took and what resources were impacted.

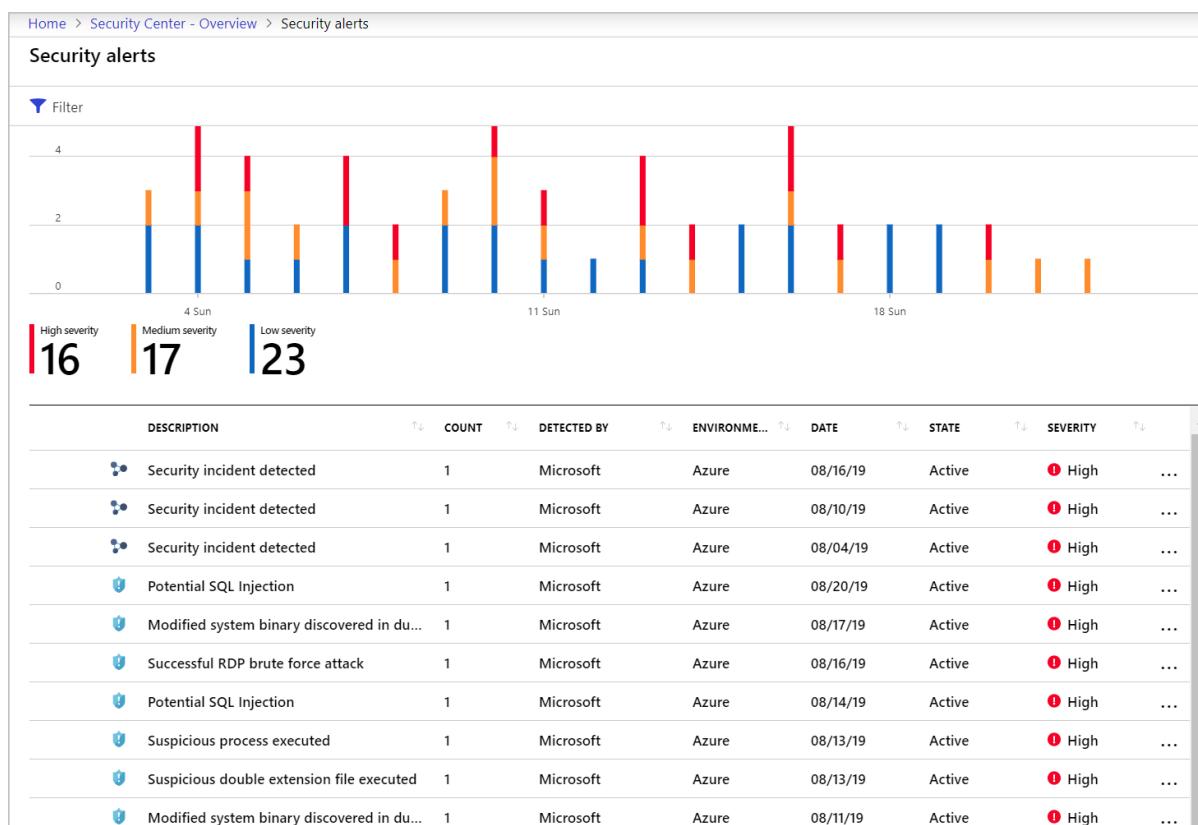
This topic explains about incidents in Security Center, and how to use remediate their alerts.

What is a security incident?

In Security Center, a security incident is an aggregation of all alerts for a resource that align with [kill chain](#) patterns. Incidents appear in the [Security Alerts](#) list. Click on an incident to view the related alerts, which enables you to obtain more information about each occurrence.

Managing security incidents

1. On the Security Center dashboard, click the **Security alerts** tile. The incidents and alerts are listed. Notice that the security incident description has a different icon compared to other alerts.



2. To view details, click on an incident. The **Security incident detected** blade displays further details. The **General Information** section can offer an insight into what triggered the security alert. It displays information such as the target resource, source IP address (when applicable), if the alert is still active, and recommendations about how to remediate.

Security incident detected

Incident Detected

The incident which started on 2019-08-09 01:01:00Z and most recently detected on 2019-08-10 10:01:00Z indicate that an attacker has attacked other resources from your virtual machine vm1

| | |
|-------------------|---|
| Description | |
| Activity time | Saturday, August 10, 2019, 1:01:00 PM |
| Severity | ! High |
| State | Active |
| Attacked Resource | vm1 |
| Subscription | ASC DEMO |
| Detected by |  Microsoft |
| Action Taken | Detected |
| Environment | Azure |
| Remediation Steps | <p>1. Escalate the alert to the information security team.</p> <p>2. Review the remediation steps of each one of the alerts</p> |

Alerts included in this incident

| DESCRIPTION | COUNT | ACTIVITY TIME | ATTACKED RESOURCE | SEVERITY |
|---|-------|--------------------|-------------------|--|
|  SQL injection blocked | 4 | 08/09/19, 04:01 AM | vm1 | ! Low |
|  Failed RDP Brute Force Attack | 4 | 08/09/19, 05:01 AM | vm1 | ! Low |
|  Successful RDP brute force attack | 4 | 08/10/19, 05:01 AM | vm1 | ! High |
|  Suspicious SVCHOST process executed | 4 | 08/10/19, 06:01 AM | vm1 | ! Low |
|  Multiple Domain Accounts Queried | 4 | 08/10/19, 07:01 AM | vm1 | ! Low |
|  Network communication with a malicious machine detected | 4 | 08/10/19, 08:01 AM | vm1 | ! Medium |

3. To obtain more information on each alert, click on an alert. The remediation suggested by Security Center vary according to the security alert.

NOTE

The same alert can exist as part of an incident, as well as to be visible as a standalone alert.

Home > Security Center - Overview > Security alerts > Security incident detected > Successful RDP brute force attack

Successful RDP brute force attack

vm1

[Learn more](#)

General information

| | |
|-------------------|---|
| DESCRIPTION | Several Remote Desktop login attempts were detected from FreeRDP (96.81.218.10), some of which were able to successfully login to the machine. Event logs analysis shows that in the last 30 minutes there were 60 failed attempts. 20 of the failed login attempts aimed at non-existent users. 1 of the failed login attempts aimed at existing users. |
| ACTIVITY TIME | Saturday, August 10, 2019, 5:01:00 AM |
| SEVERITY | ! High |
| STATE | Active |
| ATTACKED RESOURCE | vm1 |
| SUBSCRIPTION | ASC DEMO (212f9889-769e-45ae-ab43-6da33674bd26) |
| DETECTED BY | ■ Microsoft |
| ACTION TAKEN | Detected |
| ENVIRONMENT | Azure |
| RESOURCE TYPE | _VM_ Virtual Machine |
| SUCCESSFUL LOGINS | 1 |
| REPORTS | Report: RDP Brute Forcing |

Remediation steps

| | |
|----------------|---|
| REMEDIAL STEPS | 1. Escalate the alert to the information security team 2. If available, add the source IP to NSG block list for 24 hours (see https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-nsg/) 3. Enforce the use of strong passwords and do not re-use them across multiple VMs and services (see http://windows.microsoft.com/en-us/Windows7/Tips-for-creating-strong-passwords-and-passphrases) 4. Create an allow list for RDP access in NSG (see https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-nsg/) |
|----------------|---|

Was this useful? Yes No

4. Follow the remediation steps given for each alert.

For more information about alerts, [Managing and responding to security alerts](#).

The following topics guide you through the different alerts, according to resource types:

- [Alerts for IaaS Windows machines](#)
- [Alerts for IaaS Linux machines](#)
- [Alerts for Azure App Service](#)
- [Alerts for Azure containers](#)
- [Alerts for SQL Database and SQL Data Warehouse](#)
- [Alerts for Azure Storage](#)
- [Alerts for Cosmos DB](#)

The following topics explain how Security Center uses the different telemetry that it collects from integrating with the Azure infrastructure, in order to apply additional protection layers for resources deployed on Azure:

- [Alerts for Azure management layer \(Azure Resource Manager\) \(Preview\)](#)
- [Alerts for Azure Key Vault \(Preview\)](#)
- [Alerts for Azure network layer](#)
- [Alerts from other services](#)

See also

In this document, you learned how to use the security incident capability in Security Center. To learn more about Security Center, see the following:

- [Security alerts in Azure Security Center.](#)
- [Manage security alerts](#)
- [Azure Security Center Planning and Operations Guide](#)

Threat protection in Azure Security Center

2/27/2020 • 12 minutes to read • [Edit Online](#)

This page briefly describes the sources of the security alerts displayed by Azure Security Center for users on the standard pricing tier.

When Security Center detects a threat in any of the areas of your environment listed below, it generates an alert. These alerts describe details of the affected resources, suggested remediation steps, and in some cases an option to trigger a logic app in response.

Whether an alert is generated by Security Center, or received by Security Center from a different security product, you can export it. To export your alerts to Azure Sentinel (or a third-party SIEM) or any other external locations, follow the instructions in [Exporting alerts and recommendations](#).

Threat protection for Windows machines

Azure Security Center integrates with Azure services to monitor and protect your Windows-based machines. Security Center presents the alerts and remediation suggestions from all of these services in an easy-to-use format.

- **Microsoft Defender ATP** - Security Center extends its cloud workload protection platforms by integrating with Microsoft Defender Advanced Threat Protection (ATP). Together, they provide comprehensive endpoint detection and response (EDR) capabilities.

IMPORTANT

The Microsoft Defender ATP sensor is automatically enabled on Windows servers that use Security Center.

When Microsoft Defender ATP detects a threat, it triggers an alert. The alert is shown on the Security Center dashboard. From the dashboard, you can pivot to the Microsoft Defender ATP console, and perform a detailed investigation to uncover the scope of the attack. For more information about Microsoft Defender ATP, see [Onboard servers to the Microsoft Defender ATP service](#).

- **Crash dump analysis** - When software crashes, a crash dump captures a portion of memory at the time of the crash.

A crash might have been caused by malware or contain malware. To avoid being detected by security products, various forms of malware use a fileless attack, which avoids writing to disk or encrypting software components written to disk. This type of attack is difficult to detect by using traditional disk-based approaches.

However, by using memory analysis, you can detect this kind of attack. By analyzing the memory in the crash dump, Security Center can detect the techniques the attack is using. For example, the attack might be attempting to exploit vulnerabilities in the software, access confidential data, and surreptitiously persist within a compromised machine. Security Center does this work with minimal performance impact to hosts.

For details of the crash dump analysis alerts, see the [Reference table of alerts](#).

- **Fileless attack detection** - Fileless attacks targeting your endpoints are common. To avoid detection, fileless attacks inject malicious payloads into memory. Attacker payloads persist within the memory of compromised processes, and perform a wide range of malicious activities.

With fileless attack detection, automated memory forensic techniques identify fileless attack toolkits, techniques, and behaviors. This solution periodically scans your machine at runtime, and extracts insights directly from the memory of security-critical processes.

It finds evidence of exploitation, code injection, and execution of malicious payloads. Fileless attack detection generates detailed security alerts to accelerate alert triage, correlation, and downstream response time. This approach complements event-based EDR solutions, providing greater detection coverage.

For details of the fileless attack detection alerts, see the [Reference table of alerts](#).

TIP

You can simulate Windows alerts by downloading [Azure Security Center Playbook: Security Alerts](#).

Threat protection for Linux machines

Security Center collects audit records from Linux machines by using **auditd**, one of the most common Linux auditing frameworks. auditd lives in the mainline kernel.

- **Linux auditd alerts and Microsoft Monitoring Agent (MMA) integration** - The auditd system consists of a kernel-level subsystem, which is responsible for monitoring system calls. It filters them by a specified rule set, and writes messages for them to a socket. Security Center integrates functionalities from the auditd package within the Microsoft Monitoring Agent (MMA). This integration enables collection of auditd events in all supported Linux distributions, without any prerequisites.

auditd records are collected, enriched, and aggregated into events by using the Linux MMA agent. Security Center continuously adds new analytics that use Linux signals to detect malicious behaviors on cloud and on-premises Linux machines. Similar to Windows capabilities, these analytics span across suspicious processes, dubious sign in attempts, kernel module loading, and other activities. These activities can indicate a machine is either under attack or has been breached.

For a list of the Linux alerts, see the [Reference table of alerts](#).

TIP

You can simulate Linux alerts by downloading [Azure Security Center Playbook: Linux Detections](#).

Threat protection for Azure App Service

NOTE

This service is not currently available in Azure government and sovereign cloud regions.

Security Center uses the scale of the cloud to identify attacks targeting applications running over App Service. Attackers probe web applications to find and exploit weaknesses. Before being routed to specific environments, requests to applications running in Azure go through several gateways, where they're inspected and logged. This data is then used to identify exploits and attackers, and to learn new patterns that will be used later.

By using the visibility that Azure has as a cloud provider, Security Center analyzes App Service internal logs to identify attack methodology on multiple targets. For example, methodology includes widespread scanning and distributed attacks. This type of attack typically comes from a small subset of IPs, and shows patterns of crawling to similar endpoints on multiple hosts. The attacks are searching for a vulnerable page or plugin, and can't be identified from the standpoint of a single host.

If you're running a Windows-based App Service plan, Security Center also has access to the underlying sandboxes and VMs. Together with the log data mentioned above, the infrastructure can tell the story, from a new attack circulating in the wild to compromises in customer machines. Therefore, even if Security Center is deployed after a web app has been exploited, it may be able to detect ongoing attacks.

For a list of the Azure App Service alerts, see the [Reference table of alerts](#).

For more information on App Service plans, see [App Service plans](#).

Threat protection for Azure containers

NOTE

This service is not currently available in Azure government and sovereign cloud regions.

Security Center provides real-time threat protection for your containerized environments and generates alerts for suspicious activities. You can use this information to quickly remediate security issues and improve the security of your containers.

Security Center provides threat protection at different levels:

- **Host level** - Security Center's agent (available on the Standard tier, see [pricing](#) for details) monitors Linux for suspicious activities. The agent triggers alerts for suspicious activities originating from the node or a container running on it. Examples of such activities include web shell detection and connection with known suspicious IP addresses.

For a deeper insight into the security of your containerized environment, the agent monitors container-specific analytics. It will trigger alerts for events such as privileged container creation, suspicious access to API servers, and Secure Shell (SSH) servers running inside a Docker container.

IMPORTANT

If you choose not to install the agents on your hosts, you will only receive a subset of the threat protection benefits and security alerts. You'll still receive alerts related to network analysis and communications with malicious servers.

For a list of the host level alerts, see the [Reference table of alerts](#).

- At the **AKS cluster level**, the threat protection is based on analyzing Kubernetes' audit logs. To enable this **agentless** monitoring, add the Kubernetes option to your subscription from the **Pricing & settings** page (see [pricing](#)). To generate alerts at this level, Security Center monitors your AKS-managed services using the logs retrieved by AKS. Examples of events at this level include exposed Kubernetes dashboards, creation of high privileged roles, and the creation of sensitive mounts.

NOTE

Security Center generates security alerts for Azure Kubernetes Service actions and deployments occurring after the Kubernetes option is enabled on the subscription settings.

For a list of the AKS cluster level alerts, see the [Reference table of alerts](#).

Also, our global team of security researchers constantly monitor the threat landscape. They add container-specific alerts and vulnerabilities as they're discovered.

Threat protection for Azure network layer

Security Center network-layer analytics are based on sample [IPFIX data](#), which are packet headers collected by Azure core routers. Based on this data feed, Security Center uses machine learning models to identify and flag malicious traffic activities. Security Center also uses the Microsoft Threat Intelligence database to enrich IP addresses.

Some network configurations may restrict Security Center from generating alerts on suspicious network activity. For Security Center to generate network alerts, ensure that:

- Your virtual machine has a public IP address (or is on a load balancer with a public IP address).
- Your virtual machine's network egress traffic isn't blocked by an external IDS solution.
- Your virtual machine has been assigned the same IP address for the entire hour during which the suspicious communication occurred. This also applies to VMs created as part of a managed service (for example, AKS, Databricks).

For a list of the Azure network layer alerts, see the [Reference table of alerts](#).

For details of how Security Center can use network-related signals to apply threat protection, see [Heuristic DNS detections in Security Center](#).

Threat protection for Azure Key Vault (Preview)

NOTE

This service is not currently available in Azure government and sovereign cloud regions.

Azure Key Vault is a cloud service that safeguards encryption keys and secrets like certificates, connection strings, and passwords.

Azure Security Center includes Azure-native, advanced threat protection for Azure Key Vault, providing an additional layer of security intelligence. Security Center detects unusual and potentially harmful attempts to access or exploit Key Vault accounts. This layer of protection allows you to address threats without being a security expert, and without the need to manage third-party security monitoring systems.

When anomalous activities occur, Security Center shows alerts and optionally sends them via email to subscription administrators. These alerts include the details of the suspicious activity and recommendations on how to investigate and remediate threats.

For a list of the Azure Key Vault alerts, see the [Reference table of alerts](#).

Threat protection for SQL Database and SQL Data Warehouse

Advanced Threat Protection for Azure SQL Database detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit databases.

You'll see alerts when there are suspicious database activities, potential vulnerabilities, or SQL injection attacks, and anomalous database access and query patterns.

Advanced Threat Protection for Azure SQL Database and SQL is part of the [Advanced Data Security \(ADS\)](#) unified package for advanced SQL security capabilities, covering Azure SQL Databases, Azure SQL Database managed instances, Azure SQL Data Warehouse databases, and SQL servers on Azure Virtual Machines.

For more information, see:

- [How to enable Advanced Threat Protection for Azure SQL Database](#)
- [How to enable Advanced Threat Protection for SQL servers on Azure Virtual Machines](#)

- [The list of threat protection alerts for SQL Database and SQL Data Warehouse](#)

Threat protection for Azure Storage

NOTE

This service is not currently available in Azure government and sovereign cloud regions.

Advanced Threat Protection for Storage (currently available for Blob storage only) detects unusual and potentially harmful attempts to access or exploit storage accounts. This layer of protection allows you to address threats without requiring you to be a security expert, and helps you manage your security monitoring systems.

For more information, see:

- [How to enable Advanced Threat Protection for Azure Storage](#)
- [The list of threat protection alerts for Azure Storage](#)

Threat protection for Azure Cosmos DB

The Azure Cosmos DB alerts are generated by unusual and potentially harmful attempts to access or exploit Azure Cosmos DB accounts.

For more information, see:

- [Advanced Threat Protection for Azure Cosmos DB \(Preview\)](#)
- [The list of threat protection alerts for Azure Cosmos DB \(Preview\)](#)

Threat protection for Azure management layer (Azure Resource Manager) (Preview)

Security Center's protection layer based on Azure Resource Manager is currently in preview.

Security Center offers an additional layer of protection by using Azure Resource Manager events, which is considered to be the control plane for Azure. By analyzing the Azure Resource Manager records, Security Center detects unusual or potentially harmful operations in the Azure subscription environment.

For a list of the Azure Resource Manager (Preview) alerts, see the [Reference table of alerts](#).

NOTE

Several of the preceding analytics are powered by Microsoft Cloud App Security. To benefit from these analytics, you must activate a Cloud App Security license. If you have a Cloud App Security license, then these alerts are enabled by default. To disable the alerts:

1. In the **Security Center** blade, select **Security policy**. For the subscription you want to change, select **Edit settings**.
2. Select **Threat detection**.
3. Under **Enable integrations**, clear **Allow Microsoft Cloud App Security to access my data**, and select **Save**.

NOTE

Security Center stores security-related customer data in the same geo as its resource. If Microsoft hasn't yet deployed Security Center in the resource's geo, then it stores the data in the United States. When Cloud App Security is enabled, this information is stored in accordance with the geo location rules of Cloud App Security. For more information, see [Data storage for non-regional services](#).

Security alerts from other Microsoft services

Threat protection for Azure WAF

Azure Application Gateway offers a web application firewall (WAF) that provides centralized protection of your web applications from common exploits and vulnerabilities.

Web applications are increasingly targeted by malicious attacks that exploit commonly known vulnerabilities. The Application Gateway WAF is based on Core Rule Set 3.0 or 2.2.9 from the Open Web Application Security Project. The WAF is updated automatically to protect against new vulnerabilities.

If you have a license for Azure WAF, your WAF alerts are streamed to Security Center with no additional configuration needed. For more information on the alerts generated by WAF, see [Web application firewall CRS rule groups and rules](#).

Threat protection for Azure DDoS Protection

Distributed denial of service (DDoS) attacks are known to be easy to execute. They've become a great security concern, particularly if you're moving your applications to the cloud.

A DDoS attack attempts to exhaust an application's resources, making the application unavailable to legitimate users. DDoS attacks can target any endpoint that can be reached through the internet.

To defend against DDoS attacks, purchase a license for Azure DDoS Protection and ensure you're following application design best practices. DDoS Protection provides different service tiers. For more information, see [Azure DDoS Protection overview](#).

For a list of the Azure DDoS Protection alerts, see the [Reference table of alerts](#).

Next steps

To learn more about the security alerts from these threat protection features, see the following articles:

- [Reference table for all Azure Security Center alerts](#)
- [Security alerts in Azure Security Center](#)
- [Manage and respond to security alerts in Azure Security Center](#)
- [Export security alerts and recommendations \(Preview\)](#)

Cloud smart alert correlation in Azure Security Center (incidents)

11/6/2019 • 2 minutes to read • [Edit Online](#)

Azure Security Center continuously analyzes hybrid cloud workloads by using advanced analytics and threat intelligence to alert you about malicious activity.

The breadth of threat coverage is growing. The need to detect even the slightest compromise is important, and it can be challenging for security analysts to triage the different alerts and identify an actual attack. Security Center helps analysts cope with this alert fatigue. It helps diagnose attacks as they occur, by correlating different alerts and low fidelity signals into security incidents.

Fusion analytics is the technology and analytic back end that powers Security Center incidents, enabling it to correlate different alerts and contextual signals together. Fusion looks at the different signals reported on a subscription across the resources. Fusion finds patterns that reveal attack progression or signals with shared contextual information, indicating that you should use a unified response procedure for them.

Fusion analytics combines security domain knowledge with AI to analyze alerts, discovering new attack patterns as they occur.

Security Center leverages MITRE Attack Matrix to associate alerts with their perceived intent, helping formalize security domain knowledge. In addition, by using the information gathered for each step of an attack, Security Center can rule out activity that appears to be steps of an attack, but actually isn't.

Because attacks often occur across different tenants, Security Center can combine AI algorithms to analyze attack sequences that are reported on each subscription. This technique identifies the attack sequences as prevalent alert patterns, instead of just being incidentally associated with each other.

During an investigation of an incident, analysts often need extra context to reach a verdict about the nature of the threat and how to mitigate it. For example, even when a network anomaly is detected, without understanding what else is happening on the network or with regard to the targeted resource, it's difficult to understand what actions to take next. To help, a security incident can include artifacts, related events, and information. The additional information available for security incidents varies, depending on the type of threat detected and the configuration of your environment.

Security incident detected

Incident Detected



| | |
|-------------------|--|
| DESCRIPTION | The incident which started on 2017-05-21 01:01:00Z and most recently detected on 2017-05-22 10:01:00Z indicate that an attacker has attacked other resources from your virtual machine vm1 |
| DETECTION TIME | Monday, May 22, 2017, 1:01:00 PM |
| SEVERITY | ! High |
| STATE | Active |
| ATTACKED RESOURCE | vm1 |
| SUBSCRIPTION | ASC DEMO |
| DETECTED BY | Microsoft |
| ACTION TAKEN | Detected |
| ENVIRONMENT | Azure |
| REMEDIATION STEPS | <ol style="list-style-type: none">1. Escalate the alert to the information security team.2. Review the remediation steps of each one of the alerts |

Alerts included in this incident

| DESCRIPTION | COUNT | DETECTION TIME | ATTACKED RESOURCE | SEVERITY |
|--|-------|-------------------|-------------------|--|
| Failed RDP Brute Force Attack | 1 | 05/21/17, 5:01 AM | vm1 | ! Low |
| Successful RDP brute force attack | 1 | 05/22/17, 5:01 AM | vm1 | ! High |
| Suspicious SVCHOST process executed | 1 | 05/22/17, 6:01 AM | vm1 | ! Low |
| Multiple Domain Accounts Queried | 1 | 05/22/17, 7:01 AM | vm1 | ! Low |
| Network communication with a malicious machin... | 1 | 05/22/17, 8:01 AM | vm1 | ! Medium |

Notable events included in this incident

| DESCRIPTION | COUNT | DETECTION TIME | ATTACKED RESOURCE |
|--------------------------|-------|-------------------|-------------------|
| An event log was cleared | 1 | 05/21/17, 4:01 AM | vm1 |

To better understand security incidents, see [How to handle security incidents in Azure Security Center](#).

Security alerts map and threat intelligence

2/25/2020 • 2 minutes to read • [Edit Online](#)

This article helps you to use the Azure Security Center security alerts map and security event-based threat intelligence map to address security-related issues.

NOTE

The Security *events* map button has been retired on July 31st, 2019. For more information and alternative services, see [Retirement of Security Center features \(July 2019\)](#).

How the security alerts map works

Security Center provides you with a map that helps you identify security threats against the environment. For example, you can identify whether a particular computer is part of a botnet, and where the threat is coming from. Computers can become nodes in a botnet when attackers illicitly install malware that secretly interacts with command and control that manage the botnet.

To build this map, Security Center uses data that comes from multiple sources within Microsoft. Security Center uses this data to map potential threats against your environment.

One of the steps of a [security incident response process](#) is to identify the severity of the compromised system(s). In this phase, you should perform the following tasks:

- Determine the nature of the attack.
- Determine the point of origin of the attack.
- Determine the intent of the attack. Was the attack directed at your organization to acquire specific information, or was it random?
- Identify the systems that were compromised.
- Identify the files that were accessed and determine the sensitivity of those files.

You can use the Security alerts map in Security Center to help with these tasks.

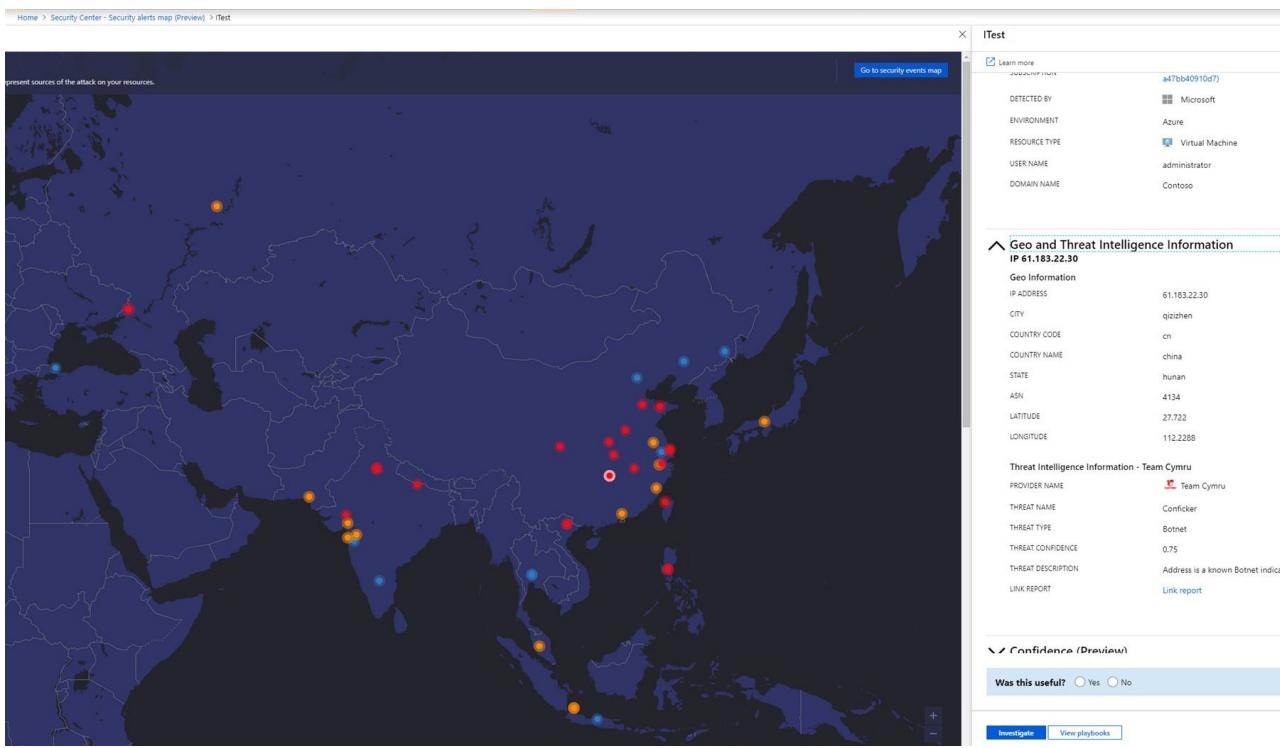
Access the Security alerts map

To visualize the current threats on your environment, open the Security alerts map:

1. Open the **Security Center** dashboard.
2. In the left pane, under **Threat Protection** select **Security alerts map**. The map opens.
3. To get more information about the alert and receive remediation steps, click on the Alert dot on the map and follow the instructions.

The security alerts map is based on alerts. These alerts are based on activities for which network communication was associated with an IP address that was successfully resolved, whether or not the IP address is a known risky IP address (for example, a known cryptominer) or an IP address that is not recognized previously as risky. The map provides alerts across any subscriptions you previously selected in Azure.

The alerts on the map are displayed according to the geographical location where they are detected as originating from, and they are color coded by severity.



See also

In this article, you learned how to use threat intelligence in Security Center to assist you in identifying suspicious activity. To learn more about Security Center, see the following articles:

- [Manage and respond to security alerts in Azure Security Center](#). Learn how to manage alerts and respond to security incidents in Security Center.
- [Security health monitoring in Azure Security Center](#). Learn how to monitor the health of your Azure resources.
- [Understand security alerts in Azure Security Center](#). Learn about the different types of security alerts.
- [Azure Security Center troubleshooting guide](#). Learn how to troubleshoot common issues in Security Center.

Alert validation (EICAR test file) in Azure Security Center

2/25/2020 • 2 minutes to read • [Edit Online](#)

This document helps you learn how to verify if your system is properly configured for Azure Security Center alerts.

What are security alerts?

Alerts are the notifications that Security Center generates when it detects threats on your resources. It prioritizes and lists the alerts along with the information needed to quickly investigate the problem. Security Center also provides recommendations for how you can remediate an attack. For more information, see [Security alerts in Security Center](#) and [Managing and responding to security alerts](#)

Alert validation

- [Windows](#)
- [Linux](#)
- [Kubernetes](#)

Validate alerts on Windows VMs

After Security Center agent is installed on your computer, follow these steps from the computer where you want to be the attacked resource of the alert:

1. Copy an executable (for example `calc.exe`) to the computer's desktop, or other directory of your convenience, and rename it as **ASC_AlertTest_662jfi039N.exe**.
2. Open the command prompt and execute this file with an argument (just a fake argument name), such as:
`ASC_AlertTest_662jfi039N.exe -foo`
3. Wait 5 to 10 minutes and open Security Center Alerts. An alert similar to the [example](#) below should be displayed:

NOTE

When reviewing this test alert for Windows, make sure the field **Arguments Auditing Enabled** is **true**. If it is **false**, then you need to enable command-line arguments auditing. To enable it, use the following command:

```
reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\policies\system\Audit" /f /v "ProcessCreationIncludeCmdLine_Enabled"
```

Validate alerts on Linux VMs

After Security Center agent is installed on your computer, follow these steps from the computer where you want to be the attacked resource of the alert:

1. Copy an executable to a convenient location and rename it to **./asc_alerttest_662jfi039n**, for example:

```
cp /bin/echo ./asc_alerttest_662jfi039n
```

2. Open the command prompt and execute this file:

```
./asc_alerttest_662jfi039n testing eicar pipe
```

3. Wait 5 to 10 minutes and open Security Center Alerts. An alert similar to the [example](#) below should be displayed:

Alert example



| | |
|-------------------------------|--|
| DESCRIPTION | This is a test alert generated by Azure Security Center. No further action is needed. |
| DETECTION TIME | Tuesday, September 5, 2017, 8:05:34 AM |
| SEVERITY | ! High |
| STATE | Active |
| ATTACKED RESOURCE | E2EINTVM2 |
| SUBSCRIPTION | [REDACTED] |
| DETECTED BY | ■ Microsoft |
| ACTION TAKEN | Detected |
| ENVIRONMENT | ■ Azure |
| RESOURCE TYPE | ■ Virtual Machine |
| ARGUMENTS AUDITING ENABLED | true |
| SUSPICIOUS PROCESS | [REDACTED]\appdata\local\temp\asc_alerttest_662jfi039n.exe |
| SUSPICIOUS COMMAND LINE | asc_alerttest_662jfi039n.exe -foo |
| USER NAME | [REDACTED] |
| PARENT PROCESS | unknown |
| COMPROMISED HOST | E2EINTVM2 |
| ACCOUNT SESSION ID | [REDACTED] |
| REMEDIATION STEPS | No further action is needed. |

Validate alerts on Kubernetes

If you're using the Security Center preview feature of integrating Azure Kubernetes Service, run the following kubectl command to test that your alerts are working:

```
kubectl get pods --namespace=asc-alerttest-662jfi039n
```

For more information about the integration of Azure Kubernetes Service and Azure Security Center, see [this article](#).

Next steps

This article introduced you to the alerts validation process. Now that you're familiar with this validation, try the following articles:

- [Managing and responding to security alerts in Azure Security Center](#) - Learn how to manage alerts, and respond to security incidents in Security Center.
- [Security health monitoring in Azure Security Center](#) - Learn how to monitor the health of your Azure resources.
- [Understanding security alerts in Azure Security Center](#) - Learn about the different types of security alerts.
- [Azure Security Center Troubleshooting Guide](#) - Learn how to troubleshoot common issues in Security Center.
- [Azure Security Blog](#) - Find blog posts about Azure security and compliance.

Onboarding to Azure Security Center Standard for enhanced security

2/27/2020 • 4 minutes to read • [Edit Online](#)

Upgrade to Security Center Standard to take advantage of enhanced security management and threat protection for your hybrid cloud workloads. You can try Standard free. See the Security Center [pricing page](#) for more information.

Security Center standard tier includes:

- **Hybrid security** – Get a unified view of security across all of your on-premises and cloud workloads. Apply security policies and continuously assess the security of your hybrid cloud workloads to ensure compliance with security standards. Collect, search, and analyze security data from a variety of sources, including firewalls and other partner solutions.
- **Security alerts** - Use advanced analytics and the Microsoft Intelligent Security Graph to get an edge over evolving cyber-attacks. Leverage built-in behavioral analytics and machine learning to identify attacks and zero-day exploits. Monitor networks, machines, and cloud services for incoming attacks and post-breach activity. Streamline investigation with interactive tools and contextual threat intelligence.
- **Access and application controls** - Block malware and other unwanted applications by applying whitelisting recommendations adapted to your specific workloads and powered by machine learning. Reduce the network attack surface with just-in-time, controlled access to management ports on Azure VMs, drastically reducing exposure to brute force and other network attacks.

Detecting unprotected resources

Security Center automatically detects any Azure subscriptions or workspaces not enabled for Security Center Standard. This includes Azure subscriptions using Security Center Free and workspaces that do not have the Security solution enabled.

You can upgrade an entire Azure subscription to the Standard tier, which is inherited by all supported resources within the subscription. Applying the Standard tier to a workspace applies to all resources reporting to the workspace.

NOTE

You may want to manage your costs and limit the amount of data collected for a solution by limiting it to a particular set of agents. [Solution targeting](#) allows you to apply a scope to the solution and target a subset of computers in the workspace. If you are using solution targeting, Security Center lists the workspace as not having a solution.

Upgrade an Azure subscription or workspace

To upgrade a subscription or workspace to standard:

1. Under the Security Center main menu, select **Getting started**.

2. Under **Upgrade**, Security Center lists subscriptions and workspaces eligible for onboarding.

- You can click on the expandable **Apply your trial** to see a list of all subscriptions and workspaces with their trial eligibility status.
- You can upgrade subscriptions and workspaces that are not eligible for trial.
- You can select eligible workspaces and subscriptions to start your trial.

3. Click **Start trial** to start your trial on the selected subscriptions.

NOTE

Security Center's Free capabilities are applied to your Azure VMs and VMSS only. The Free capabilities are not applied to your non-Azure computers. If you select Standard, the Standard capabilities are applied to all Azure VMs, VM scale sets, and non-Azure computers reporting to the workspace. We recommend that you apply Standard to provide advanced security for your Azure and non-Azure resources.

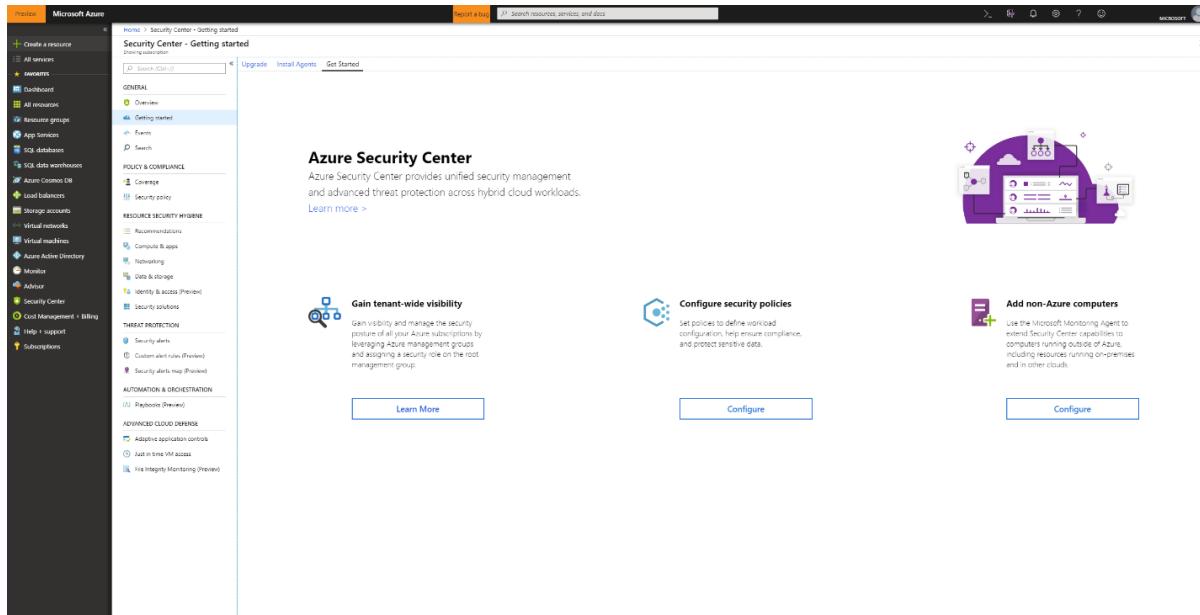
Onboard non-Azure computers

Security Center can monitor the security posture of your non-Azure computers but you need to first onboard these resources. You can add non-Azure computers from the **Getting started** blade or from the **Compute** blade. We'll walk through both methods.

Add new non-Azure computers from Getting started

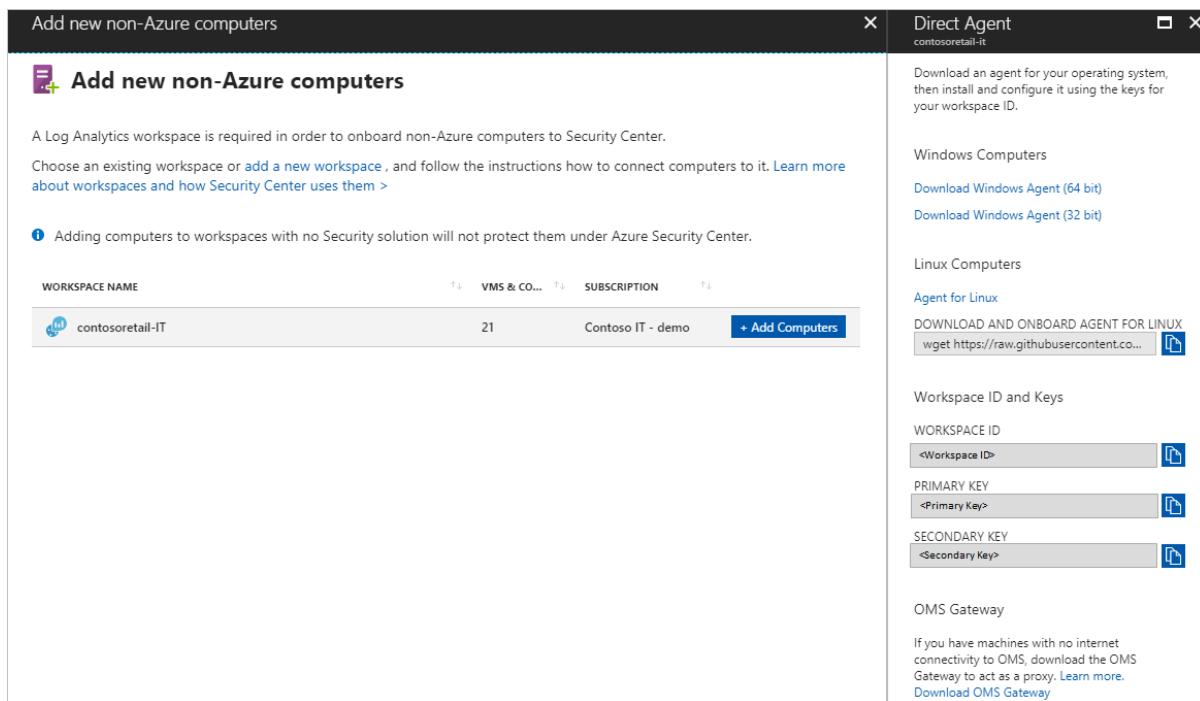
1. Return to **Getting started**.

2. Select the **Get started** tab.



3. Click **Configure** under **Add new non-Azure computers**. A list of your Log Analytics workspaces is shown.

The list includes, if applicable, the default workspace created for you by Security Center when automatic provisioning was enabled. Select this workspace or another workspace you want to use.



Add new non-Azure computers

Add new non-Azure computers

A Log Analytics workspace is required in order to onboard non-Azure computers to Security Center. Choose an existing workspace or [add a new workspace](#), and follow the instructions how to connect computers to it. [Learn more about workspaces and how Security Center uses them >](#)

Adding computers to workspaces with no Security solution will not protect them under Azure Security Center.

| WORKSPACE NAME | VMS & CO... | SUBSCRIPTION | + Add Computers |
|------------------|-------------|-------------------|-----------------|
| contosoretail-IT | 21 | Contoso IT - demo | + Add Computers |

Direct Agent

contosoretail-it

Download an agent for your operating system, then install and configure it using the keys for your workspace ID.

Windows Computers

[Download Windows Agent \(64 bit\)](#)

[Download Windows Agent \(32 bit\)](#)

Linux Computers

[Agent for Linux](#)

[DOWNLOAD AND ONBOARD AGENT FOR LINUX](#)

`wget https://raw.githubusercontent.com/Microsoft/omsagent/v1.1.1/agent/debian_64bit/omsagent_1.1.1-1_amd64.deb`

Workspace ID and Keys

WORKSPACE ID
`<Workspace ID>`

PRIMARY KEY
`<Primary Key>`

SECONDARY KEY
`<Secondary Key>`

OMS Gateway

If you have machines with no internet connectivity to OMS, download the OMS Gateway to act as a proxy. [Learn more](#).

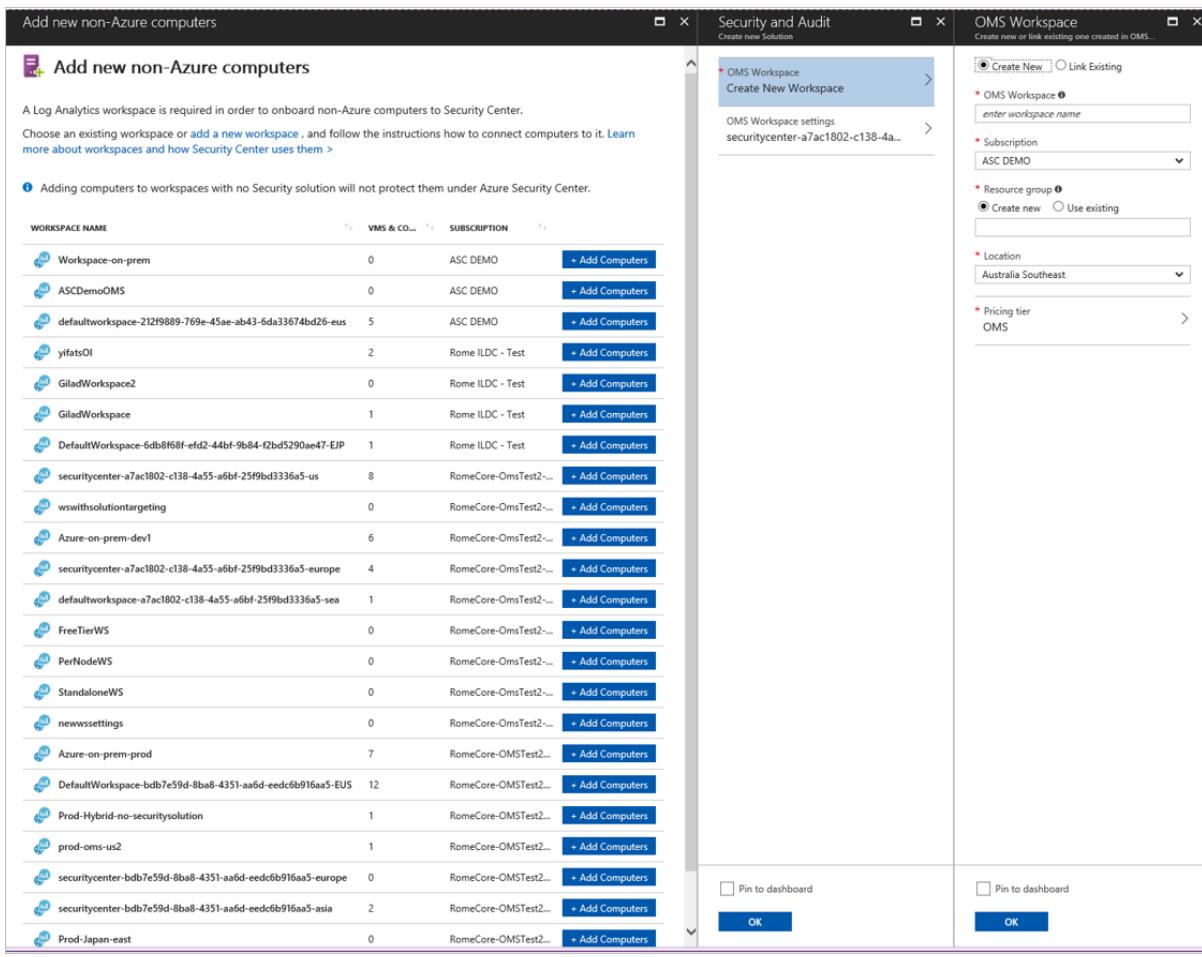
[Download OMS Gateway](#)

If you have existing workspaces, they are listed under **Add new Non-Azure computers**. You can add computers to an existing workspace or create a new workspace. To create a new workspace, select the link **add a new workspace**.

Add new non-Azure computers from Compute

Create a new workspace and add computer

1. Under **Add new non-Azure computers**, select **add a new workspace**.



- Under **Security and Audit**, select **OMS Workspace** to create a new workspace.

NOTE

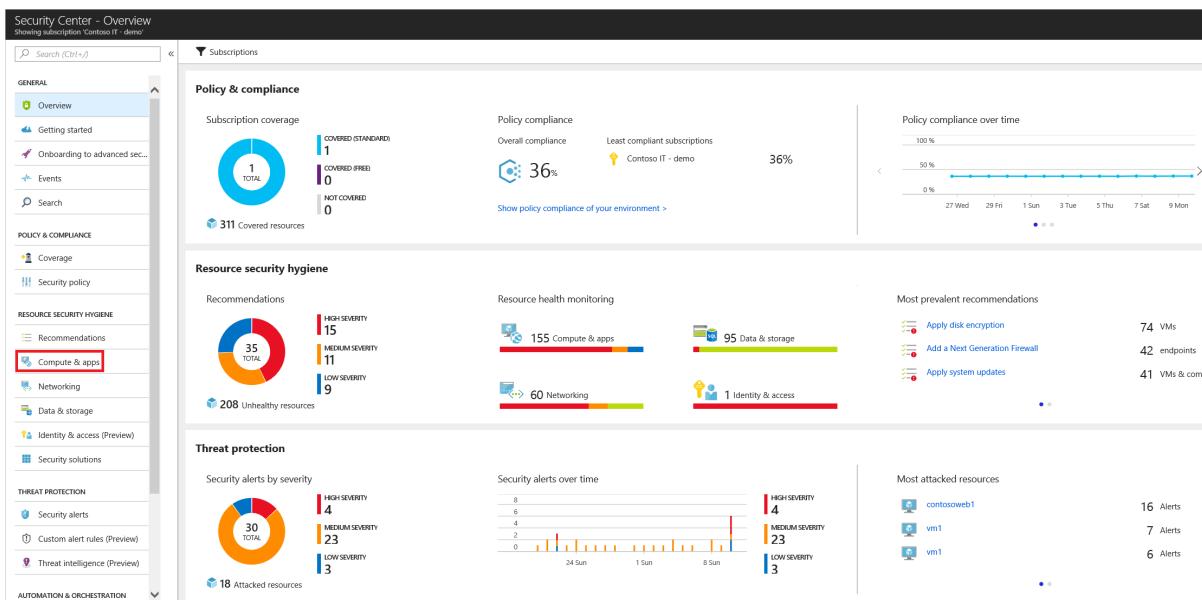
OMS workspaces are now referred to as Log Analytics workspaces.

- Under **OMS Workspace**, enter the information for your workspace.
- Under **OMS Workspace**, select **OK**. After you select OK, you will get a link for downloading a Windows or Linux agent and keys for your workspace ID to use in configuring the agent.
- Under **Security and Audit**, select **OK**.

Select an existing workspace and add computer

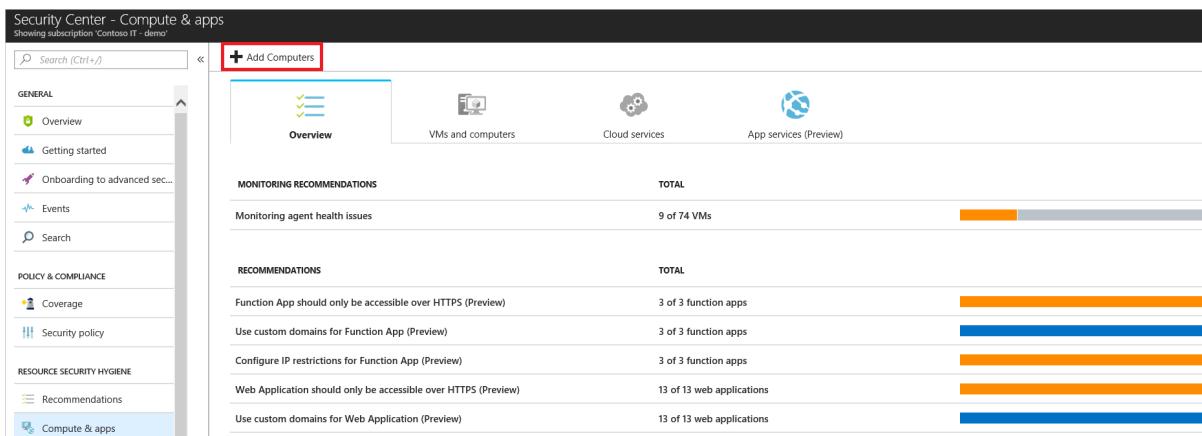
You can add a computer by following the workflow from **Onboarding**, as shown above. You can also add a computer by following the workflow from **Compute**. In this example, we use **Compute**.

- Return to Security Center's main menu and **Overview** dashboard.



2. Select **Compute & apps**.

3. Under **Compute & apps**, select **Add computers**.



4. Under **Add new non-Azure computers**, select a workspace to connect your computer to and click **Add Computers**.

Add new non-Azure computers

Add new non-Azure computers

A Log Analytics workspace is required in order to onboard non-Azure computers to Security Center. Choose an existing workspace or [add a new workspace](#), and follow the instructions how to connect computers to it. [Learn more about workspaces and how Security Center uses them](#) >

Adding computers to workspaces with no Security solution will not protect them under Azure Security Center.

| WORKSPACE NAME | VMS & CO... | SUBSCRIPTION | + Add Computers |
|------------------|-------------|-------------------|-----------------|
| contosoretail-IT | 21 | Contoso IT - demo | + Add Computers |

Direct Agent
contosoretail-it

Download an agent for your operating system, then install and configure it using the keys for your workspace ID.

Windows Computers

[Download Windows Agent \(64 bit\)](#)
[Download Windows Agent \(32 bit\)](#)

Linux Computers

[Agent for Linux](#)

[DOWNLOAD AND ONBOARD AGENT FOR LINUX](#)
`wget https://raw.githubusercontent.com/` [\[Download\]](#)

Workspace ID and Keys

WORKSPACE ID: `<Workspace ID>` [\[Copy\]](#)

PRIMARY KEY: `<Primary Key>` [\[Copy\]](#)

SECONDARY KEY: `<Secondary Key>` [\[Copy\]](#)

OMS Gateway

If you have machines with no internet connectivity to OMS, download the OMS Gateway to act as a proxy. [Learn more](#). [Download OMS Gateway](#)

The **Direct Agent** blade provides a link for downloading a Windows or Linux agent as well as the

workspace ID and keys to use in configuring the agent.

Next steps

In this article you learned how to onboard Azure and non-Azure resources in order to benefit from Security Center's advanced security. To do more with your onboarded resources, see

- [Enable data collection](#)
- [Threat intelligence report](#)
- [Just-in-time VM access](#)

Vulnerability assessments for your Azure Virtual Machines

2/4/2020 • 2 minutes to read • [Edit Online](#)

A core component of every cyber risk and security program is the identification and analysis of vulnerabilities. Azure Security Center's Standard pricing tier includes vulnerability scanning for your virtual machines at no extra cost. Additionally, Security Center can automatically deploy this tool for you. This feature is currently in preview.

Security Center presents one of two recommendations if it doesn't find a vulnerability assessment solution installed on a VM:

- **For standard tier users,** a recommendation offers to install an Azure Security Center Vulnerability Assessment extension (powered by Qualys) for you at no additional cost. This extension reports its findings directly back to Security Center. To learn more, see [Integrated vulnerability scanner for virtual machines](#).
- **For users on the free tier,** Security Center recommends that you install a partner solution. You'll need to purchase a license for your chosen solution separately. Supported solutions report vulnerability data to the partner's management platform. In turn, that platform provides vulnerability and health monitoring data back to Security Center. You can identify vulnerable VMs on the Security Center dashboard. Switch to the partner management console directly from Security Center for additional reports and information. To learn more, see [Deploying a partner vulnerability scanning solution](#).

Security Center also offers vulnerability analysis for your:

- SQL databases - see [Explore vulnerability assessment reports in the vulnerability assessment dashboard](#)
- Azure Container Registry images - see [Azure Container Registry integration with Security Center \(Preview\)](#)

Integrated vulnerability scanner for virtual machines (Standard tier only)

2/27/2020 • 5 minutes to read • [Edit Online](#)

The vulnerability scanner included with Azure Security Center is powered by Qualys and widely recognized as the leading tool for identifying vulnerabilities in real time across your Azure Virtual Machines. It's only available to users on the standard pricing tier. This feature is currently in preview.

NOTE

Security Center supports the integration of tools from other vendors, but you'll need to handle the licensing costs, deployment, and configuration. For more information, see [Deploying a partner vulnerability scanning solution](#).

Deploying the Qualys built-in vulnerability scanner (Standard tier only)

The simplest way to scan your Azure-based virtual machines for vulnerabilities is to use the built-in vulnerability scanner.

To deploy the vulnerability scanner extension:

1. Open Azure Security Center and go to the **Recommendations** page.
2. Select the recommendation named "Enable the built-in vulnerability assessment solution on virtual machines (powered by Qualys)".

The screenshot shows the Azure Security Center - Recommendations page. On the left, there's a navigation sidebar with links like Overview, Getting started, Pricing & settings, Community, Workflow automation, Policy & Compliance (Coverage, Secure score, Security policy, Regulatory compliance), Resource Security Hygiene (Recommendations, Compute & apps, Networking, IoT Hubs & resources). The main area has a search bar at the top. Below it, there's a dashboard with a pie chart showing 98 total recommendations (98 TOTAL), a bar chart for Resource health by severity (High Severity: 75, Medium Severity: 8, Low Severity: 15), and a section for Networking (62 Unhealthy resources, 232 Monitored resources). A note says "There are 10 high severity recommendations to resolve." At the bottom, there's a table for the "Remediate vulnerabilities found on your virtual machines (powered by Qualys) (Preview)" recommendation, which includes a "Quick Fix" button. Other recommendations listed are "Enable the built-in vulnerability assessment solution on virtual machines (powered by Qualys) (Preview)" and "Vulnerabilities in Azure Container Registry images should be remediated (powered by Qualys) (Preview)".

Your VMs will appear in one or more of the following groups:

- **Healthy resources** – the vulnerability scanner extension has been deployed to these VMs.
- **Unhealthy resources** – the vulnerability scanner extension can be deployed to these VMs.
- **Not applicable resources** – these VMs can't have the vulnerability scanner extension deployed.
Your VM might be in this tab because it's on the free pricing tier, it's missing the ImageReference class (relevant to custom images and VMs restored from backup, as explained in the Azure for .NET documentation) (<https://docs.microsoft.com/dotnet/api/microsoft.azure.batch.imagereference?>)

[view=azure-dotnet](#)), or it's not running one of the supported OSes:

- All versions of Windows
- Red Hat Enterprise Linux 6.7, 7.6
- Ubuntu 14.04, 18.04
- CentOS 6.10, 7, 7.6
- Oracle Linux 6.8, 7.6
- SUSE Enterprise Linux 12, 15
- Debian 7, 8

3. From the Unhealthy resources tab, select the VMs on which you want to deploy the Qualys scanner and click **Remediate**.

The screenshot shows the 'Affected resources' section of the Azure Security Center interface. The 'Unhealthy resources (2)' tab is selected, showing two virtual machines: 'ContosoAS' and 'ContosoAz'. Both machines have a blue checkmark next to them, indicating they are selected. Below the list are two buttons: 'Remediate' and 'Trigger Logic App (Preview)'. The 'Remediate' button is highlighted with a blue background.

The scanner extension will be installed on all of the selected VMs.

Scanning begins automatically as soon as the extension is successfully deployed.

Viewing and remediating discovered vulnerabilities

When Security Center identifies vulnerabilities, it presents findings and related information (remediation steps, related CVEs, CVSS scores, and more) as recommendations. You can view the identified vulnerabilities for one or more subscriptions, or for a specific virtual machine.

To see the findings and remediate the identified vulnerability:

1. Open Azure Security Center and go to the **Recommendations** page.
2. Select the recommendation named "Remediate vulnerabilities found on your virtual machines (powered by Qualys)".

Security Center shows you all the findings for all VMs in the currently selected subscriptions. The findings are ordered by severity.

Microsoft Azure

Search resources, services, and docs (G+/-)

Dashboard > Security Center - Recommendations > Remediate vulnerabilities found on your virtual machines (powered by Qualys) (Preview)

Remediate vulnerabilities found on your virtual machines (powered by Qualys) (Preview)

Description

Monitors for vulnerabilities on your virtual machines as discovered by Azure Security Center's built-in vulnerability assessment solution (powered by Qualys).

General Information

| | |
|-----------------------|------|
| Recommendation score | 0/30 |
| Recommendation impact | +30 |
| User impact | Low |
| Implementation effort | Low |

Threats

Remediation steps

Affected resources

Security Checks

Findings

Search to filter items...

| ID | Security Check | Category | Applies To | Severity |
|--------|--|-------------------|------------------|----------|
| 100369 | Microsoft Edge and Internet Explorer same-origin policy bypass vulnerability (Zero Day) | Internet Explorer | 4 of 8 resources | Medium |
| 91426 | Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltdown) | Windows | 3 of 8 resources | Medium |
| 91537 | Microsoft Windows Server Registry Key Configuration Missing (ADV190013) | Windows | 3 of 8 resources | Medium |
| 100319 | Microsoft Internet Explorer Security Update for September 2017 | Internet Explorer | 3 of 8 resources | Medium |
| 91462 | Microsoft Windows Security Update Registry Key Configuration Missing (ADV180002) | Windows | 3 of 8 resources | Medium |
| 90126 | Pending Reboot Detected | Windows | 2 of 8 resources | Medium |
| 100269 | Microsoft Internet Explorer Cumulative Security Update (MS15-124) | Internet Explorer | 2 of 8 resources | Medium |
| 100390 | Microsoft Internet Explorer Security Update for November 2019 | Internet Explorer | 1 of 8 resources | Medium |
| 91481 | Microsoft Windows Security Update November 2018 | Windows | 1 of 8 resources | Medium |
| 100350 | Microsoft Internet Explorer Memory Corruption Remote Code Execution Vulnerability (Zero Day) | Internet Explorer | 1 of 8 resources | Medium |

1 | 25 | < | > | ▲ | ▼

- To filter the findings by a specific VM, open the "Affected resources" section and click the VM that interests you. Alternatively, select a VM from the resource health view, and view all relevant recommendations for that resource.

Security Center shows the findings for that VM, ordered by severity.

ContosoWeb2

Resource: ContosoWeb2 Total vulnerabilities: **94**

Vulnerabilities by severity:

- High: 0
- Medium: 5
- Low: 89

| ID | Security Check | Category | Severity |
|--------|---|-----------------------|-----------|
| 91537 | Microsoft Windows Server Registry Key Configuration Missing (ADV190013) | Windows | ⚠️ Medium |
| 91462 | Microsoft Windows Security Update Registry Key Configuration Missing (ADV180012) (... | Windows | ⚠️ Medium |
| 100369 | Microsoft Edge and Internet Explorer same-origin policy bypass vulnerability (Zero Day) | Internet Explorer | ⚠️ Medium |
| 91426 | Microsoft Windows Security Update for Windows Server (ADV180002) (Spectre/Meltd...) | Windows | ⚠️ Medium |
| 100319 | Microsoft Internet Explorer Security Update for September 2017 | Internet Explorer | ⚠️ Medium |
| 45038 | Host Scan Time | Information gathering | ⓘ Low |
| 90295 | Windows Internet Explorer Version | Windows | ⓘ Low |
| 45063 | NTFS Settings Enumerated | Information gathering | ⓘ Low |
| 90107 | Windows Product Type | Windows | ⓘ Low |
| 105237 | SAMR Pipe Permissions Enumerated | Security Policy | ⓘ Low |

In this example, you can see that 94 vulnerabilities were discovered and that 5 of them are medium severity.

4. To learn more about a specific vulnerability, select it.

91426-Microsoft Windows Security Update for Windows Server...

Description
Monitors for vulnerabilities on your virtual machines as discovered by Azure Secur

General Information

- Recommendation score: 0/30
- Recommendation Impact: +30
- User Impact: Low
- Implementation effort: Low

Threats

Remediation steps

Affected resources

Security Checks

| ID | Security Check | Category |
|--------|--|-------------------|
| 100369 | Microsoft Edge and Internet Explor... | Internet Explorer |
| 91537 | Microsoft Windows Server Registry ... | Windows |
| 100319 | Microsoft Internet Explorer Security ... | Internet Explorer |
| 91462 | Microsoft Windows Security Update... | Windows |
| 91426 | Microsoft Windows Security Update... | Windows |
| 90126 | Pending Reboot Detected | Windows |
| 100269 | Microsoft Internet Explorer Cumulat... | Internet Explorer |
| 236971 | Red Hat Update for kernel (RHSA-2... | RedHat |

General information

- ID: 91426
- Severity: ⚠️ Medium
- Category: Windows
- Published Time: N/A
- Time Generated: 12/3/2019, 2:56 PM GMT+2
- Patchable: Yes
- CVSS base score: v2.0: 4.7
v3.0: 5.6
- CVEs:
 - CVE-2017-5753
 - CVE-2017-5715
 - CVE-2017-5754

Threat

Remediation

Additional References

Affected resources

| Name | Subscription |
|-------------|-------------------|
| vm4 | ASC DEMO |
| vm2 | ASC DEMO |
| ContosoWeb2 | Contoso IT - demo |

The details pane that appears contains extensive information about the vulnerability, including:

- Links to all relevant CVEs (where available)
- Remediation steps

- Any additional reference pages
5. To remediate a finding, follow the remediation steps from this details pane.

Built-in Qualys vulnerability scanner FAQ

Are there any additional charges for the Qualys license?

No. The built-in scanner is free to all Standard tier users. The "Enable the built-in vulnerability assessment solution on virtual machines (powered by Qualys)" recommendation deploys a scanner that includes all the necessary licensing and configuration information. No additional licenses are required.

What permissions are required to install the Qualys extension?

The Azure Security Center Vulnerability Assessment extension (powered by Qualys), like other extensions, runs on top of the Azure Virtual Machine agent. So it runs as Local Host on Windows, and Root on Linux.

Can I remove the Security Center Qualys extension?

If you want to remove the extensions from a VM, you can do it manually or with any of your programmatic tools.

You'll need the following details:

- On Linux, the extension is called "LinuxAgent.AzureSecurityCenter" and provider name is "Qualys"
- On Windows, the extension is called "WindowsAgent.AzureSecurityCenter" and provider name is "Qualys"

How does the extension get updated?

Like the Azure Security Center agent as well as all Azure extensions, minor versions of the Qualys scanner may be automatically updated in the background. All agents and extensions are tested extensively before being automatically deployed.

Some updates to the vulnerability scanner extension may require manual deployment. For example, **if you are running v1.0.0.4, you must take the following steps:**

1. Verify the version of the Qualys vulnerability scanner extension running on your VM:

- a. From the Azure portal, open Virtual machines.
- b. Select the VM on which the agent is installed.
- c. From the sidebar navigation, open **Extensions** and select the following extension:

Name: **WindowsAgent.AzureSecurityCenter** Type:
Qualys.WindowsAgent.AzureSecurityCenter

- d. Review the version information of the extension.

| | |
|----------------------|---|
| Type | Qualys.WindowsAgent.AzureSecurityCenter |
| Status | Provisioning succeeded |
| Version | 1.0.0.5 |
| Status level | Info |
| Status message | (none) |
| Detailed status | View detailed status |
| Handler status | Ready |
| Handler status level | Info |
| Resource ID | /subscriptions/d07c00.../WindowsAgent.AzureSecurityCenter |

- e. If the version is 1.0.0.4, click **Uninstall** and wait until the extension is no longer listed in the Extensions page of the VM.
- f. Restart the VM.
- g. When the VM's status is "Running", deploy the extension as described above in [Deploying the Qualys built-in vulnerability scanner](#).

Why does my VM show as "not applicable" in the recommendation?

When you open the recommendation, you'll see your VMs in one or more of the following groups:

- **Healthy resources** – the vulnerability scanner extension has been deployed to these VMs.
- **Unhealthy resources** – the vulnerability scanner extension can be deployed to these VMs.
- **Not applicable resources** – These VMs can't have the vulnerability scanner extension deployed. Your VM might be in this tab because it's on the free pricing tier, it's missing the ImageReference class (relevant to custom images and VMs restored from backup, as explained in the Azure for .NET documentation] (<https://docs.microsoft.com/dotnet/api/microsoft.azure.batch.imagereference?view=azure-dotnet>), or it's not running one of the supported OSes:
 - All versions of Windows
 - Red Hat Enterprise Linux 6.7, 7.6
 - Ubuntu 14.04, 18.04
 - CentOS 6.10, 7, 7.6
 - Oracle Linux 6.8, 7.6
 - SUSE Enterprise Linux 12, 15
 - Debian 7, 8

What is scanned by the built-in vulnerability scanner?

The scanner is running on your virtual machine and looking for vulnerabilities of the VM itself. From the virtual machine, it cannot scan your network.

Does the scanner integrate with my existing Qualys console?

The Security Center extension is a separate tool from your existing Qualys scanner and, because of licensing restrictions, can only be used within Azure Security Center.

Microsoft Defender Advanced Threat Protection also includes Threat & Vulnerability Management (TVM). How is the Security Center Vulnerability Assessment extension different?

Microsoft is actively developing world-class vulnerability management with Microsoft Defender ATP's Threat &

Vulnerability Management solution, built into Windows.

Today, Azure Security Center's Vulnerability Assessment extension is powered by Qualys. This ensures support for both Windows and Linux virtual machines. The extension also benefits from Qualys's own knowledge of vulnerabilities that don't yet have CVEs.

Next steps

This article described the Azure Security Center Vulnerability Assessment extension (powered by Qualys) for scanning your VMs. For related material, see the following articles:

- [Learn about the different elements of a recommendation](#)
- [Learn how to remediate recommendations](#)

Deploying a partner vulnerability scanning solution (Free tier users only)

12/30/2019 • 2 minutes to read • [Edit Online](#)

Customers on the Free tier can choose to deploy vulnerability assessment solutions from [Qualys](#) and [Rapid7](#). You can install the solution on multiple VMs. The VMs must belong to the same subscription.

Configuring a partner solution

1. On the **Security Center** dashboard, in the **Overview** section, click **Recommendations**.
2. On the **Recommendations** page, select **Vulnerability assessment solution should be installed on your virtual machines**.

| Recommendations | | | | | |
|--|------------------|-------|----------|------------------------------------|--|
| <input type="button" value="Filter"/> <input type="button" value="Install"/> | | | | | |
| DESCRIPTION | RESOURCE | STATE | SEVERITY | | |
| Enable VM Agent | 2 virtual mac... | Open | ⓘ High | <input type="button" value="..."/> | |
| Install Endpoint Protection | 4 virtual ma... | Open | ⓘ High | <input type="button" value="..."/> | |
| Add a web application firewall | 2 web applic... | Open | ⓘ High | <input type="button" value="..."/> | |
| Add a Next Generation Firewall | Marketing-A... | Open | ⓘ High | <input type="button" value="..."/> | |
| Route traffic through NGFW only | vm3 | Open | ⓘ High | <input type="button" value="..."/> | |
| Enable Auditing & Threat detection on... | sqlserver1as... | Open | ⓘ High | <input type="button" value="..."/> | |
| Remediate vulnerabilities (by Qualys) | 2 virtual mac... | Open | ⓘ High | <input type="button" value="..."/> | |
| Enable Auditing & Threat detection on... | 2 SQL datab... | Open | ⓘ High | <input type="button" value="..."/> | |
| Apply a Just-In-Time network access co... | CheckPoint-... | Open | ⓘ High | <input type="button" value="..."/> | |
| Apply disk encryption | 6 virtual mac... | Open | ⓘ High | <input type="button" value="..."/> | |
| Enable encryption for Azure Storage Ac... | 17 storage a... | Open | ⓘ High | <input type="button" value="..."/> | |
| Restrict access through Internet facing... | vm2 | Open | ⚠ Medium | <input type="button" value="..."/> | |
| Add a vulnerability assessment solution | 3 virtual mac... | Open | ⚠ Medium | <input type="button" value="..."/> | |
| Enable Transparent Data Encryption | 4 SQL datab... | Open | ⚠ Medium | <input type="button" value="..."/> | |
| Reboot after system updates | 3 virtual mac... | Open | ⚠ Medium | <input type="button" value="..."/> | |
| Remediate OS vulnerabilities (by Micros... | 2 virtual mac... | Open | ⓘ Low | <input type="button" value="..."/> | |

3. On the **Vulnerability assessment solution should be installed on your virtual machines** page, select the VMs where you want to install the vulnerability assessment solution.

| Add a vulnerability assessment solution | | | | | |
|---|-------------------|-------|----------|------------------------------------|--|
| <input type="button" value="Filter"/> <input type="button" value="Install on 3 VMs"/> | | | | | |
| VIRTUAL MACHINE | SUBSCRIPTION NAME | STATE | SEVERITY | | |
| <input checked="" type="checkbox"/> vm2 | ASC DEMO | Open | ⚠ Medium | <input type="button" value="..."/> | |
| <input checked="" type="checkbox"/> vm2WL | ASC DEMO | Open | ⚠ Medium | <input type="button" value="..."/> | |
| <input checked="" type="checkbox"/> vm3WL | ASC DEMO | Open | ⚠ Medium | <input type="button" value="..."/> | |

4. On the **Vulnerability assessment solution should be installed on your virtual machines** page, click

Install on 2 VMs (the name might vary according to the number of VMs that you selected):



5. You can create a new vulnerability assessment or use an existing solution. If you create a new vulnerability assessment, you can select a partner solution in the **Azure Marketplace**. Or, under **Use existing solution**, select **Qualys** or **Rapid7**.

To deploy the agent from Security Center, you need a license code and public key from the vendor. To learn how to get the license code and public key, see the [Qualys documentation](#) or [Rapid7 documentation](#).

6. To create a new assessment, click **Create new**. The partner's **vulnerability management** page opens. The options shown on this page might change depending on the partner.

To set up Qualys (for example), select **Qualys** then:

- a. For **Resource group**, select **Use existing**.
- b. For **Location**, select where the solution is geographically located.
- c. In the **License code** box (this is specific for Qualys), enter the license provided by the partner.

- d. In the **Public key** box (this is specific for Qualys), enter the public key information provided by the partner.
- e. To automatically install a vulnerability assessment agent on all discovered VMs in the subscription of this Qualys solution, select the **Auto update** check box.
- f. Click **OK**.

Review the recommendation

After the vulnerability assessment solution is installed on the target VM, Security Center scans the VM to detect and identify system and application vulnerabilities.

NOTE

It might take a couple of hours for the first scan to complete. After that, it is an hourly process.

Detected issues are shown under the **Virtual Machines Recommendations**.

Next steps

This article described the built-in vulnerability assessment tool powered by Qualys for scanning your VMs. For related material, see the following articles:

- [Learn about the different elements of a recommendation](#)
- [Learn how to remediate recommendations](#)

Monitoring the security of your containers

2/27/2020 • 4 minutes to read • [Edit Online](#)

This page explains how to use the container security features described in the [Container Security article](#) in our concepts section.

Azure Security Center covers the following three aspects of container security:

- **Vulnerability management** - If you're on Security Center's standard pricing tier (see [pricing](#)), you can scan your ARM-based Azure Container Registry every time a new image is pushed. The scanner (powered by Qualys) presents findings as Security Center recommendations. For detailed instructions, see [Scanning your container registries for vulnerabilities](#) below.
- **Hardening your containers' Docker hosts** - Security Center finds unmanaged containers hosted on IaaS Linux VMs or other Linux machines running Docker, and continuously compares the containers' configurations with the Center for Internet Security (CIS) Docker Benchmark. Security Center alerts you if your containers don't satisfy any of the controls. Continuous monitoring for security risks due to misconfigurations is a crucial component of any security program. For detailed instructions, see [Hardening your containers' Docker hosts](#) below.
- **Hardening your Azure Kubernetes Service clusters** - Security Center provides recommendations when it finds vulnerabilities in the configuration of your Azure Kubernetes Service clusters. For details of the specific recommendations that may appear, see the [Kubernetes Service recommendations](#).
- **Runtime protection** - If you're on Security Center's standard pricing tier, you'll get real-time threat protection for your containerized environments. Security Center generates alerts for suspicious activities at the host and AKS cluster level. For details of the relevant security alerts that might appear, see the [Alerts for Azure Kubernetes Service clusters](#) and [Alerts for containers - host level](#) sections of the alerts reference table.

Scanning your ARM-based container registries for vulnerabilities

1. To enable vulnerability scans of your Azure Container Registry images:
 - a. Ensure you're on Azure Security Center's standard pricing tier.
 - b. From the **Pricing & settings** page, enable the optional Container Registries bundle for your subscription:

Dashboard > Security Center - Pricing & settings > Settings - Pricing tier

Settings - Pricing tier

ASC DEMO

Search (Ctrl+ /) << Save

| Resource Type | Plan |
|--------------------------------|--|
| Virtual machines | Enabled Disabled |
| App Service | Enabled Disabled |
| PaaS SQL servers | Enabled Disabled |
| SQL servers on VMs (Preview) | Enabled Disabled |
| Storage accounts | Enabled Disabled |
| Kubernetes Services (Preview) | Enabled Disabled |
| Container Registries (Preview) | Enabled  Disabled |

Security Center is now ready to scan images that get pushed to the registry.

NOTE

This feature is charged per image.

2. To trigger the scan of an image, push it to your registry.

When the scan completes (typically after approximately 10 minutes), findings are available in Security Center recommendations.

3. To view the findings, go to the **Recommendations** page. If issues were found, you'll see the following recommendation:

Recommendation

Vulnerabilities in Azure Container Registry images should be remediated (powered by Qualys) (Preview) 

4. Select the recommendation. The recommendation details page opens with additional information. This information includes the list of registries with vulnerable images ("Affected resources") and the remediation steps.
5. Select a specific registry to see the repositories within it that have vulnerable repositories.

Dashboard > Security Center - Recommendations > Vulnerabilities in Azure Container Registry images should be remediated (powered by Qualys) (Preview)

Vulnerabilities in Azure Container Registry images should be remediated (powered by Qualys) (Preview)

| Unhealthy registries | Severity | Total vulnerabilities | Vulnerabilities by severity |
|----------------------|----------|-----------------------|-------------------------------|
| 2 / 3 | High | 123 | High 33 Medium 89 Low 1 |

Affected resources

- Unhealthy registries (2) [Healthy registries \(1\)](#) [Unscanned registries \(3\)](#)

Search container registries

| Name | Scanned Images | Vulnerable Images |
|-------------|----------------|-------------------|
| ascdemo | 3 | |
| img_ascdemo | | |

The registry details page opens with the list of affected repositories.

6. Select a specific repository to see the repositories within it that have vulnerable images.

ascdemo
Registry security health

| Registry | Total vulnerable images | Vulnerable images by severity |
|------------------|-------------------------|-------------------------------|
| ascdemo | 8 | High 7 Medium 1 Low 0 |
| Out of 9 scanned | | |

[Unhealthy repositories \(6\)](#) [Healthy repositories \(1\)](#) [Unscanned repositories \(0\)](#)

Search repositories

| Name | Scanned Images | Vulnerable Images |
|-------------------------|----------------|-------------------|
| dotnet/core/sdk | 2 | |
| library/dotnet/core/sdk | 1 | |

The repository details page opens. It lists the vulnerable images together with an assessment of the severity of the findings.

7. Select a specific image to see the vulnerabilities.

[Unhealthy images \(2\)](#) [Healthy images \(0\)](#) [Unscanned images \(0\)](#)

Search images

| Digest | Scan report time |
|---------------------|----------------------------|
| 2e7c9245e5fd | 10/28/2019, 12:57 AM GMT+2 |
| fc9f02e7e/c9245e5fd | 10/28/2019, 12:58 AM GMT+2 |

The list of findings for the selected image opens.

Image 2e7c9245e5fd **Total vulnerabilities** 3 **Vulnerabilities by severity**

| Severity | Count |
|----------|-------|
| High | 0 |
| Medium | 3 |
| Low | 0 |

Findings

| ID | Security Check | Category | Severity |
|--------|--|----------|-----------|
| 91571 | Microsoft .NET Core Security Update September 2019 | Windows | ⚠️ Medium |
| 177338 | Debian Security Update for expat (DSA 4530-1) | Debian | ⚠️ Medium |
| 177277 | Debian Security Update for nghttp2 (DSA 4511-1) | Debian | ⚠️ Medium |

- To learn more about a finding, select the finding.

The findings details pane opens.

Dashboard > Security Center - Recommendations > Vulnerabilities in Azure Container Registry images

2e7c9245e5fd

Description

.NET Core is a general purpose development platform maintained by Microsoft and the .NET community on GitHub. It is cross-platform, supporting Windows, macOS and Linux, and can be used in device, cloud, and embedded/IoT scenarios.

A denial of service vulnerability exists when .NET Core improperly handles web requests.

Affected versions

- .NET Core 2.1.0 prior to 2.1.13
- .NET Core 2.2.0 prior to 2.2.7

Qid detection logic: Authenticated

The qid looks for sub directories under %programfiles%\dotnet\shared \Microsoft.NETCore.App, %programfiles(x86)%\dotnet\shared \Microsoft.NETCore.App and checks for vulnerable versions in .version file on windows.

General information

| ID | 91571 |
|---------------------|-------------------------------|
| Severity | ⚠️ Medium |
| Type | Vulnerability |
| Published | 9/11/2019, 6:44 AM GMT+3 |
| Patchable | Yes |
| Cvss 3.0 base score | 7.5 |
| CVEs | CVE-2019-1301 |

Remediation

Microsoft has released an update. Please refer to vendor security advisory [.NET Core CVE-2019-1301](#) for more information.

This pane includes a detailed description of the issue and links to external resources to help mitigate the threats.

- Follow the steps in the remediation section of this pane.
- When you have taken the steps required to remediate the security issue, replace the image in your registry:
 - Push the updated image. This will trigger a scan.
 - Check the recommendations page for the recommendation "Vulnerabilities in Azure Container Registry images should be remediated". If the recommendation still appears and the image you've handled still appears in the list of vulnerable images, check the remediation steps again.
 - When you are sure the updated image has been pushed, scanned, and is no longer appearing in the

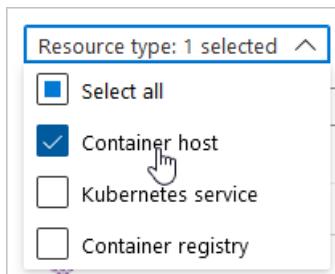
recommendation, delete the "old" vulnerable image from your registry.

Hardening your containers' Docker hosts

Security Center constantly monitors the configuration of your Docker hosts, and generates security recommendations that reflect industry standards.

To view Azure Security Center's security recommendations for your containers' Docker hosts:

1. From the Security Center navigation bar, open **Compute & apps** and select the **Containers** tab.
2. Optionally, filter the list of your container resources to container hosts hosts.



3. From the list of your container host machines, select one to investigate further.

A screenshot of the 'Compute & apps' section in the Azure Security Center. On the left, there's a sidebar with links like Overview, Getting started, Pricing & settings, Community, Workflow automation, Policy & Compliance (Coverage, Secure Score, Security policy, Regulatory compliance), Resource Security Hygiene (Recommendations, Compute & apps, Networking), and a search bar. The main area has tabs for Overview, VMs and Servers, VM scale sets, Cloud services, App services, and Containers (which is highlighted with a blue border). Below these tabs are filters for 'Resource type: 1 selected' and 'Severity: All', and a search bar. A table lists container hosts: rade-3, rade-2, rade-1, node-4, k8s-master, g-master, and ascd. Each host has a small icon, a name, a 'Total' column showing '1 of 1 recommendations', and a severity bar filled with red.

The **Container host information page** opens with details of the host and a list of recommendations.

4. From the recommendations list, select a recommendation to investigate further.

Dashboard > Security Center - Compute & apps > k8s-master

k8s-master

Container host security health

| Resource health | Total recommendations | Recommendations summary |
|--|-----------------------|--|
|  k8s-master | 1 | High 1 <div style="width: 100%; background-color: red; height: 10px;"></div> Medium 0 Low 0 |

Container host information

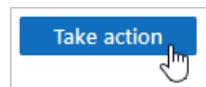
| | |
|--------------------------|-------------------|
| Resource Name | k8s-master |
| Resource Group | contoso-k8s-01 |
| Subscription | Contoso IT - demo |
| Docker version | Unknown |
| Orchestrator | Unknown |
| Operating system | Unknown |
| Image count | Unknown |
| Running containers count | Unknown |

Recommendation list

| Recommendation | Status |
|---|---|
| Vulnerabilities in container security configurations should be remediated |  High |

5. Optionally, read the description, information, threats, and remediation steps.

6. Select **Take Action** at the bottom of the page.



Log Analytics opens with a custom operation ready to run. The default custom query includes a list of all failed rules that were assessed, along with guidelines to help you resolve the issues.

Dashboard > Security Center - Compute & apps > k8s-master > Vulnerabilities in container security configurations should be remediated

Logs

contosoretail-IT

New Query 1* +

contosoretail-IT Select Scope Run Time range : Custom Save Copy link New alert

Tables Filter <

Search =

Group by: Solution Filters: not selected ^

```
SecurityBaseline
| where BaselineType == "Docker"
| where Computer == "k8s-master" and AnalyzeResult == "Failed"
| summarize arg_max(TimeGenerated, *) by CceId
| project CceId, Description, Resource, ResourceGroup, RuleSeverity
| order by RuleSeverity asc nulls last
```

7. Tweak the query parameters and select **Run** when you're sure it's ready for your host.

Next steps

In this article, you learned how to use Security Center's container security features.

For other related material, see the following pages:

- [Security Center recommendations for containers](#)

- Alerts for AKS cluster level
- Alerts for Container host level

Microsoft Defender Advanced Threat Protection with Azure Security Center

2/28/2020 • 4 minutes to read • [Edit Online](#)

Azure Security Center is extending its Cloud Workload Protection Platforms offering by integrating with [Microsoft Defender Advanced Threat Protection \(ATP\)](#). This change brings comprehensive Endpoint Detection and Response (EDR) capabilities. With Microsoft Defender ATP integration, you can spot abnormalities. You can also detect and respond to advanced attacks on server endpoints monitored by Azure Security Center.

Microsoft Defender ATP features in Security Center

When you use Microsoft Defender ATP, you get:

- **Advanced post-breach detection sensors:** Microsoft Defender ATP sensors for Windows servers collect a vast array of behavioral signals.
- **Analytics-based, cloud-powered post breach detection:** Microsoft Defender ATP quickly adapts to changing threats. It uses advanced analytics and big data. Microsoft Defender ATP is amplified by the power of the Intelligent Security Graph with signals across Windows, Azure, and Office to detect unknown threats. It provides actionable alerts and enables you to respond quickly.
- **Threat intelligence:** Microsoft Defender ATP generates alerts when it identifies attacker tools, techniques, and procedures. It uses data generated by Microsoft threat hunters and security teams, augmented by intelligence provided by partners.

The following capabilities are now available in Azure Security Center:

- **Automated onboarding:** The Microsoft Defender ATP sensor is automatically enabled for Windows servers that are onboarded to Azure Security Center.
- **Single pane of glass:** The Azure Security Center console displays Microsoft Defender ATP alerts.
- **Detailed machine investigation:** Azure Security Center customers can use Microsoft Defender ATP console to conduct a detailed investigation to uncover the scope of a breach.

Suspicious Powershell commandline

| ATTACKED RESOURCE | COUNT | DETECTION TIME | ENVIRONMENT | STATE | SEVERITY | ... |
|-------------------|-------|----------------|-------------|--------|-----------|-----|
| wdatp-mw-vm2 | 1 | 11:02:13 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm3 | 1 | 11:02:05 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm2 | 1 | 10:32:13 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm3 | 1 | 10:32:02 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm2 | 1 | 10:02:13 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm3 | 1 | 10:02:02 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm2 | 1 | 09:32:13 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm3 | 1 | 09:32:02 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm2 | 1 | 09:02:13 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm3 | 1 | 09:02:02 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm2 | 1 | 08:32:13 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm3 | 1 | 08:32:02 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm3 | 1 | 08:02:19 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm2 | 1 | 08:02:13 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm3 | 1 | 08:02:02 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm2 | 1 | 07:32:13 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm2 | 1 | 07:32:13 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm3 | 1 | 07:32:05 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm3 | 1 | 07:32:04 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm3 | 1 | 07:02:20 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm2 | 1 | 07:02:13 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm2 | 1 | 07:02:13 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm3 | 1 | 07:02:02 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm3 | 1 | 07:02:02 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm3 | 1 | 06:32:20 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm2 | 1 | 06:32:13 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm2 | 1 | 06:32:13 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm3 | 1 | 06:32:08 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm3 | 1 | 06:32:03 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm2 | 1 | 06:02:13 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm2 | 1 | 06:02:13 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm3 | 1 | 06:02:05 AM | Azure | Active | ⚠️ Medium | ... |
| wdatp-mw-vm3 | 1 | 05:32:23 AM | Azure | Active | ⚠️ Medium | ... |

Suspicious Powershell commandline (Preview)

Learn more

General information

A suspicious Powershell commandline was found on the machine. This commandline might be used during installation, exploration, or in some cases with lateral movement activities which are used by attackers to invoke modules, download external payloads, and get more information about the system. Attackers usually use Powershell to bypass security protection mechanisms by executing their payload in memory without touching the disk and leaving any trace.

The process powershell.exe was executing suspicious commandline "powershell.exe" -ExecutionPolicy Bypass -WindowStyle Hidden (New-Object System.Net.WebClient).DownloadFile("http://127.0.0.1/2.exe", "%TEMP%\Invoice.exe") dir c:\2018-06-19-07-32-16.609\Start-Process %TEMP%\Invoice.exe"

DESCRIPTION

DETECTION TIME

Tuesday, June 19, 2018 10:32:13 AM

SEVERITY

⚠️ Medium

STATE

Active

ATTACKED RESOURCE

wdatp-mw-vm2

SUBSCRIPTION

Visual Studio Ultimate with MSDN (4a5896d3-4c63-445c-8c8d-6ffbd5b2bf07)

DETECTED BY

Microsoft

ENVIRONMENT

Azure

RESOURCE TYPE

Virtual Machine

FILE NAME

powershell.exe

FILE PATH

C:\Windows\SysWOW64\WindowsPowerShell\v1.0

USER NAME

omsadmin

USER DOMAIN

wdatp-mw-vm2

MACHINE NAME

wdatp-mw-vm2

Remediation steps

Investigate View playbooks

To investigate further, use Microsoft Defender ATP. Microsoft Defender ATP provides additional information such as the alert process tree and the incident graph. You can also see a detailed machine timeline that shows every behavior for a historical period of up to six months.

Windows Defender Security Center

Alerts > Suspicious Powershell commandline

Suspicious Powershell commandline

Actions

Severity: Medium Category: Suspicious Activity Detection source: EDR

Description

A suspicious Powershell commandline was found on the machine. This commandline might be used during installation, exploration, or in some cases with lateral movement activities which are used by attackers to invoke modules, download external payloads, and get more information about the system. Attackers usually use Powershell to bypass security protection mechanisms by executing their payload in memory without touching the disk and leaving any trace.

The process powershell.exe was executing suspicious commandline "powershell.exe" -ExecutionPolicy Bypass -WindowStyle Hidden (New-Object System.Net.WebClient).DownloadFile("http://127.0.0.1/2.exe", "%TEMP%\Invoice.exe") dir c:\2018-06-19-07-32-16.609\Start-Process %TEMP%\Invoice.exe"

Alert context

wdatp-mw-vm2
wdatp-mw-vm3

Status

State: New Classification: Not set Assigned to: Not assigned

Recommended actions

- Examine the PowerShell commandline to understand what commands were executed. Note: the script may need to be decoded if it is base64-encoded
- Search the script for more indicators to investigate - for example IP addresses (potential C2C servers), target computers etc.
- Explore the timeline of this and other related machines for additional suspect activities around the time of the alert.
- Look for the process that invoked this PowerShell run and their origins. Consider submitting any suspect files in the chain for deep analysis for detailed behavior information.

Show more

Alert process tree

```

graph TD
    wdatp-mw-vm2[wdatp-mw-vm2] --> servicesexe[services.exe]
    servicesexe --> webhostexe[webhost.exe]
    webhostexe --> WDATPAlertSimulatorexe[WDATPAlertSimulator.exe]
    WDATPAlertSimulatorexe --> powershellexe[powershell.exe]
    powershellexe --> cohostexe[cohost.exe]
  
```

Incident graph

```

graph LR
    wdatp-mw-vm2[wdatp-mw-vm2] --> powershellexe[powershell.exe]
  
```

Artifact timeline

| Description | First Observed | Details |
|------------------------|---------------------|---------|
| http://127.0.0.1/2.exe | 06/19/2018 07:32:13 | |

Platform support

Microsoft Defender ATP in Security Center supports detection on Windows Server 2016, 2012 R2, and 2008 R2 SP1, for Azure VMs you need a Standard tier subscription and for Non-Azure VMs you need Standard tier in the workspace level only.

NOTE

When you use Azure Security Center to monitor servers, a Microsoft Defender ATP tenant is automatically created and the Microsoft Defender ATP data is stored in Europe by default. If you need to move your data to another location, you need to contact Microsoft Support to reset the tenant. Server endpoint monitoring utilizing this integration has been disabled for Office 365 GCC customers.

Onboarding servers to Security Center

To onboard servers to Security Center, click **Go to Azure Security Center to onboard servers** from the Microsoft Defender ATP server onboarding.

1. In the **Onboarding** area, select or create a workspace in which to store the data.
2. If you can't see all your workspaces, it may be due to a lack of permissions, make sure your workspace is set to Azure Security Standard tier. For more information, see [Upgrade to Security Center's Standard tier for enhanced security](#).
3. Select **Add servers** to view instructions on how to install the Microsoft Monitoring Agent.
4. After onboarding, you can monitor the machines under **Compute and apps**.

The screenshot shows the 'Onboard computers to Security Center' page. At the top, there's a navigation bar with 'Dashboard > Onboard computers to Security Center'. Below the navigation is a header 'Onboard computers to Security Center'. A blue banner at the top says 'Visit [Security Center](#) To manage security across your virtual networks, data, apps, and more'. The main section is titled 'Onboard computers to Security Center' with a plus sign icon. It contains instructions: 'To onboard computers to Security Center:'. Step 1: 'Select or create a workspace in which to store the data.' with a 'Create New Workspace' button. Step 2: 'Select [Upgrade](#) to set the workspace's pricing tier to Standard and start your free 30-day trial.' Step 3: 'Select [Add Computers](#) to view instructions on how to install the Microsoft Monitoring Agent. [Learn more](#)' Step 4: 'After onboarding, you can monitor the machines under [Compute and apps](#)'. Below these steps is a table with columns: WORKSPACE NAME, COVERAGE, VMS & COMPUTERS, and SUBSCRIPTION. The table shows 'No workspaces found.' and a note: 'Azure Security Center Standard will be applied \$15/node/month. [Pricing details](#)'.

Enable Microsoft Defender ATP integration

To view if Microsoft Defender ATP integration is enabled, select **Security center > Pricing & settings** > click on your subscription. Here you can see the integrations currently enabled.

Home > Security Center - Security policy > Settings - Threat detection

Settings - Threat detection

Visual Studio Ultimate with MSDN

Search (Ctrl+ /) Save

Settings

Data Collection

Threat detection

Email notifications

Pricing tier

Enable integrations

To enable Security Center to integrate with other Microsoft security services, allow those services to access your data.

Allow Microsoft Cloud App Security to access my data. [Learn more >](#)

Allow Windows Defender ATP to access my data. [Learn more >](#)

- If you've already onboarded the servers to Azure Security Center standard tier, you need take no further action. Azure Security Center will automatically onboard the servers to Microsoft Defender ATP. Onboarding might take up to 24 hours.
- If you've never onboarded the servers to Azure Security Center standard tier, onboard them to Azure Security Center as usual.
- If you've onboarded the servers through Microsoft Defender ATP:
 - Refer to the documentation for guidance on [how to offboard server machines](#).
 - Onboard these servers to Azure Security Center.

Access to the Microsoft Defender ATP portal

Follow the instructions in [Assign user access to the portal](#).

Set the firewall configuration

If you have a proxy or firewall that is blocking anonymous traffic, as a Microsoft Defender ATP sensor is connecting from the system context, make sure that anonymous traffic is permitted. Follow the instructions in [Enable access to Microsoft Defender ATP service URLs in the proxy server](#).

Test the feature

To generate a benign Microsoft Defender ATP test alert:

1. Create a folder 'C:\test-MDATP-test'.
2. Use Remote Desktop to access either a Windows Server 2012 R2 VM or a Windows Server 2016 VM. Open a command line window.
3. At the prompt, copy and run the following command. The Command Prompt window will close automatically.

```
powershell.exe -NoExit -ExecutionPolicy Bypass -WindowStyle Hidden (New-Object System.Net.WebClient).DownloadFile('http://127.0.0.1/1.exe', 'C:\\\\test-MDATP-test\\\\invoice.exe'); Start-Process 'C:\\\\test-MDATP-test\\\\invoice.exe'
```



4. If the command is successful, you'll see a new alert on the Azure Security Center dashboard and the Microsoft Defender ATP portal. This alert might take a few minutes to appear.
5. To review the alert in Security Center, go to **Security Alerts > Suspicious Powershell CommandLine**.

6. From the investigation window, select the link to go to the Microsoft Defender ATP portal.

Next steps

- [Platforms and features supported by Azure Security Center](#)
- [Setting security policies in Azure Security Center](#): Learn how to configure security policies for your Azure subscriptions and resource groups.
- [Managing security recommendations in Azure Security Center](#): Learn how recommendations help you protect your Azure resources.
- [Security health monitoring in Azure Security Center](#): Learn how to monitor the health of your Azure resources.

Advanced data security for SQL servers on Azure Virtual Machines (Preview)

2/25/2020 • 6 minutes to read • [Edit Online](#)

Advanced data security for SQL Servers on Azure Virtual Machines is a unified package for advanced SQL security capabilities. This preview feature includes functionality for identifying and mitigating potential database vulnerabilities and detecting anomalous activities that could indicate threats to your database.

This security offering for Azure VMs SQL servers is based on the same fundamental technology used in the [Azure SQL Database Advanced Data Security package](#).

Overview

Advanced data security provides a set of advanced SQL security capabilities, consisting of Vulnerability assessment and Advanced Threat Protection.

- [Vulnerability assessment](#) is an easy to configure service that can discover, track, and help you remediate potential database vulnerabilities. It provides visibility into your security state, and includes the steps to resolve security issues and enhance your database fortifications.
- [Advanced Threat Protection](#) detects anomalous activities indicating unusual and potentially harmful attempts to access or exploit your SQL server. It continuously monitors your database for suspicious activities and provides action-oriented security alerts on anomalous database access patterns. These alerts provide the suspicious activity details and recommended actions to investigate and mitigate the threat.

Get started with Advanced data security for SQL on Azure VMs

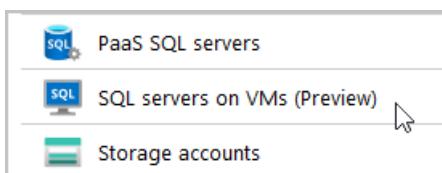
The following steps get you started with Advanced Data Security for SQL on Azure VMs Public Preview.

Set up advanced data security for SQL on Azure VMs

Enable Advanced Data Security for SQL Servers on Virtual Machines at the subscription/workspace level:

1. From Security Center's sidebar, open the **Pricing & settings** page.
2. Select the subscription or workspace for which you want to enable Advanced Data Security for SQL on Azure VMs.
3. Toggle the option for **SQL servers on VM (Preview)** to enabled.

(Click the screenshot to expand)



Advanced Data Security for SQL Servers will be enabled on all SQL Servers connected to the selected workspace or the default workspace of the selected subscription.

NOTE

The solution will be fully active after the first restart of the SQL Server.

To create a new workspace, follow the instructions in [Create a Log Analytics workspace](#).

To connect the SQL Server's host to a workspace, follow the instructions in [Connect Windows computers to Azure Monitor](#).

Set up email notification for security alerts

You can set a list of recipients to receive an email notification when Security Center alerts are generated. The email contains a direct link to the alert in Azure Security Center with all the relevant details.

1. Go to **Security Center > Pricing & settings** and click on the relevant subscription

The screenshot shows the 'Pricing & Settings' section of the Azure Security Center. On the left, there's a navigation menu with sections like Overview, Getting started, Pricing & settings (which is selected), Policy & Compliance, Resource Security Hygiene, Advanced Cloud Defense, Threat Protection, Automation & Orchestration, Logs, and Events. The main area displays '10 MANAGEMENT GROUPS', '3 SUBSCRIPTIONS', and '2 WORKSPACES'. A search bar at the top allows searching by name. Below it is a table listing subscriptions under management groups. The table columns are 'NAME' and 'PRICING TIER'. Subscriptions listed include 'ASC DEMO' (Standard), 'Non Production' (Free), 'NonProd Outside Ring' (Free), 'Production' (Free), 'Prod Outside Ring' (Standard), 'Prod Ring1' (Standard), and 'File Integrity Monitoring' (Standard partial). There are also two workspaces: 'exportSecurityCenterDataToLogAWorkspaceTest' (Standard) and another unnamed workspace (Free).

2. From the Settings menu, click **Email notifications**.

3. In the **Email address** text box, enter the email addresses to receive the notifications. You can enter more than one email address by separating the email addresses with a comma (,). For example
admin1@mycompany.com,admin2@mycompany.com,admin3@mycompany.com

The screenshot shows the 'Settings - Email notifications' page. The left sidebar has a 'Settings' section with options: Data Collection, Threat detection, and Email notifications (which is selected and highlighted with a green border). Other options include Pricing tier and Edit security configurations. The main area has a 'Save' button and a note: 'Enter contact information for the administrator who should be notified when Azure Security Center detects compromised resources.' Below this is a 'Email address' input field containing a placeholder email address. There's also a 'Phone number' input field. Under 'Email notification settings', there are two toggle switches: 'Send email notification for high severity alerts' (On) and 'Also send email notification to subscription owners' (On). A note below explains that an email notification is sent once a day for each high severity alert when it is first detected, and all notifications are sent from a US-based service regardless of the geographical location of the affected resources. A 'Learn more >' link is provided.

4. In the **Email notification** settings, set the following options:

- **Send email notification for high severity alerts:** Instead of sending emails for all alerts, send only for high severity alerts.
- **Also send email notifications to subscription owners:** Send notifications to the subscriptions owners too.

5. In the top of the **Email notifications** screen, click **Save**.

NOTE

Be sure to click **Save** before closing the window, or the new **Email notification** settings will not be saved.

Explore vulnerability assessment reports

The Vulnerability assessment dashboard provides an overview of your assessment results across all your databases. You can view the distribution of databases according to SQL Server version, along with a summary of failing versus passing databases and an overall summary of failing checks according to risk distribution.

You can view the vulnerability assessment results directly from Security Center.

1. From Security Center's sidebar, under RESOURCE SECURITY HYGIENE, select **Data & Storage**.
2. Select the recommendation **Vulnerabilities on your SQL databases in VMs should be remediated (Preview)**. For more information, see [Security Center Recommendations](#).

The screenshot shows the Azure Security Center interface for the 'Data & storage' section. On the left, there's a sidebar with various navigation items like Overview, Getting started, Pricing & settings, Community, Workflow automation (Preview), Policy & Compliance, and Resource Security Hygiene (with 'Data & storage' highlighted). The main area is titled 'SQL Information Protection' and contains several cards: Overview, SQL, Storage accounts, Redis, Data Lake Analytics, and Data Lake Store. Below these is a 'Search recommendations' bar. A list of recommendations is displayed, with the first one, 'Vulnerabilities on your SQL databases in VMs should be remediated (Preview)', highlighted with a red border. This recommendation has a 'Secure Score Impact' of +30, 6 failed resources (6 of 6 SQL virtual machines), and a Severity of High. Other recommendations listed include 'Vulnerabilities on your SQL databases should be remediated (Preview)', 'Sensitive data in your SQL databases should be classified', 'An Azure Active Directory administrator should be provisioned for SQL servers', 'Secure transfer to storage accounts should be enabled', 'Vulnerability assessment should be enabled on your SQL servers', 'Vulnerability assessment should be enabled on your SQL managed instances', 'Storage accounts should be migrated to new Azure Resource Manager resources', 'Diagnostic logs in Azure Data Lake Store should be enabled', and 'Diagnostic logs in Data Lake Analytics should be enabled'. Each recommendation includes a 'Quick Fix' button.

The detailed view for this recommendation appears.

Vulnerabilities on your SQL databases in VMs should be remediated (Preview)

Description

General Information

Threats

Affected resources

Unhealthy resources (7) Healthy resources (0) Unscanned resources (0) Search SQL virtual machines

Name

↑↓ Subscription



AD

D



sqlv

D



SQ

D

Security Checks

Findings

Passed

 Search to filter items...

| ID | Security Check | Category | Applies To | Severity |
|--------|--|--------------------------------|-------------------|--|
| VA2110 | Execute permissions to access the registry sh... | AuthenticationAndAuthorization | 2 of 2 databases | ! High |
| VA1258 | Database owners are as expected | AuditingAndLogging | 2 of 2 databases | ! High |
| VA2108 | Minimal set of principals should be members... | AuthenticationAndAuthorization | 2 of 14 databases | ! High |
| VA1220 | Database communication using TDS should ... | DataProtection | 2 of 2 databases | ! High |
| VA2114 | Minimal set of principals should be members... | AuthenticationAndAuthorization | 2 of 2 databases | ! High |
| VA2052 | Minimal set of principals should be granted ... | AuthenticationAndAuthorization | 7 of 16 databases | ! Medium |

3. To drill down for more details:

- For an overview of scanned resources (databases) and the list of security checks that were tested, click the server of interest.

Vulnerabilities on your SQL databases in 'AD' should be remediated (Preview)

>Description

General Information

Threats

Affected resources

Unhealthy resources (3) [Healthy resources \(0\)](#)

| Name | Machine Name | Server Instance Name | Subscription |
|--------|--------------|----------------------|--------------|
| msdb | AD | MSSQLSERVER | D |
| model | AD | MSSQLSERVER | D |
| master | AD | MSSQLSERVER | D |

Security Checks

Findings [Passed](#)

Search to filter items...

| ID | Security Check | Category | Applies To | Severity |
|--------|--|--------------------------------|------------------|----------|
| VA1072 | Authentication mode should be Windows Authentication | AuthenticationAndAuthorization | 1 of 1 databases | Medium |
| VA2052 | Minimal set of principals should be granted to PUBLIC role... | AuthenticationAndAuthorization | 1 of 1 databases | Medium |
| VA1069 | Permissions to select from system tables and views should... | AuthenticationAndAuthorization | 2 of 2 databases | Low |
| VA1054 | Excessive permissions should not be granted to PUBLIC role... | AuthenticationAndAuthorization | 1 of 1 databases | Low |
| VA1092 | SQL Server instance shouldn't be advertised by the SQL Server... | SurfaceAreaReduction | 1 of 1 databases | Low |
| VA1091 | Auditing of both successful and failed login attempts (defau... | AuditingAndLogging | 1 of 1 databases | Low |

- For an overview of the vulnerabilities grouped by a specific SQL database, click the database of interest.

master (AD/MSSQLSERVER)

security health



Resource



master

Total vulnerabilities

8

Vulnerabilities by severity

High 0

Medium 1

Low 7

Findings [Passed](#)

Search to filter items...

| ID | Security Check | Category | Severity |
|--------|--|--------------------------------|----------|
| VA1072 | Authentication mode should be Windows Authentication | AuthenticationAndAuthorization | Medium |
| VA1069 | Permissions to select from system tables and views should... | AuthenticationAndAuthorization | Low |
| VA1054 | Excessive permissions should not be granted to PUBLIC role... | AuthenticationAndAuthorization | Low |
| VA1092 | SQL Server instance shouldn't be advertised by the SQL Server... | SurfaceAreaReduction | Low |
| VA1091 | Auditing of both successful and failed login attempts (defau... | AuditingAndLogging | Low |
| VA1093 | Maximum number of error logs should be 12 or more | AuditingAndLogging | Low |
| VA1047 | Password expiration check should be enabled for all SQL logins | AuthenticationAndAuthorization | Low |
| VA1046 | CHECK_POLICY should be enabled for all SQL logins | AuthenticationAndAuthorization | Low |

In each view, the security checks are sorted by **Severity**. Click a specific security check to see a details pane with a **Description**, how to **Remediate** it, and other related information such as **Impact** or **Benchmark**.

Advanced threat protection for SQL servers on Azure VMs alerts

Alerts are generated by unusual and potentially harmful attempts to access or exploit SQL Servers. These events can trigger the following alerts:

Anomalous access pattern alerts (Preview)

- **Access from unusual location:** This alert is triggered when there is a change in the access pattern to SQL server, where someone has logged on to the SQL server from an unusual geographical location. Potential causes:
 - An attacker or former malicious employ has accessed your SQL Server.
 - A legitimate user has accessed your SQL Server from a new location.
- **Access from a potentially harmful application:** This alert is triggered when a potentially harmful application is used to access the database. Potential causes:
 - An attacker trying to breach your SQL using common attack tools.
 - A legitimate penetration testing in action.
- **Access from unfamiliar principal:** This alert is triggered when there is a change in the access pattern to SQL server, where someone has logged on to the SQL server using an unusual principal (SQL user). Potential causes:
 - An attacker or former malicious employ has accessed your SQL Server.
 - A legitimate user has accessed your SQL Server from with a new principal.
- **Brute force SQL credentials:** This alert is triggered when there is an abnormal high number of failed logins with different credentials. Potential causes:
 - An attacker trying to breach your SQL using brute force.
 - A legitimate penetration testing in action.

Potential SQL injection attacks (Supported in SQL Server 2019)

- **Vulnerability to SQL injection:** This alert is triggered when an application generates a faulty SQL statement in the database. This alert may indicate a possible vulnerability to SQL injection attacks. Potential causes:
 - A defect in application code that constructs the faulty SQL statement
 - Application code or stored procedures don't sanitize user input when constructing the faulty SQL statement, which may be exploited for SQL Injection
- **Potential SQL injection:** This alert is triggered when an active exploit happens against an identified application vulnerability to SQL injection. This means the attacker is trying to inject malicious SQL statements using the vulnerable application code or stored procedures.

Unsafe command (Supported in SQL Server 2019)

- **Potentially Unsafe Action:** This alert is triggered when a highly privileged and potentially unsafe command is executed. Potential causes:
 - Command which recommended to be disabled for better security posture is enabled.
 - An attacker trying to exploit SQL access or escalate privileges.

Explore and investigate security alerts

Your data security alerts are available in Security Center's alerts page, the resource's security tab, or through the direct link in the alert emails.

1. To view alerts:
 - In Security Center - Click **Security alerts** from the sidebar and select an alert.
 - In the resource scope - Open the relevant resource page, and from the sidebar click **Security**.
2. Alerts are designed to be self-contained, with detailed remediation steps and investigation information in each one. You can investigate further by using other Azure Security Center and Azure Sentinel capabilities

for a broader view:

- Enable SQL Server's auditing feature for further investigations. If you're an Azure Sentinel user, you can upload the SQL auditing logs from the Windows Security Log events to Sentinel and enjoy a rich investigation experience.
- To improve your security posture, use Security Center's recommendations for the host machine indicated in each alert. This will reduce the risks of future attacks.

Next steps

For related material, see the following article:

- [How to remediate recommendations](#)

Protect your Azure App Service web apps and APIs

2/25/2020 • 2 minutes to read • [Edit Online](#)

Azure App Service is a fully managed platform for building and hosting your web apps and APIs without worrying about having to manage the infrastructure. It provides management, monitoring, and operational insights to meet enterprise-grade performance, security, and compliance requirements. For more information, see [Azure App Service](#).

To enable advanced threat protection for your Azure App Service plan, you must:

- Subscribe to Azure Security Center's Standard pricing tier
- Enable the App Service plan as shown below. Security Center is natively integrated with App Service, eliminating the need for deployment and onboarding - the integration is transparent.
- Have an App Service plan that is associated with dedicated machines. Supported plans are: Basic, Standard, Premium, Isolated, or Linux. Security Center doesn't support the Free, Shared, or Consumption plans. For more information, see [App Service Plans](#).

With the App Service plan enabled, Security Center assesses the resources covered by your App Service plan and generates security recommendations based on its findings. Security Center protects the VM instance in which your App Service is running and the management interface. It also monitors requests and responses sent to and from your apps running in App Service.

Security Center leverages the scale of the cloud, and the visibility that Azure has as a cloud provider, to monitor for common web app attacks. Security Center can discover attacks on your applications and identify emerging attacks - even while attackers are in the reconnaissance phase, scanning to identify vulnerabilities across multiple Azure-hosted applications. As an Azure-native service, Security Center is also in a unique position to offer host-based security analytics covering the underlying compute nodes for this PaaS, enabling Security Center to detect attacks against web applications that were already exploited. For more details, see [Threat protection for Azure App Service](#).

Enabling monitoring and protection of App Service

1. In the Azure portal, choose Security Center.
2. Go to **Pricing & settings** and choose a subscription.
3. Under **Pricing tier**, in the **App service** row, toggle your plan to **Enabled**.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Security Center - Pricing & settings > Settings - Pricing tier

Settings - Pricing tier

ASC DEMO

Search (Ctrl+ /) Save

The Standard tier provides enhanced security. [Learn more >](#)

| Free (for Azure resources only) | Standard |
|--|--|
| ✓ Continuous assessment and security recommendations | ✓ Continuous assessment and security recommendations |
| ✓ Azure Secure Score | ✓ Azure Secure Score |
| ✗ Just in time VM Access | ✓ Just in time VM Access |
| ✗ Adaptive application controls and network hardening | ✓ Adaptive application controls and network hardening |
| ✗ Regulatory compliance dashboard and reports | ✓ Regulatory compliance dashboard and reports |
| ✗ Threat protection for Azure VMs and non-Azure servers (Including Server EDR) | ✓ Threat protection for Azure VMs and non-Azure servers (including Server EDR) |
| ✗ Threat protection for supported PaaS services | ✓ Threat protection for supported PaaS services |

Pricing will apply to: 128 resources in this subscription

Select pricing tier by resource type

| Resource Type | Resource Quantity | Pricing | Plan |
|--------------------------|--------------------------------|-------------------------|--------------------|
| Virtual machines | 48 VMs and VMSS instances | \$15/Server/Month | Enabled (Disabled) |
| App Service | 5 instances | \$15/Instance/Month | Enabled (Disabled) |
| PaaS SQL servers | 6 resources | \$15/Server/Month | Enabled (Disabled) |
| SQL servers on VMs ... | 0 SQL servers on VMs | FREE durin... ⓘ | Enabled (Disabled) |
| Storage accounts | 47 Storage accounts | \$0.02/10K Transactions | Enabled (Disabled) |
| Kubernetes Services ... | 20 Kubernetes services' cor... | \$2/VM core/Month | Enabled (Disabled) |
| Container Registries ... | 2 Container registries | \$0.29/Image | Enabled (Disabled) |

NOTE

The number of instances listed for your **Resource Quantity** represents the total number of compute instances, in all App Service plans on this subscription, running at the moment when you opened the pricing tier blade.

Azure App Service offers a variety of plans. Your App Service plan defines the set of compute resources for a web app to run. These are equivalent to server farms in conventional web hosting. One or more apps can be configured to run on the same computing resources (or in the same App Service plan).

To validate the count, head to 'App Service plans' in the Azure Portal, where you can see the number of compute instances used by each plan.

To disable monitoring and recommendations for your App Service, repeat this process and toggle your **App Service plan to Disabled**.

See also

In this article, you learned how to use monitoring capabilities in Azure Security Center. To learn more about Azure Security Center, see the following articles:

- [Setting security policies in Azure Security Center](#): Learn how to configure security settings in Azure Security Center.
- [Managing and responding to security alerts in Azure Security Center](#): Learn how to manage and respond to security alerts.
- [App services](#): View a list of your App service environments with health summaries.
- [Monitoring partner solutions with Azure Security Center](#): Learn how to monitor the health status of your

partner solutions.

- [Azure Security Blog](#): Find blog posts about Azure security and compliance.

Working with security policies

11/11/2019 • 5 minutes to read • [Edit Online](#)

This article explains how security policies are configured, and how to view them in Security Center.

Introduction to security policies

A security policy defines the desired configuration of your workloads and helps ensure you're complying with the security requirements of your company or regulators.

Azure Security Center makes its security recommendations based on your chosen policies. Security Center policies are based on policy initiatives created in Azure Policy. You can use [Azure Policy](#) to manage your policies and to set policies across Management groups and across multiple subscriptions.

Security Center offers the following options for working with security policies:

- **View and edit the built-in default policy** - When you enable Security Center, a built-in initiative named 'ASC default' is automatically assigned to all Security Center registered subscriptions (Free or Standard tiers). To customize this initiative, you can enable or disable individual policies within it. See the list of [built-in security policies](#) to understand the options available out-of-the-box.
- **Add your own custom policies** - If you want to customize the security initiatives applied to your subscription, you can do so within Security Center. You'll then receive recommendations if your machines don't follow the policies you create. For instructions on building and assigning custom policies, see [Using custom security policies](#).
- **Add regulatory compliance policies** - Security Center's regulatory compliance dashboard shows the status of all the assessments within your environment in the context of a particular standard or regulation (such as Azure CIS, NIST SP 800-53 R4, SWIFT CSP CSCF-v2020). For more information, see [Improve your regulatory compliance](#).

Managing your security policies

To view your security policies in Security Center:

1. In the **Security Center** dashboard, select **Security policy**.

Security Center - Security policy

Showing 3 subscriptions

Search (Ctrl+)

Overview

Getting started

Pricing & settings

Policy & Compliance

- Coverage
- Secure score
- Regulatory compliance

Security policy

Resource Security Hygiene

- Recommendations
- Compute & apps
- Networking
- IoT hubs & resources (Preview)
- Data & storage
- Identity & access (Preview)
- Security solutions

Advanced Cloud Defense

- Adaptive application controls
- Just in time VM access
- Network hardening (Preview)
- File Integrity Monitoring

Threat Protection

- Security alerts
- Custom alert rules (Preview)
- Security alerts map (Preview)

Automation & Orchestration

- Playbooks (Preview)

Logs

- Events
- Search

Policy Management

Manage the security policies by choosing a subscription or management group from the list below. In order to define additional policies, manage exclusions and advanced settings, go to Azure policies > Click here to learn more >

10 MANAGEMENT GROUPS 3 SUBSCRIPTIONS

Search by name

NAME

- (3 of 49 subscriptions)
- (1 of 1 subscriptions)
 - ASC DEMO
- (1 of 46 subscriptions)
 - Non Production (1 of 42 subscriptions)
 - NonProd Outside Ring (1 of 40 subscriptions)
 - NonProd Ring1 (0 of 2 subscriptions)
 - Production (0 of 4 subscriptions)
 - Prod Outside Ring (0 of 3 subscriptions)
 - Prod Ring1 (0 of 1 subscriptions)
 - (0 of 1 subscriptions)

In the **Policy management** screen, you can see the number of management groups, subscriptions, and workspaces as well as your management group structure.

2. Select the subscription or management group whose policies you want to view.
3. The security policy page for that subscription or management group appears. It shows the available and assigned policies.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Security Center - Security policy > Security policy

Security policy
ASC DEMO

Security policy on: ASC DEMO

Policies assigned in this subscription

^  Security center default policy

ASC default (1) This is the default policy for Azure Security Center recommendations which is enabled by default on your subscription.

[View effective policy](#)

^  Industry & regulatory standards (preview)

Compliance policies that you can view in the compliance dashboard. To add more compliance standards, click [Add more standards](#).

| Policy | Description | Status |
|------------------------|--|----------------|
| Azure CIS 1.1.0 | Track Azure CIS 1.1.0 controls in the Compliance Dashboard, based on a recommended set of policies and assessments. | Out of the box |
| PCI DSS 3.2.1 | Track PCI-DSS v3.2.1:2018 controls in the Compliance Dashboard, based on a recommended set of policies and assessments. | Out of the box |
| ISO 27001 | Track ISO 27001:2013 controls in the Compliance Dashboard, based on a recommended set of policies and assessments. | Out of the box |
| SOC TSP | Track SOC TSP controls in the Compliance Dashboard, based on a recommended set of policies and assessments. | Out of the box |
| SWIFT CSP CSCF v2020 | Track SWIFT CSP CSCF v2020 controls in the Compliance Dashboard, based on a recommended set of policies and assessments. | Manually added |
| UK OFFICIAL and UK NHS | Track UK OFFICIAL and UK NHS controls in the Compliance Dashboard, based on a recommended set of policies and assessments. | Manually added |
| Azure CIS 1.1.0 (New) | Track Azure CIS 1.1.0 (New) controls in the Compliance Dashboard, based on a recommended set of policies and assessments. | Manually added |

[Add more standards](#)

^  Your custom initiatives (preview)

Custom initiative policies which you have created which are available in the [Recommendations](#) page. To add another custom initiative policy, click [Add a custom initiative](#).

| Initiative | Action |
|------------------|------------------------|
| CustomPolicyDemo | Delete |

[Add a custom initiative](#)

NOTE

If there is a label "MG Inherited" alongside your default policy, it means that the policy has been assigned to a management group and inherited by the subscription you're viewing.

4. Choose from the available options on this page:

- To work with industry policies, click **Add more standards**. For more information, see [Update to dynamic compliance packages](#).
- To assign and manage custom initiatives, click **Add custom initiatives**. For more information, see [Using custom security policies](#).
- To view and edit the default policy, click **View effective policy** and proceed as described below.

Security policy

Contoso IT

The selected subscription has 2 security policy assignments. The overall effective policies in Security Center are displayed below.

In order to configure a specific policy assignment, choose one of the assignments below:

ASC Default (subscription: abcd-1234-abcd-1234-abcd)

[Preview]: Enable Monitoring in Azure Security Center

The following security policies are assessed and displayed in Security Center:

Compute And Apps (14 out of 14 policies enabled)

| | |
|---|------------------|
| Endpoint protection | AuditIfNotExists |
| System updates | AuditIfNotExists |
| Security configurations | AuditIfNotExists |
| Disk encryption | AuditIfNotExists |
| Vulnerability Assessment | AuditIfNotExists |
| Adaptive Application Controls | AuditIfNotExists |
| cluster protection level in Service Fabric | Audit |
| Azure Active Directory authentication in Service Fabric | Audit |
| Diagnostic logs in Service Bus | AuditIfNotExists |
| Diagnostic logs in Virtual Machines Scale Sets | AuditIfNotExists |
| Diagnostic logs in Batch accounts | AuditIfNotExists |
| Metric alert rules in Batch accounts | AuditIfNotExists |
| Service Bus namespace authorization rules | Audit |
| Use of Classic Virtual Machines | Audit |

Network (4 out of 4 policies enabled)

Data (12 out of 12 policies enabled)

Identity (10 out of 10 policies enabled)

| | |
|-------------------------------------|------------------|
| Limit subscription owners to 3 | AuditIfNotExists |
| Set additional subscription owner | AuditIfNotExists |
| Set MFA for owner permissions | AuditIfNotExists |
| Set MFA for write permissions | AuditIfNotExists |
| Set MFA for read permissions | AuditIfNotExists |
| Remove deprecated accounts | AuditIfNotExists |
| Remove deprecated accounts (owners) | AuditIfNotExists |

This **Security policy** screen reflects the action taken by the policies assigned on the subscription or management group you selected.

- Use the links at the top to open a policy **assignment** that applies on the subscription or management group. These links let you access the assignment and edit or disable the policy. For example, if you see that a particular policy assignment is effectively denying endpoint protection, use the link to edit or disable the policy.
- In the list of policies, you can see the effective application of the policy on your subscription or management group. The settings of each policy that apply to the scope are taken into consideration and the cumulative outcome of actions taken by the policy is shown. For example, if in one assignment of the policy is disabled, but in another it's set to AuditIfNotExist, then the cumulative effect applies AuditIfNotExist. The more active effect always takes precedence.
- The policies' effect can be: Append, Audit, AuditIfNotExists, Deny, DeployIfNotExists, Disabled. For more information on how effects are applied, see [Understand Policy effects](#).

NOTE

When you view assigned policies, you can see multiple assignments and you can see how each assignment is configured on its own.

Who can edit security policies?

You can edit security policies through the Azure Policy portal, via REST API or using Windows PowerShell.

Security Center uses Role-Based Access Control (RBAC), which provides built-in roles that can be assigned to users, groups, and services in Azure. When users open Security Center, they see only information that's related to resources they have access to. Which means that users are assigned the role of *owner*, *contributor*, or *reader* to the resource's subscription. As well as these roles, there are two specific Security Center roles:

- **Security reader:** Have view rights to Security Center, which includes recommendations, alerts, policy, and health, but they can't make changes.
- **Security admin:** Have the same view rights as *security reader*, and they can also update the security policy and dismiss recommendations and alerts.

Disable security policies

If the default security policy is generating a recommendation that's not relevant for your environment, you can stop it by disabling the policy definition that sends the recommendation. For more information about recommendations, see [Managing security recommendations](#).

1. In the Security Center, from the **Policy & Compliance** section, click **Security policy**.

| NAME | COVERAGE | SETTINGS |
|----------------------------------|----------|------------------------------------|
| Visual Studio Ultimate with MSDN | Partial | Edit settings > |

2. Click the subscription or management group for which you want to disable the recommendation.

NOTE

Remember that a management group applies its policies to its subscriptions. Therefore, if you disable a subscription's policy, and the subscription belongs to a management group that still uses the same policy, then you will continue to receive the policy recommendations. The policy will still be applied from the management level and the recommendations will still be generated.

3. Click **View effective policy**.

Security policy

ASC DEMO

Security policy on: ASC DEMO

Policies assigned in this subscription

^  Security center default policy

ASC default (1) This is the default policy for Azure Security Center recommendations which is enabled by default on your subscription.

[View effective policy](#) 

- Click the assigned policy.

Home > Security Center - Security policy > Security policy

Security policy
ASC DEMO

Security policies are displayed with their effect as defined through Azure Policy. Learn more →

The selected subscription has 1 security policy assignments. The overall effective policies in Security Center are displayed below.

In order to configure a specific policy assignment, choose one of the assignments below:

 [Preview]: Enable Monitoring in Azure Security Center

The following security policies are assessed and displayed in Security Center:

| Compute And Apps (29 out of 29 policies enabled) | |
|---|--|
| Virtual machines endpoint protection ⓘ |  AuditIfNotExists |
| Virtual machines system updates ⓘ |  AuditIfNotExists |
| Virtual machines security configurations ⓘ |  AuditIfNotExists |
| Virtual machine scale sets OS vulnerabilities ⓘ |  AuditIfNotExists |
| Virtual machine scale sets endpoint protection ⓘ |  AuditIfNotExists |
| Virtual machine scale sets system updates ⓘ |  AuditIfNotExists |
| Disk encryption ⓘ |  AuditIfNotExists |
| Vulnerability Assessment ⓘ |  AuditIfNotExists |
| Adaptive Application Controls ⓘ |  AuditIfNotExists |
| Cluster protection level in Service Fabric ⓘ |  Audit |
| Azure Active Directory authentication in Service Fabric ⓘ |  Audit |
| Diagnostic logs in Service Bus ⓘ |  AuditIfNotExists |

- In the **PARAMETERS** section, search for the policy that invokes the recommendation that you want to disable, and from the dropdown list, select **Disabled**

ASC Default (subscription: a8b45ee3-d6c6-4617-95c1-1d19303c502b)

Edit Initiative Assignment

Assigned by

Security Center

PARAMETERS

* Monitor virtual machine scale sets system updates ⓘ

Disabled

AuditIfNotExists

Disabled

* Monitor virtual machine scale sets OS vulnerabilities ⓘ

AuditIfNotExists

* Monitor system updates ⓘ

AuditIfNotExists

* Monitor OS vulnerabilities ⓘ

AuditIfNotExists

* Monitor endpoint protection ⓘ

AuditIfNotExists

* Monitor disk encryption ⓘ

AuditIfNotExists

* Monitor network security groups ⓘ

AuditIfNotExists

* Monitor web application firewall ⓘ

AuditIfNotExists

* Enable Next Generation Firewall (NGFW) monitoring ⓘ

AuditIfNotExists

* Monitor vulnerability assessment ⓘ

AuditIfNotExists

6. Click **Save**.**NOTE**

The disable policy changes can take up to 12 hours to take effect.

Next steps

In this article, you learned about security policies. For related information, see the following articles:

- For instructions on how to set policies using PowerShell, see [Quickstart: Create a policy assignment to identify non-compliant resources using the Azure PowerShell module](#)
- For instructions on how to edit a security policy in Azure Policy, see [Create and manage policies to enforce compliance](#).
- For instructions on how to set a policy across subscriptions or on Management groups using Azure Policy, see [What is Azure Policy?](#)

Azure security policies monitored by Security Center

2/25/2020 • 9 minutes to read • [Edit Online](#)

This article provides a list of [Azure Policy](#) definitions and initiatives that you can monitor in Azure Security Center. For more information about security policies, see [Working with security policies](#).

Built-in policy definitions

To learn about the built-in policies that are monitored by Security Center, see the following table:

| Name | Description | Effect(s) | Version | Source |
|--|--|----------------------------|---------------|------------------------|
| [Preview] Vulnerability Assessment should be enabled on Virtual Machines | Monitors vulnerabilities detected by Azure Security Center Vulnerability Assessment on Virtual Machines | AuditIfNotExists, Disabled | 1.0.0-preview | GitHub |
| [Preview]: Authorized IP ranges should be defined on Kubernetes Services | Restrict access to the Kubernetes Service Management API by granting API access only to IP addresses in specific ranges. It is recommended to limit access to authorized IP ranges to ensure that only applications from allowed networks can access the cluster. | Audit, Disabled | 1.0.0-preview | GitHub |
| [Preview]: IP Forwarding on your virtual machine should be disabled | Enabling IP forwarding on a virtual machine's NIC allows the machine to receive traffic addressed to other destinations. IP forwarding is rarely required (e.g., when using the VM as a network virtual appliance), and therefore, this should be reviewed by the network security team. | AuditIfNotExists, Disabled | 1.0.0-preview | GitHub |

| Name | Description | Effect(s) | Version | Source |
|--|---|----------------------------|---------------|------------------------|
| [Preview]: Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version | Upgrade your Kubernetes service cluster to a later Kubernetes version to protect against known vulnerabilities in your current Kubernetes version. Vulnerability CVE-2019-9946 has been patched in Kubernetes versions 1.11.9+, 1.12.7+, 1.13.5+, and 1.14.0+ | Audit, Disabled | 1.0.0-preview | GitHub |
| [Preview]: Pod Security Policies should be defined on Kubernetes Services | Define Pod Security Policies to reduce the attack vector by removing unnecessary application privileges. It is recommended to configure Pod Security Policies to only allow pods to access the resources which they have permissions to access. | Audit, Disabled | 1.0.0-preview | GitHub |
| [Preview]: Role-Based Access Control (RBAC) should be used on Kubernetes Services | To provide granular filtering on the actions that users can perform, use Role-Based Access Control (RBAC) to manage permissions in Kubernetes Service Clusters and configure relevant authorization policies. | Audit, Disabled | 1.0.0-preview | GitHub |
| A maximum of 3 owners should be designated for your subscription | It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| A security contact email address should be provided for your subscription | Enter an email address to receive notifications when Azure Security Center detects compromised resources | AuditIfNotExists, Disabled | 1.0.0 | GitHub |

| Name | Description | Effect(s) | Version | Source |
|---|--|----------------------------|---------|------------------------|
| A security contact phone number should be provided for your subscription | Enter a phone number to receive notifications when Azure Security Center detects compromised resources | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| Access through Internet facing endpoint should be restricted | Azure Security center has identified some of your Network Security Groups' inbound rules to be too permissive. Inbound rules should not allow access from 'Any' or 'Internet' ranges. This can potentially enable attackers to easily target your resources. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| Adaptive Application Controls should be enabled on virtual machines | Possible Application Whitelist configuration will be monitored by Azure Security Center | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| Adaptive Network Hardening recommendations should be applied on internet facing virtual machines | Azure Security Center analyzes the traffic patterns of Internet facing virtual machines and provides Network Security Group rule recommendations that reduce the potential attack surface | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| Automatic provisioning of the Log Analytics monitoring agent should be enabled on your subscription | Enable automatic provisioning of the Log Analytics monitoring agent in order to collect security data | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| DDoS Protection Standard should be enabled | DDoS protection standard should be enabled for all virtual networks with a subnet that is part of an application gateway with a public IP. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |

| NAME | DESCRIPTION | EFFECT(S) | VERSION | SOURCE |
|---|--|-------------------------------|---------|------------------------|
| Deprecated accounts should be removed from your subscription | Deprecated accounts should be removed from your subscriptions. Deprecated accounts are accounts that have been blocked from signing in. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| Deprecated accounts with owner permissions should be removed from your subscription | Deprecated accounts with owner permissions should be removed from your subscription. Deprecated accounts are accounts that have been blocked from signing in. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| Disk encryption should be applied on virtual machines | VMs without an enabled disk encryption will be monitored by Azure Security Center as recommendations | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| Email notification for high severity alerts should be enabled | Enable emailing security alerts to the security contact, in order to have them receive security alert emails from Microsoft. This ensures that the right people are aware of any potential security issues and are able to mitigate the risks | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| Email notification to subscription owner for high severity alerts should be enabled | Enable emailing security alerts to the subscription owner, in order to have them receive security alert emails from Microsoft. This ensures that they are aware of any potential security issues and can mitigate the risk in a timely fashion | AuditIfNotExists, Disabled | 1.0.0 | GitHub |

| Name | Description | Effect(s) | Version | Source |
|---|--|----------------------------|---------|------------------------|
| Enable Azure Security Center on your subscription | Identifies existing subscriptions that are not monitored by Azure Security Center (ASC). Subscriptions not monitored by ASC will be registered to the free pricing tier. Subscriptions already monitored by ASC (free or standard), will be considered compliant. To register newly created subscriptions, open the compliance tab, select the relevant non-compliant assignment and create a remediation task. Repeat this step when you have one or more new subscriptions you want to monitor with Security Center. | deployIfNotExists | 1.0.0 | GitHub |
| Endpoint protection solution should be installed on virtual machine scale sets | Audit the existence and health of an endpoint protection solution on your virtual machines scale sets, to protect them from threats and vulnerabilities. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| External accounts with owner permissions should be removed from your subscription | External accounts with owner permissions should be removed from your subscription in order to prevent unmonitored access. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| External accounts with read permissions should be removed from your subscription | External accounts with read privileges should be removed from your subscription in order to prevent unmonitored access. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| External accounts with write permissions should be removed from your subscription | External accounts with write privileges should be removed from your subscription in order to prevent unmonitored access. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |

| Name | Description | Effect(s) | Version | Source |
|---|--|----------------------------|---------|------------------------|
| Internet-facing virtual machines should be protected with Network Security Groups | Protect your VM from potential threats by restricting access to it with a Network Security Group (NSG). To learn more about controlling traffic with NSGs, visit https://aka.ms/nsg-doc | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| Just-In-Time network access control should be applied on virtual machines | Possible network Just In Time (JIT) access will be monitored by Azure Security Center as recommendations | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| Management ports should be closed on your virtual machines | Open remote management ports are exposing your VM to a high level of risk from Internet-based attacks. These attacks attempt to brute force credentials to gain admin access to the machine. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| MFA should be enabled accounts with write permissions on your subscription | Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| MFA should be enabled on accounts with owner permissions on your subscription | Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| MFA should be enabled on accounts with read permissions on your subscription | Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with read privileges to prevent a breach of accounts or resources. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |

| Name | Description | Effect(s) | Version | Source |
|--|---|----------------------------|---------------|------------------------|
| Monitor missing Endpoint Protection in Azure Security Center | Servers without an installed Endpoint Protection agent will be monitored by Azure Security Center as recommendations | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| Security Center standard pricing tier should be selected | The standard pricing tier enables threat detection for networks and virtual machines, providing threat intelligence, anomaly detection, and behavior analytics in Azure Security Center | Audit, Disabled | 1.0.0 | GitHub |
| Sensitive data in your SQL databases should be classified | Azure Security Center monitors the data discovery and classification scan results for your SQL databases and provides recommendations to classify the sensitive data in your databases for better monitoring and security | AuditIfNotExists, Disabled | 1.0.0-preview | GitHub |
| Subnets should be associated with a Network Security Group | Protect your subnet from potential threats by restricting access to it with a Network Security Group (NSG). NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to your subnet. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| System updates on virtual machine scale sets should be installed | Audit whether there are any missing system security updates and critical updates that should be installed to ensure that your Windows and Linux virtual machine scale sets are secure. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |

| Name | Description | Effect(s) | Version | Source |
|---|---|----------------------------|---------|------------------------|
| System updates should be installed on your machines | Missing security system updates on your servers will be monitored by Azure Security Center as recommendations | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| There should be more than one owner assigned to your subscription | It is recommended to designate more than one subscription owner in order to have administrator access redundancy. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| Vulnerabilities in container security configurations should be remediated | Audit vulnerabilities in security configuration on machines with Docker installed and display as recommendations in Azure Security Center. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| Vulnerabilities in security configuration on your machines should be remediated | Servers which do not satisfy the configured baseline will be monitored by Azure Security Center as recommendations | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| Vulnerabilities in security configuration on your virtual machine scale sets should be remediated | Audit the OS vulnerabilities on your virtual machine scale sets to protect them from attacks. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| Vulnerabilities on your SQL databases should be remediated | Monitor Vulnerability Assessment scan results and recommendations for how to remediate database vulnerabilities. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |
| Vulnerabilities should be remediated by a Vulnerability Assessment solution | Monitors vulnerabilities detected by Vulnerability Assessment solution and VMs without a Vulnerability Assessment solution in Azure Security Center as recommendations. | AuditIfNotExists, Disabled | 1.0.0 | GitHub |

Built-in policy initiatives

To learn about the built-in initiatives that are monitored by Security Center, see the following table:

| NAME | DESCRIPTION | POLICIES | VERSION |
|---|--|----------|---------------|
| [Preview]: Enable Data Protection Suite | Enable data protection for SQL servers. This initiative is assigned automatically by Azure Security Center Standard Tier. | 1 | 1.0.0-preview |
| [Preview]: Enable Monitoring in Azure Security Center | Monitor all the available security recommendations in Azure Security Center. This is the default policy for Azure Security Center. | 96 | 2.0.0-preview |

Next steps

In this article, you learned about Azure Policy security policy definitions in Security Center. To learn more, see the following articles.

- [Azure Security Center planning and operations guide](#): Learn how to plan and understand design considerations in Azure Security Center.
- [Security health monitoring in Azure Security Center](#): Learn how to monitor the health of your Azure resources.
- [Manage and respond to security alerts in Azure Security Center](#): Learn how to manage and respond to security alerts.
- [Monitor partner solutions with Azure Security Center](#): Learn how to monitor the health status of your partner solutions.
- [Azure Policy](#): Learn to audit and govern your Azure resources.

Using custom security policies (Preview)

1/6/2020 • 2 minutes to read • [Edit Online](#)

To help secure your systems and environment, Azure Security Center generates security recommendations. These recommendations are based on industry best practices, which are incorporated into the generic, default security policy supplied to all customers. They can also come from Security Center's knowledge of industry and regulatory standards.

With this preview feature, you can add your own *custom* initiatives. You'll then receive recommendations if your environment doesn't follow the policies you create. Any custom initiatives you create will appear alongside the built-in initiatives in the regulatory compliance dashboard described in the tutorial [Improve your regulatory compliance](#).

As discussed [here](#) in the Azure Policy documentation, when you specify a location for your custom initiative, it must be a management group or a subscription.

To add a custom initiative to your subscription

1. From Security Center's sidebar, open the **Security policy** page.
2. Select a subscription or Management Group to which you would like to add a custom initiative.

The screenshot shows the Microsoft Azure Security Center - Security policy page. The left sidebar includes links for Overview, Getting started, Pricing & settings, Coverage, Secure score, Security policy (which is selected), Regulatory compliance, Recommendations, and Compute & apps. The main content area features a "Policy Management" section with a "Policy Management" icon and a brief description: "Manage the security policies by choosing a subscription or management group from the list below. In order to define additional policies, manage exclusions and advanced settings, go to Azure policies >". Below this is a summary: "11 MANAGEMENT GROUPS 1 SUBSCRIPTIONS". A search bar labeled "Search by name" is present. A list of management groups is shown, with "ASC DEMO" highlighted with a cursor icon.

NOTE

You must add custom standards at the subscription level (or higher) for them to be evaluated and displayed in Security Center.

When you add a custom standard, it assigns an *initiative* to that scope. We therefore recommend that you select the widest scope required for that assignment.

3. In the Security policy page, under Your custom initiatives (Preview), click **Add a custom initiative**.

Microsoft Azure

Home > Security Center - Security policy > Security policy

Security policy

DEMO X

Security policy on: DEMO

Policies assigned in this subscription

- ▼  Security center default policy
- ▼  Industry & regulatory standards (preview)
- ^  Your custom initiatives (preview)

Custom initiative policies which you have created which are available in the **Recommendations** blade.
To add another custom initiative policy click **Add a custom initiative**.

[Add a custom initiative](#)

The following page appears:

Add custom initiatives

[Create new](#)  Refresh

To create a new [Custom policy initiative](#), click **Create new**.
Or, to add an existing initiative from the list below, click **Add** in the relevant row.
After adding the policy initiative, it will be listed as a recommendation in the **Recommendations** blade, and to have it added in the **Regulatory compliance** dashboard.

(i) If the initiative is not already assigned on this subscription, after clicking **Add**, be sure to assign the initiative on the subscription.

| NAME | DESCRIPTION | STATUS | |
|-----------------------|---------------|--------------|---|
| Organizational policy | custom policy | Not assigned | Add |

4. In the Add custom initiatives page, review the list of custom policies already created in your organization. If you see one you want to assign to your subscription, click **Add**. If there isn't an initiative in the list that meets your needs, skip this step.
5. To create a new custom initiative:
 - a. Click **Create new**.
 - b. Enter the definition's location and name.
 - c. Select the policies to include and click **Add**.
 - d. Enter any desired parameters.
 - e. Click **Save**.
 - f. In the Add custom initiatives page, click refresh and your new initiative will be shown as available.
 - g. Click **Add** and assign it to your subscription.

NOTE

Creating new initiatives requires subscription owner credentials. For more information about Azure roles, see [Permissions in Azure Security Center](#).

Your new initiative takes effect and you can see the impact in the following two ways:

- From the Security Center sidebar, under Policy & Compliance, select **Regulatory compliance**. The

compliance dashboard opens to show your new custom initiative alongside the built-in initiatives.

- You'll begin to receive recommendations if your environment doesn't follow the policies you've defined.
6. To see the resulting recommendations for your policy, click **Recommendations** from the sidebar to open the recommendations page. The recommendations will appear with a "Custom" label and be available within approximately one hour.

| Search recommendations | |
|--|--------|
| Recommendation | ↑↓ |
| [Preview]: Show audit results from Windows VMs that do not have a minimum password age of 1 day | Custom |
| [Preview]: Show audit results from Windows VMs that do not have a maximum password age of 70 days | Custom |
| [Preview]: Show audit results from Windows VMs that allow re-use of the previous 24 passwords | Custom |
| [Preview]: Show audit results from Windows VMs on which the Log Analytics agent is not connected as expected | Custom |

Next steps

In this article, you learned how to create custom security policies.

For other related material, see the following articles:

- [The overview of security policies](#)
- [A list of the built-in security policies](#)

Configure a security policy in Azure Policy using the REST API

2/18/2020 • 2 minutes to read • [Edit Online](#)

As part of the native integration with Azure Policy, Azure Security Center enables you to take advantage of Azure Policy's REST API to create policy assignments. The following instructions walk you through creation of policy assignments, as well as customization of existing assignments.

Important concepts in Azure Policy:

- A **policy definition** is a rule
- An **initiative** is a collection of policy definitions (rules)
- An **assignment** is an application of an initiative or a policy to a specific scope (management group, subscription, etc.)

Security Center has a built-in initiative that includes all of its security policies. To assess Security Center's policies on your Azure resources, you should create an assignment on the management group, or subscription you want to assess.

The built-in initiative has all of Security Center's policies enabled by default. You can choose to disable certain policies from the built-in initiative. For example, to apply all of Security Center's policies except **web application firewall**, change the value of the policy's effect parameter to **Disabled**.

API examples

In the following examples, replace these variables:

- **{scope}** enter the name of the management group or subscription to which you're applying the policy.
- **{policyAssignmentName}** enter the [name of the relevant policy assignment](#).
- **{name}** enter your name, or the name of the administrator who approved the policy change.

This example shows you how to assign the built-in Security Center initiative on a subscription or management group

```
PUT
```

```
https://management.azure.com/{scope}/providers/Microsoft.Authorization/policyAssignments/{policyAssignmentName}  
?api-version=2018-05-01
```

```
Request Body (JSON)
```

```
{  
  "properties":{  
    "displayName":"Enable Monitoring in Azure Security Center",  
    "metadata":{  
      "assignedBy":"{Name}"  
    },  
    "policyDefinitionId":"/providers/Microsoft.Authorization/policySetDefinitions/1f3afdf9-d0c9-4c3d-847f-  
89da613e70a8",  
    "parameters":{}  
  }  
}
```

This example shows you how to assign the built-in Security Center initiative on a subscription, with the following policies disabled:

- System updates ("systemUpdatesMonitoringEffect")
- Security configurations ("systemConfigurationsMonitoringEffect")
- Endpoint protection ("endpointProtectionMonitoringEffect")

```

PUT
https://management.azure.com/{scope}/providers/Microsoft.Authorization/policyAssignments/{policyAssignmentName}
?api-version=2018-05-01

Request Body (JSON)

{
  "properties":{

    "displayName":"Enable Monitoring in Azure Security Center",

    "metadata":{

      "assignedBy":"{Name}"

    },

    "policyDefinitionId":"/providers/Microsoft.Authorization/policySetDefinitions/1f3afdf9-d0c9-4c3d-847f-
89da613e70a8",

    "parameters":{

      "systemUpdatesMonitoringEffect":{"value":"Disabled"},

      "systemConfigurationsMonitoringEffect":{"value":"Disabled"},

      "endpointProtectionMonitoringEffect":{"value":"Disabled"},

    }

  }

}

```

This example shows you how to remove an assignment:

```

DELETE

https://management.azure.com/{scope}/providers/Microsoft.Authorization/policyAssignments/{policyAssignmentName}
?api-version=2018-05-01

```

Policy names reference

| POLICY NAME IN SECURITY CENTER | POLICY NAME DISPLAYED IN AZURE POLICY | POLICY EFFECT PARAMETER NAME |
|--------------------------------|---|-----------------------------------|
| SQL Encryption | Monitor unencrypted SQL database in Azure Security Center | sqlEncryptionMonitoringEffect |
| SQL Auditing | Monitor unaudited SQL database in Azure Security Center | sqlAuditingMonitoringEffect |
| System updates | Monitor missing system updates in Azure Security Center | systemUpdatesMonitoringEffect |
| Storage encryption | Audit missing blob encryption for storage accounts | storageEncryptionMonitoringEffect |

| POLICY NAME IN SECURITY CENTER | POLICY NAME DISPLAYED IN AZURE POLICY | POLICY EFFECT PARAMETER NAME |
|--------------------------------|---|---|
| JIT Network access | Monitor possible network just-in-time (JIT) access in Azure Security Center | jitNetworkAccessMonitoringEffect |
| Adaptive application controls | Monitor possible app Whitelisting in Azure Security Center | adaptiveApplicationControlsMonitoringEffect |
| Network security groups | Monitor permissive network access in Azure Security Center | networkSecurityGroupsMonitoringEffect |
| Security configurations | Monitor OS vulnerabilities in Azure Security Center | systemConfigurationsMonitoringEffect |
| Endpoint protection | Monitor missing Endpoint Protection in Azure Security Center | endpointProtectionMonitoringEffect |
| Disk encryption | Monitor unencrypted VM Disks in Azure Security Center | diskEncryptionMonitoringEffect |
| Vulnerability assessment | Monitor VM Vulnerabilities in Azure Security Center | vulnerabilityAssessmentMonitoringEffect |
| Web application firewall | Monitor unprotected web application in Azure Security Center | webApplicationFirewallMonitoringEffect |
| Next generation firewall | Monitor unprotected network endpoints in Azure Security Center | |

Next steps

For other related material, see the following articles:

- [Custom security policies](#)
- [Security policy overview](#)

Update to dynamic compliance packages in your Regulatory Compliance dashboard (Preview)

2/25/2020 • 2 minutes to read • [Edit Online](#)

Azure Security Center continually compares the configuration of your resources with requirements in industry standards, regulations, and benchmarks. The **regulatory compliance dashboard** provides insights into your compliance posture based on how you're meeting specific compliance controls and requirements.

One standard for which you can track your compliance posture is [Azure CIS 1.1.0](#) (more formally, the "CIS Microsoft Azure Foundations Benchmark version 1.1.0").

The representation of Azure CIS that initially appears in your compliance dashboard relies on a static set of rules that is included with Security Center.

With the **dynamic compliance packages (preview)** feature, Security Center automatically improves its coverage of industry standards over time. Compliance packages are essentially initiatives defined in Azure Policy. They can be assigned to your selected scope (subscription, management group, and so on). To see compliance data mapped as assessments in your dashboard, add a compliance package to your management group or subscription from within the Security Policy. Adding a compliance package effectively assigns the regulatory compliance initiative to your selected scope. In this way, you can track newly published regulatory initiatives as compliance standards in your dashboard. When Microsoft releases new content for the initiative (new policies that map to more controls in the standard), the additional content appears automatically in your dashboard.

The dynamic compliance package for the Azure CIS benchmark, [Azure CIS 1.1.0 \(new\)](#), improves on the original *static* version by:

- Including more policies
- Automatically updating with new coverage as it's added

Update to the new dynamic package as described below.

Adding a dynamic compliance package

The following steps explain how to add the dynamic package for monitoring your compliance with the Azure CIS benchmark v1.1.0.

Update to the Azure CIS 1.1.0 (new) dynamic compliance package

1. Open the **Security policy** page. This page shows the number of management groups, subscriptions, workspaces, and your management group structure.
2. Select the subscription or management group for which you want to manage the regulatory compliance posture. We recommend selecting the highest scope for which the standard is applicable so that compliance data is aggregated and tracked for all nested resources.
3. In the Industry & regulatory standards (preview) section, you'll see that Azure CIS 1.1.0 can be updated for new content. Click **Update now**.
4. Optionally, click **Add more standards** to open the **Add regulatory compliance standards** page. There, you can search manually for [Azure CIS 1.1.0 \(New\)](#) and dynamic packages for other compliance standards such as **NIST SP 800-53 R4**, **SWIFT CSP CSCF-v2020**, **UKO and UK NHS**, and **Canada PBMM**.

Dashboard > Security Center - Security policy > Security policy > Add regulatory compliance standards

Add regulatory compliance standards

Click **Add** on the standards that you want to add to the regulatory compliance dashboard and then assign it to the subscription. After completing the assignment , the custom policies will be available in the **Regulatory compliance** dashboard.

| Search to filter items... | | NAME | DESCRIPTION | |
|---------------------------|--|------------------------|--|----------------------|
| <input type="checkbox"/> | | NIST SP 800-53 R4 | Track NIST SP 800-53 R4 controls in the Compliance Dashboard, based on a recomm... | <button>Add</button> |
| <input type="checkbox"/> | | UK OFFICIAL and UK NHS | Track UK OFFICIAL and UK NHS controls in the Compliance Dashboard, based on a r... | <button>Add</button> |
| <input type="checkbox"/> | | Canada Federal PBMM | Track Canada Federal PBMM controls in the Compliance Dashboard, based on a rec... | <button>Add</button> |
| <input type="checkbox"/> | | Azure CIS 1.1.0 (New) | Track Azure CIS 1.1.0 (New) controls in the Compliance Dashboard, based on a reco... | <button>Add</button> |
| <input type="checkbox"/> | | SWIFT CSP CSCF v2020 | Track SWIFT CSP CSCF v2020 controls in the Compliance Dashboard, based on a rec... | <button>Add</button> |

- From Security Center's sidebar, select **Regulatory compliance** to open the regulatory compliance dashboard.

- Azure CIS 1.1.0 (New) now appears in your list of Industry & regulatory standards.
- The original *static* view of your Azure CIS 1.1.0 compliance will also remain alongside it. It may be automatically removed in the future.

NOTE

It may take a few hours for a newly added standard to appear in the compliance dashboard.

Microsoft Azure (Preview) Report a bug Search resources, services, and docs (G+)

Dashboard > Security Center - Overview > Regulatory Compliance

Regulatory Compliance

Download report Manage compliance policies

Regulatory compliance assessment

| TOTAL | Failed | Passed | Skipped |
|-------|--------|--------|---------|
| 372 | 155 | 216 | 1 |

Regulatory standards compliance status

| Standard | Passed Controls | Total Controls |
|-----------------|-----------------|-----------------|
| Azure CIS 1.1.0 | 10 of 24 | passed controls |
| PCI DSS 3.2.1 | 3 of 43 | passed controls |
| ISO 27001 | 1 of 21 | passed controls |
| SOC TSP | 0 of 13 | passed controls |

Regulatory compliance

View your compliance posture relative to the standards and regulations that are important to you. Remediate assessments to watch your compliance posture improve.

Learn more >

Azure CIS 1.1.0 PCI DSS 3.2.1 ISO 27001 SOC TSP Azure CIS 1.1.0 (New)

Under each applicable compliance control is the set of assessments run by Security Center that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Security Center assessments, and therefore this report is only a partial view of your overall compliance status.

Expand all compliance controls

1. Identity and Access Management
2. Security Center
3. Storage Accounts
4. Database Services
5. Logging and Monitoring
6. Networking

Next steps

In this article, you learned:

- How to **upgrade the standards** shown in your regulatory compliance dashboard to the new *dynamic* packages
- How to **add compliance packages** to monitor your compliance with additional standards.

For other related material, see the following articles:

- [Security center regulatory compliance dashboard](#)
- [Working with security policies](#)

- [Managing security recommendations in Azure Security Center](#) - Learn how to use recommendations in Azure Security Center to help protect your Azure resources.

Customize the SQL information protection policy in Azure Security Center (Preview)

1/2/2020 • 4 minutes to read • [Edit Online](#)

You can define and customize an SQL information protection policy for your entire Azure tenant, in Azure Security Center.

Information protection is an advanced security capability for discovering, classifying, labeling, and reporting sensitive data in your Azure data resources. Discovering and classifying your most sensitive data (business, financial, healthcare, personal data, etc.) can play a pivotal role in your organizational information protection stature. It can serve as infrastructure for:

- Helping meet data privacy standards and regulatory compliance requirements
- Security scenarios such as monitoring (auditing) and alerting on anomalous access to sensitive data
- Controlling access to and hardening the security of data stores containing highly sensitive data

[SQL Information Protection](#) implements this paradigm for your SQL data stores, currently supported for Azure SQL Database. SQL Information Protection automatically discovers and classifies potentially sensitive data, provides a labeling mechanism for persistently tagging the sensitive data with classification attributes, and provides a detailed dashboard showing the classification state of the database. In addition, it calculates the result set sensitivity of SQL queries, so that queries that extract sensitive data can be explicitly audited, and the data can be protected. For more information on SQL Information Protection, see [Azure SQL Database Data Discovery and Classification](#).

The classification mechanism is based on two primary constructs that make up the classification taxonomy - **Labels** and **Information Types**.

- **Labels** – The main classification attributes, used to define the sensitivity level of the data stored in the column.
- **Information Types** – Provides additional granularity into the type of data stored in the column.

Information Protection comes with a built-in set of labels and information types, which are used by default. To customize these labels and types, you can customize the information protection policy in Security Center.

Customize the information protection policy

To customize the information protection policy for your Azure tenant, you need to have [administrative privileges on the tenant's root management group](#).

1. In the Security Center main menu, under **RESOURCE SECURITY HYGIENE** go to **Data & storage** and click on the **SQL Information Protection** button.

The screenshot shows the Azure Security Center - Data & storage interface. The left sidebar has a search bar and navigation sections for Policy & Compliance (Coverage, Secure score, Regulatory compliance, Security policy), Resource Security Hygiene (Recommendations, Compute & apps, IoT hubs & resources, Networking), and Data & storage. The 'Data & storage' section is highlighted with a red box. The main content area is titled 'SQL Information Protection' and shows an 'Overview' with three green checkmarks. Below is a table of recommendations:

| RECOMMENDATION | SE... |
|----------------------------------|-------|
| Require secure transfer to st... | +19 |
| Provision an Azure AD adm... | +15 |
| Migrate storage accounts to... | +10 |
| Enable Advanced data securi... | +8 |
| Enable auditing on SQL server | +5 |
| Restrict access to storage ac... | +5 |

2. In the **SQL Information Protection** page, you can view your current set of labels. These are the main classification attributes that are used to categorize the sensitivity level of your data. From here, you can configure the **Information protection labels** and **Information types** for the tenant.

Customizing labels

1. You can edit or delete any existing label, or add a new label. To edit an existing label, select that label and then click **Configure**, either at the top or from the context menu on the right. To add a new label, click **Create label** in the top menu bar or at the bottom of the labels table.
2. In the **Configure sensitivity label** screen, you can create or alter the label name and the description. You can also set whether the label is active or disabled by toggling the **Enabled** switch on or off. Finally, you can add or remove information types associated with the label. Any data discovered that matches that information type will automatically include the associated sensitivity label in the classification recommendations.
3. Click **OK**.

Configure sensitivity label

□ X

Enabled

* Label name

Confidential - GDPR

* Description

Sensitive data containing personal information associated with an individual, that could be misused in the hands of unauthorized people

Configure information types for automatically applying this label

If any of these information types are identified, this label is applied.

Date Of Birth



Contact Info



National ID



SSN



4. Labels are listed in order of ascending sensitivity. To change the ranking between labels, drag the labels to reorder them in the table, or use the **Move up** and **Move down** buttons to change the order.

[Save](#)[Discard](#)[Create label](#)[Manage information types](#)

Create and manage sensitivity labels

Drag labels to order in ascending sensitivity

[Configure](#)[Move up](#)[Move down](#)[Move to top](#)[Move to bottom](#)[Delete](#)

DISPLAY NAME

DESCRIPTION



Public

Business data that is



General

Business data that is



Confidential

Sensitive business da



Confidential - GDPR

Sensitive data contai



Highly confidential

Very sensitive busine



Highly confidential - GDPR

Sensitive data contai

[Create new label](#)

5. Be sure to click **Save** at the top of the screen when you are finished.

Adding and customizing information types

1. You can manage and customize information types by clicking on **Manage information types**.
2. To add a new **Information type**, select **Create information type** in the top menu. You can configure a name, description, and search pattern strings for the **Information type**. Search pattern strings can optionally use keywords with wildcard characters (using the character '%'), which the automated discovery engine uses to identify sensitive data in your databases, based on the columns' metadata.

The screenshot shows the 'Information types' blade on the left and a 'Configure information type' dialog box on the right.

Information types blade:

- Create and manage information types:** A section where you can drag information types to change their discovery ranking.
- Buttons:** Configure, Move up, Move down, Move to top, Move to bottom.
- Table:** Lists built-in information types with their associated labels.

| INFORMATION TYPE | ASSOCIATED LABEL |
|------------------|---------------------|
| Date Of Birth | Confidential - GDF |
| Contact Info | Confidential - GDF |
| Credentials | Highly confidential |
| Other | Confidential |
| Name | Highly confidential |
| National ID | Confidential - GDF |
| SSN | Confidential - GDF |
| Credit Card | Highly confidential |
| Banking | Highly confidential |
| Financial | Highly confidential |
| Health | Highly confidential |
- OK button:** Located at the bottom left of the main blade.

Configure information type dialog box:

- Enabled:** ON (radio button selected).
- Display name:** HR data (text input field with a green checkmark).
- Description:** Sensitive data from the HR systems (text area).
- Table:** Patterns and their numeric allow settings.

| PATTERN | ALLOW NUMERIC |
|----------|---------------|
| employee | Yes |
| emp%id | Yes |
| %salary% | Yes |
- OK button:** Located at the bottom right of the dialog box.

- You can also configure the built-in **Information types** by adding additional search pattern strings, disabling some of the existing strings, or by changing the description. You cannot delete built-in **Information types** or edit their names.
- Information types** are listed in order of ascending discovery ranking, meaning that the types higher in the list will attempt to match first. To change the ranking between information types, drag the types to the right spot in the table, or use the **Move up** and **Move down** buttons to change the order.
- Click **OK** when you are done.
- After you completed managing your information types, be sure to associate the relevant types with the relevant labels, by clicking **Configure** for a particular label, and adding or deleting information types as appropriate.
- Be sure to click **Save** in the main **Labels** blade to apply all your changes.

After your Information protection policy is fully defined and saved, it will apply to the classification of data on all Azure SQL databases in your tenant.

Next steps

In this article, you learned about defining a SQL Information Protection policy in Azure Security Center. To learn more about using SQL Information Protection to classify and protect sensitive data in your SQL databases, see [Azure SQL Database Data Discovery and Classification](#).

For more information on security policies and data security in Azure Security Center, see the following articles:

- [Setting security policies in Azure Security Center](#): Learn how to configure security policies for your Azure subscriptions and resource groups

- [Azure Security Center data security](#): Learn how Security Center manages and safeguards data

Integrate security solutions in Azure Security Center

2/25/2020 • 4 minutes to read • [Edit Online](#)

This document helps you to manage security solutions already connected to Azure Security Center and add new ones.

NOTE

A subset of security solutions has been retired on July 31st, 2019. For more information and alternative services, see [Retirement of Security Center features \(July 2019\)](#).

Integrated Azure security solutions

Security Center makes it easy to enable integrated security solutions in Azure. Benefits include:

- **Simplified deployment:** Security Center offers streamlined provisioning of integrated partner solutions. For solutions like antimalware and vulnerability assessment, Security Center can provision the agent on your virtual machines. For firewall appliances, Security Center can take care of much of the network configuration required.
- **Integrated detections:** Security events from partner solutions are automatically collected, aggregated, and displayed as part of Security Center alerts and incidents. These events also are fused with detections from other sources to provide advanced threat-detection capabilities.
- **Unified health monitoring and management:** Customers can use integrated health events to monitor all partner solutions at a glance. Basic management is available, with easy access to advanced setup by using the partner solution.

Currently, integrated security solutions include vulnerability assessment by [Qualys](#) and [Rapid7](#) and Microsoft Application Gateway Web application firewall.

NOTE

Security Center does not install the Microsoft Monitoring Agent on partner virtual appliances because most security vendors prohibit external agents running on their appliances.

How security solutions are integrated

Azure security solutions that are deployed from Security Center are automatically connected. You can also connect other security data sources, including computers running on-premises or in other clouds.

Security Center - Security solutions

GENERAL

- Overview
- Security policy
- Quickstart
- Welcome
- Events
- Onboarding to advanced security
- Search

PREVENTION

- Recommendations
- Security solutions**
- Compute
- Networking
- Storage & data
- Applications
- Identity & Access

DETECTION

- Security alerts
- Custom alert rules (Preview)
- Threat intelligence

AUTOMATION & ORCHESTRATION

- Playbooks (Preview)

Connected solutions (3)

View all security solutions currently connected to Azure Security Center, monitor the health of solutions, and access the solutions' management tools for advanced configuration.

| Solution | Health | Action |
|--|--------------|--------|
| QualysVa1 QUALYS, INC. Vulnerability Assessment | Healthy | VIEW |
| CheckPoint-Firewall-Cent... CHECK POINT Next Generation Firewall | Healthy | VIEW |
| Gili-WAF BARRACUDA NETWORKS, INC. Web Application Firewall | Not reported | VIEW |

Discovered solutions (1)

Connect your security solution to Azure Security Center. View, monitor and get notified on solution health and security alerts.

| | |
|---|---------|
| Azure AD Identity Protect... MICROSOFT Azure AD Identity Protection | CONNECT |
|---|---------|

Add data sources (3)

Connect your security solution to Azure Security Center.

| | | | | | |
|--|-----|--|-----|---|-----|
| Non-Azure computers MICROSOFT | ADD | Common Event Format ANY PUBLISHER | ADD | Advanced Threat Analytics MICROSOFT | ADD |
| Onboard your non-Azure computers to Azure Security Center and gain security assessment, recommendations and more powerful features | | Integrate any security solution that support Common Event Format (CEF), take advantage of Search & Custom Alert Rules, and Threat Intelligence enrichment for each log | | Integrate Microsoft Advanced Threat Analytics suspicious activities along with other detections in your environment, and gain correlations and otherwise undetectable | |

Manage integrated Azure security solutions and other data sources

- Sign in to the [Azure portal](#).
- On the **Microsoft Azure menu**, select **Security Center**. **Security Center - Overview** opens.
- Under the Security Center menu, select **Security solutions**.

Security Center - Overview

Showing subscription 'Contoso IT - demo'

GENERAL

- Overview
- Getting started
- Events
- Search

POLICY & COMPLIANCE

- Coverage
- Security policy

RESOURCE SECURITY HYGIENE

- Recommendations
- Compute & apps
- Networking
- Data & storage
- Identity & access (Preview)
- Security solutions**

Policy & compliance

Subscription coverage

| Covered (standard) | Covered (free) | Not covered |
|--------------------|----------------|-------------|
| 1 | 0 | 0 |

288 Covered resources

Policy compliance

Overall compliance: 33%

Least compliant subscriptions: Contoso IT - demo (33%)

Show policy compliance of your environment >

Resource security hygiene

Recommendations

| High Severity | Medium Severity | Low Severity |
|---------------|-----------------|--------------|
| 16 | 11 | 8 |

181 Unhealthy resources

Resource health monitoring

| Compute & apps | Data & storage | Networking | Identity & access |
|----------------|----------------|------------|-------------------|
| 132 | 99 | 56 | 1 |

In **Security solutions**, you can see the health of integrated Azure security solutions and run basic management tasks.

Connected solutions

The **Connected solutions** section includes security solutions that are currently connected to Security Center. It also shows the health status of each solution.

Connected solutions (4)

View all partner solutions currently connected to Azure Security Center, monitor the health of solutions, and access the solution's management tools for advanced configuration.

| | | | |
|---|--|--|---|
|  ASC Windows agent Microsoft ⚠ 9 of 10 VMs & computers reporting |  Linux agent Microsoft ⚠ 7 of 9 VMs & computers reporting |  Advanced Threat Analytics Microsoft ✓ Healthy |  F5 BIG-IP WAF BYOL F5 Networks ⚠ Partially unhealthy Missing protected resources. Add > |
| VIEW | VIEW | VIEW | VIEW |

The status of a partner solution can be:

- Healthy (green) - no health issues.
- Unhealthy (red) - there's a health issue that requires immediate attention.
- Health issues (orange) - the solution has stopped reporting its health.
- Not reported (gray) - the solution hasn't reported anything yet and no health data is available. A solution's status may be unreported if it was connected recently and is still deploying.

NOTE

If health status data is not available, Security Center shows the date and time of the last event received to indicate whether the solution is reporting or not. If no health data is available and no alerts were received within the last 14 days, Security Center indicates that the solution is unhealthy or not reporting.

1. Select **VIEW** for additional information and options such as:

- **Solution console.** Opens the management experience for this solution.
- **Link VM.** Opens the Link Applications page. Here you can connect resources to the partner solution.
- **Delete solution.**
- **Configure.**

Qualys

Solution console Link VM Delete solution Configure

| | |
|-----------------------|--------------------------------|
| PARTNER SOLUTION NAME | Qualys for Azure |
| TYPE | Vulnerability Assessment |
| INTEGRATION MODE | Semi-automatically provisioned |
| STATUS | Healthy |

Note: Agent status may have up to 8 hours delay

Associated resources

| RESOURCE NAME | HEALTH |
|---------------|----------------------|
| vm1 | Green checkmark |
| vm3 | Red exclamation mark |

Discovered solutions

Security Center automatically discovers security solutions running in Azure but not connected to Security Center and displays the solutions in the **Discovered solutions** section. These solutions include Azure solutions, like [Azure AD Identity Protection](#), and partner solutions.

NOTE

The Standard tier of Security Center is required at the subscription level for the discovered solutions feature. See [Pricing](#) to learn more about the pricing tiers.

Select **CONNECT** under a solution to integrate with Security Center and be notified of security alerts.

Add data sources

The **Add data sources** section includes other available data sources that can be connected. For instructions on adding data from any of these sources, click **ADD**.

▼ Add data sources (3)

Connect your security solution to Azure Security Center. Monitor, analyze your data and configure custom alert rules.



Non-Azure Computers

MICROSOFT

Onboard your non-Azure servers to Azure Security Center and gain security assessment, recommendations, and more powerful features

ADD



Common Event Format

ANY PUBLISHER

Integrate any security solution that emits Common Event Format and take advantage of Search & Custom Alert Rules and Threat Intelligence enrichment for each log

ADD



Advanced Threat Analytics

MICROSOFT

Integrate Microsoft Advanced Threat Analytics suspicious activities along with other detections in your environment and gain correlations and otherwise undetectable

ADD

Exporting data to a SIEM

NOTE

For details of a simpler method (currently in preview) for exporting data to a SIEM, see [Export security alerts and recommendations \(Preview\)](#). The new method does not use Activity Log as an intermediary and allows direct export from Security Center to Event Hubs (and then on to your SIEM), it also supports the export of Security Recommendations.

You can configure your SIEMs or other monitoring tools to receive Azure Security Center events.

All events from Azure Security Center are published to Azure Monitor's Azure [Activity log](#). Azure Monitor uses [a consolidated pipeline](#) to stream the data to an Event Hub where it can then be pulled into your monitoring tool.

The next sections describe how you can configure data to be streamed to an event hub. The steps assume that you already have Azure Security Center configured in your Azure subscription.

High-level overview



What is the Azure security data exposed to SIEM?

In this version, we expose the [security alerts](#). In upcoming releases, we will enrich the data set with security recommendations.

How to set up the pipeline

Create an Event Hub

Before you begin, [create an Event Hubs namespace](#) - the destination for all your monitoring data.

Stream the Azure Activity Log to Event Hubs

See the following article [stream activity log to Event Hubs](#).

Install a partner SIEM connector

Routing your monitoring data to an Event Hub with Azure Monitor enables you to easily integrate with partner SIEM and monitoring tools.

See the following article for the list of [supported SIEMs](#).

Example for Querying data

Here are some Splunk queries you can use to pull alert data:

| DESCRIPTION OF QUERY | QUERY |
|--|--|
| All Alerts | index=main Microsoft.Security/locations/alerts |
| Summarize count of operations by their name | index=main sourcetype="amal:security" table operationName stats count by operationName |
| Get Alerts info: Time, Name, State, ID, and Subscription | index=main Microsoft.Security/locations/alerts table _time, properties.eventName, State, properties.operationId, am_subscriptionId |

Next steps

In this article, you learned how to integrate partner solutions in Security Center. To learn more about Security Center, see the following article:

- [Security health monitoring in Security Center](#). Learn how to monitor the health of your Azure resources.

Automate onboarding of Azure Security Center using PowerShell

2/25/2020 • 2 minutes to read • [Edit Online](#)

You can secure your Azure workloads programmatically, using the Azure Security Center PowerShell module. Using PowerShell enables you to automate tasks and avoid the human error inherent in manual tasks. This is especially useful in large-scale deployments that involve dozens of subscriptions with hundreds and thousands of resources – all of which must be secured from the beginning.

Onboarding Azure Security Center using PowerShell enables you to programmatically automate onboarding and management of your Azure resources and add the necessary security controls.

This article provides a sample PowerShell script that can be modified and used in your environment to roll out Security Center across your subscriptions.

In this example, we will enable Security Center on a subscription with ID: d07c0080-170c-4c24-861d-9c817742786c and apply the recommended settings that provide a high level of protection, by implementing the Standard tier of Security Center, which provides advanced threat protection and detection capabilities:

1. Set the [Security Center standard level of protection](#).
2. Set the Log Analytics workspace to which the Microsoft Monitoring Agent will send the data it collects on the VMs associated with the subscription – in this example, an existing user defined workspace (myWorkspace).
3. Activate Security Center's automatic agent provisioning which [deploys the Microsoft Monitoring Agent](#).
4. Set the organization's [CISO as the security contact for Security Center alerts and notable events](#).
5. Assign Security Center's [default security policies](#).

Prerequisites

These steps should be performed before you run the Security Center cmdlets:

1. Run PowerShell as admin.
2. Run the following commands in PowerShell:

```
Set-ExecutionPolicy -ExecutionPolicy AllSigned  
Install-Module -Name Az.Security -Force
```

Onboard Security Center using PowerShell

1. Register your subscriptions to the Security Center Resource Provider:

```
Set-AzContext -Subscription "d07c0080-170c-4c24-861d-9c817742786c"  
Register-AzResourceProvider -ProviderNamespace 'Microsoft.Security'
```

2. Optional: Set the coverage level (pricing tier) of the subscriptions (If not defined, the pricing tier is set to Free):

```
Set-AzContext -Subscription "d07c0080-170c-4c24-861d-9c817742786c"
Set-AzSecurityPricing -Name "default" -PricingTier "Standard"
```

3. Configure a Log Analytics workspace to which the agents will report. You must have a Log Analytics workspace that you already created, that the subscription's VMs will report to. You can define multiple subscriptions to report to the same workspace. If not defined, the default workspace will be used.

```
Set-AzSecurityWorkspaceSetting -Name "default" -Scope
"/subscriptions/d07c0080-170c-4c24-861d-9c817742786c" -WorkspaceId"/subscriptions/d07c0080-170c-4c24-
861d-9c817742786c/resourceGroups/myRg/providers/Microsoft.OperationalInsights/workspaces/myWorkspace"
```

4. Auto-provision installation of the Microsoft Monitoring Agent on your Azure VMs:

```
Set-AzContext -Subscription "d07c0080-170c-4c24-861d-9c817742786c"

Set-AzSecurityAutoProvisioningSetting -Name "default" -EnableAutoProvision
```

NOTE

It is recommended to enable auto provisioning to make sure that your Azure virtual machines are automatically protected by Azure Security Center.

5. Optional: It is highly recommended that you define the security contact details for the subscriptions you onboard, which will be used as the recipients of alerts and notifications generated by Security Center:

```
Set-AzSecurityContact -Name "default1" -Email "CISO@my-org.com" -Phone "2142754038" -AlertAdmin -
NotifyOnAlert
```

6. Assign the default Security Center policy initiative:

```
Register-AzResourceProvider -ProviderNamespace 'Microsoft.PolicyInsights'
$Policy = Get-AzPolicySetDefinition | where {$_.Properties.displayName -EQ '[Preview]: Enable Monitoring
in Azure Security Center'}
New-AzPolicyAssignment -Name 'ASC Default <d07c0080-170c-4c24-861d-9c817742786c>' -DisplayName 'Security
Center Default <subscription ID>' -PolicySetDefinition $Policy -Scope '/subscriptions/d07c0080-170c-
4c24-861d-9c817742786c'
```

You now successfully onboarded Azure Security Center with PowerShell!

You can now use these PowerShell cmdlets with automation scripts to programmatically iterate across subscriptions and resources. This saves time and reduces the likelihood of human error. You can use this [sample script](#) as reference.

See also

To learn more about how you can use PowerShell to automate onboarding to Security Center, see the following article:

- [Az.Security](#).

To learn more about Security Center, see the following article:

- [Setting security policies in Azure Security Center](#) -- Learn how to configure security policies for your Azure

subscriptions and resource groups.

- [Managing and responding to security alerts in Azure Security Center](#) -- Learn how to manage and respond to security alerts.

Integrate Azure Security Center with Windows Admin Center (Preview)

11/12/2019 • 2 minutes to read • [Edit Online](#)

Windows Admin Center is a management tool for your Windows servers. It's a single location for system administrators to access the majority of the most commonly used admin tools. From within Windows Admin Center, you can directly onboard your on-prem servers into Azure Security Center. You can then view a summary of your security recommendations and alerts directly in the Windows Admin Center experience.

NOTE

Your Azure subscription and the associated Log Analytics workspace both need to have Security Center's standard tier enabled in order to enable the Windows Admin Center integration. The standard tier is free for the first 30 days if you haven't previously used it on the subscription and workspace. For more information, see [the pricing information page](#).

When you've successfully onboarded a server from Windows Admin Center to Azure Security Center, you can:

- View security alerts and recommendations inside the Security Center extension in Windows Admin Center
- View the security posture and retrieve additional detailed information of your Windows Admin Center managed servers in Security Center within the Azure portal (or via an API)

By combining these two tools, Security Center becomes your single pane of glass to view all your security information, whatever the resource: protecting your Windows Admin Center managed on-prem servers, your VMs, and any additional PaaS workloads.

Onboarding Windows Admin Center managed servers into Security Center

1. From Windows Admin Center, select one of your servers, and in the **Tools** pane, select the Azure Security Center extension:

wac2016chshum

Tools



Search Tools 

 Local Users & Groups

 Network

 PowerShell

 Processes

 Registry

 Remote Desktop

 Roles & Features

 Scheduled Tasks

 Services

 Storage

 Storage Replica

 Updates

Extensions

 Azure Security Center

 Security

...

NOTE

If the server is already onboarded to Security Center, the set-up window will not appear.

2. Click **Sign in to Azure and set up**.



Secure your Server with Azure Security Center

Start a 30-day free trial

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.

[Get an overview about Azure Security Center](#)

[Sign in to Azure and set up](#)

- Follow the instructions to connect your server to Security Center. After you've entered the necessary details and confirmed, Security Center makes the necessary configuration changes to ensure that all of the following are true:

- An Azure Gateway is registered.
- The server has a workspace to report to and an associated subscription.
- Security Center's standard tier Log Analytics solution is enabled on the workspace. This solution provides Security Center's Standard tier features for *all* servers and virtual machines reporting to this workspace.
- Security Center's standard tier pricing for Virtual Machine is enabled on the subscription.
- The Microsoft Monitoring Agent (MMA) is installed on the server and configured to report to the selected workspace. If the server already reports to another workspace, it's configured to report to the newly selected workspace as well.

NOTE

It may take some time after onboarding for recommendations to appear. In fact, depending on your server activity you may not receive *any* alerts. To generate test alerts to test your alerts are working correctly, follow the instructions in [the alert validation procedure](#).

Viewing security recommendations and alerts in Windows Admin Center

Once onboarded, you can view your alerts and recommendations directly in the Azure Security Center area of Windows Admin Center. Click a recommendation or an alert to view them in the Azure portal. There, you'll get additional information and learn how to remediate issues.

Azure Security Center PREVIEW ⓘ

Subscription name Sub MK ⓘ Server protection Protected by Azure Security Center

Workspace name wac-workspace-surashed ⓘ Documentation Learn more about Azure Security Center ⓘ Explore Server security capabilities ⓘ Provide feedback ⓘ

Recommendations ⓘ



| Severity | Count |
|----------|-------|
| Low | 1 |
| Medium | 0 |
| High | 1 |

Refresh Recommendation Vulnerabilities in security configuration on your machines should be remediated System updates should be installed on your machines

2 items Severity 1 Low 1 High

Alerts ⓘ



| Severity | Count |
|----------|-------|
| Low | 0 |
| Medium | 0 |
| High | 1 |

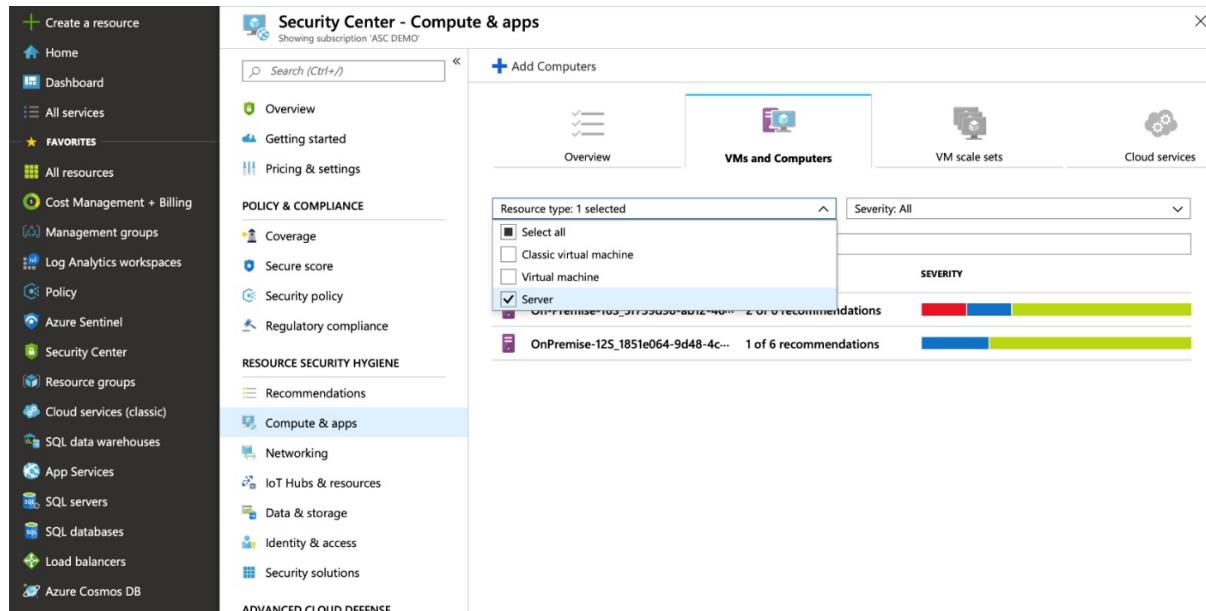
Refresh Alert Azure Security Center test alert (not a threat)

| Count | Time | Severity |
|-------|-----------|----------|
| 5 | 21/8/2019 | 1 High |

Viewing security recommendations and alerts for Windows Admin Center managed servers in Security Center

From Azure Security Center:

- To view security recommendations for all your Windows Admin Center servers, open **Compute & Apps** and click the **VMs and Computers** tab. Filter the list by resource "Server" as shown here:



Security Center - Compute & apps Showing subscription 'ASC DEMO'

Search (Ctrl+ /)

Add Computers

Overview VMs and Computers VM scale sets Cloud services

Resource type: 1 selected Severity: All

Select all Server Classic virtual machine Virtual machine OnPremise-125_1851e064-9d48-4c... 2 of 6 recommendations

OnPremise-125_1851e064-9d48-4c... 1 of 6 recommendations

- To view security alerts for all your Windows Admin Center servers, open **Security alerts**. Click **Filter** and ensure **only** "Non-Azure" is selected:

?

Filter X

Freshness

New

Older

Type

Incident

Alert

Environment

Non-Azure

Azure

Security Center - Security alerts

Showing subscription 'ASC DEMO'

Search (Ctrl+ /) Filter

Pricing & settings

POLICY & COMPLIANCE

- Coverage
- Secure score
- Security policy
- Regulatory compliance

RESOURCE SECURITY HYGIENE

- Recommendations
- Compute & apps
- Networking
- IoT Hubs & resources
- Data & storage
- Identity & access
- Security solutions

ADVANCED CLOUD DEFENSE

- Adaptive application controls
- Just in time VM access
- Adaptive network hardening
- File Integrity Monitoring

THREAT PROTECTION

- Security alerts
- Custom alert rules (Preview)

| DESCRIPTION | CO... | DETECTED ... | ENVIR... | DATE | STATE | SEVERI... |
|--------------------------------|-------|--------------|----------|----------|--------|-----------|
| Security incident detected | 1 | Microsoft | Azure | 08/10/19 | Active | High |
| Security incident detected | 1 | Microsoft | Azure | 08/04/19 | Active | High |
| Security incident detected | 1 | Microsoft | Azure | 07/29/19 | Active | High |
| Potential SQL Injection | 1 | Microsoft | Azure | 08/14/19 | Active | High |
| Modified system binary disc... | 1 | Microsoft | Azure | 08/11/19 | Active | High |
| Successful RDP brute force ... | 1 | Microsoft | Azure | 08/10/19 | Active | High |
| Potential SQL Injection | 1 | Microsoft | Azure | 08/08/19 | Active | High |
| Suspicious process executed | 1 | Microsoft | Azure | 08/07/19 | Active | High |

Compare baselines using File Integrity Monitoring (FIM)

11/6/2019 • 2 minutes to read • [Edit Online](#)

File Integrity Monitoring (FIM) informs you when changes occur to sensitive areas in your resources, so you can investigate and address unauthorized activity. FIM monitors Windows files, Windows registries, and Linux files.

This topic explains how to enable FIM on the files and registries. For more information about FIM, see [File Integrity Monitoring in Azure Security Center](#).

Why use FIM?

Operating system, applications, and associated configurations control the behavior and security state of your resources. Therefore, attackers target the files that control your resources, in order to overtake a resource's operating system and/or execute activities without being detected.

In fact, many regulatory compliance standards such as PCI-DSS & ISO 17799 require implementing FIM controls.

Enable built-in recursive registry checks

The FIM registry hive defaults provide a convenient way to monitor recursive changes within common security areas. For example, an adversary may configure a script to execute in LOCAL_SYSTEM context by configuring an execution at startup or shutdown. To monitor changes of this type, enable the built-in check.

| | | |
|-------------|-------|--|
| Recommended | false | HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Shutdown |
| Recommended | false | HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Group Policy\Scripts\Startup |
| Recommended | false | HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Internet Explorer\Extensions |

NOTE

Recursive checks apply only to recommended security hives and not to custom registry paths.

Adding a custom registry check

FIM baselines start by identifying characteristics of a known-good state for the operating system and supporting application. For this example, we will focus on the password policy configurations for Windows Server 2008 and higher.

| POLICY NAME | REGISTRY SETTING |
|---|--|
| Domain controller: Refuse machine account password changes | MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RefusePasswordChange |
| Domain member: Digitally encrypt or sign secure channel data (always) | MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireSignOrSeal |

| POLICY NAME | REGISTRY SETTING |
|---|---|
| Domain member: Digitally encrypt secure channel data (when possible) | MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SealSecureChannel |
| Domain member: Digitally sign secure channel data (when possible) | MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\SignSecureChannel |
| Domain member: Disable machine account password changes | MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DisablePasswordChange |
| Domain member: Maximum machine account password age | MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\MaximumPasswordAge |
| Domain member: Require strong (Windows 2000 or later) session key | MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RequireStrongKey |
| Network security: Restrict NTLM: NTLM authentication in this domain | MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\RestrictNTLMInDomain |
| Network security: Restrict NTLM: Add server exceptions in this domain | MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\DCAllowedNTLMServers |
| Network security: Restrict NTLM: Audit NTLM authentication in this domain | MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters\AuditNTLMInDomain |

NOTE

To learn more about registry settings supported by various operating system versions, refer to the [Group Policy Settings reference spreadsheet](#).

To configure FIM to monitor registry baselines:

1. In the **Add Windows Registry for Change Tracking** window, in the **Windows Registry Key** text box, enter the registry key.



HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters

Add Windows Registry for Change Tracking

Save Delete Discard

Enabled

True False

* Item Name

Authentication ✓

Group

Password Policy settings

* Windows Registry Key

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ Netlogon\Parameters ✓

Tracking changes to Windows files

1. In the **Add Windows File for Change Tracking** window, in the **Enter path** text box, enter the folder which contains the files that you want to track. In the example in the following figure, **Contoso Web App** resides in the D:\ drive within the **ContosWebApp** folder structure.
2. Create a custom Windows file entry by providing a name of the setting class, enabling recursion, and specifying the top folder with a wildcard (*) suffix.

Add Windows File for Change Tracking X

 Save

 Delete

 Discard

Enabled

True

False

* Item Name

Contoso Web configurations 

Group

Application security

* Enter Path

d:\ContosoWebApp* 

Recursion

On

Off

Retrieving change data

File Integrity Monitoring data resides within the Azure Log Analytics / ConfigurationChange table set.

1. Set a time range to retrieve a summary of changes by resource. In the following example, we are retrieving all changes in the last fourteen days in the categories of registry and files:

```
ConfigurationChange  
| where TimeGenerated > ago(14d)  
| where ConfigChangeType in ('Registry', 'Files')  
| summarize count() by Computer, ConfigChangeType
```

2. To view details of the registry changes:

- a. Remove **Files** from the **where** clause,

b. Remove the summarization line and replace it with an ordering clause:

```
ConfigurationChange  
| where TimeGenerated > ago(14d)  
| where ConfigChangeType in ('Registry')  
| order by Computer, RegistryKey
```

Reports can be exported to CSV for archival and/or channeled to a Power BI report.

The screenshot shows the Power BI Query Editor interface. At the top, there is a query editor pane containing M code:

```
ConfigurationChange  
| where TimeGenerated > ago(14d)  
| where ConfigChangeType in ('Registry')  
| order by Computer, RegistryKey
```

Below the query editor is a results pane showing a table of data. The table has columns: Computer, ConfigChangeType, ChangeCategory, SourceComputerId, SoftwareType, SoftwareName, and Previous. The data shows multiple rows for 'retailEUS3' with 'Registry' as ConfigChangeType and 'Modified' as ChangeCategory. The SourceComputerId column contains values like '4152690f-b8ff-47f9-9420-7dd4def8fe14'. The SoftwareType and SoftwareName columns are empty. The Previous column is partially visible.

On the right side of the interface, there is a ribbon bar with Save, Copy link, and Export buttons. A red circle highlights a dropdown menu that appears when the Export button is clicked. The menu contains three options: "Export to CSV - All Columns", "Export to CSV - Displayed Columns", and "Export to Power BI (M Query)".

Workflow automation (Preview)

12/13/2019 • 3 minutes to read • [Edit Online](#)

Every security program includes multiple workflows for incident response. These processes might include notifying relevant stakeholders, launching a change management process, and applying specific remediation steps. Security experts recommend that you automate as many steps of those procedures as you can. Automation reduces overhead. It can also improve your security by ensuring the process steps are done quickly, consistently, and according to your predefined requirements.

This article describes the Workflow automation feature (preview) of Azure Security Center. This preview feature can trigger Logic Apps on security alerts and recommendations. For example, you might want Security Center to email a specific user when an alert occurs. You'll also learn how to create Logic Apps using [Azure Logic Apps](#).

NOTE

If you previously used the Playbooks (Preview) view on the sidebar, you'll find the same features together with the expanded functionality in the new Workflow automation (Preview) page.

Requirements

- To work with Azure Logic Apps workflows, you must have the following Logic Apps roles/permissions:
 - [Logic App Operator](#) permissions are required or Logic App read/trigger access (this role can't create or edit logic apps; only *run* existing ones)
 - [Logic App Contributor](#) permissions are required for Logic App creation and modification
- If you want to use Logic App connectors, you may need additional credentials to sign in to their respective services (for example, your Outlook/Teams/Slack instances)

Create a Logic App and define when it should automatically run

1. From Security Center's sidebar, select **Workflow automation (Preview)**.

| Name | Status | Scope | Trigger type | Description |
|-------|----------|----------|---------------------------------|-------------|
| Du | Disabled | ASC DEMO | Security Center alert | |
| Du14 | Disabled | ASC DEMO | Security Center recommendati... | |
| Tes | Disabled | ASC DEMO | Security Center recommendati... | |
| Keeee | Enabled | ASC DEMO | Security Center alert | |
| Muto | Enabled | ASC DEMO | Security Center alert | |
| Trts | Enabled | ASC DEMO | Security Center alert | |
| US | Enabled | ASC DEMO | Security Center recommendati... | |

From this page you can create new automation rules, as well as enable, disable, or delete existing ones.

2. To define a new workflow, click **Add workflow automation**.

A pane appears with the options for your new automation. Here you can enter:

- A name and description for the automation.
- The triggers that will initiate this automatic workflow. For example, you might want your Logic App to run when a security alert that contains "SQL" is generated.
- The Logic App that will run when your trigger conditions are met.

3. From the Actions section, click **Create a new one** to begin the Logic App creation process.

You'll be taken to Azure Logic Apps.

The screenshot shows the 'Logic App' creation form in the Microsoft Azure portal. The form includes fields for Name, Subscription, Resource group, Location, and Log Analytics. A note indicates that triggers and actions can be added after creation. At the bottom are 'Create' and 'Automation options' buttons.

Logic App

Name *

Subscription *

ASC DEMO

Resource group *

Create new Use existing

Location *

Log Analytics

On Off

i You can add triggers and actions to your Logic App after creation.

Create Automation options

4. Enter a name, resource group, and location, and click **Create**.

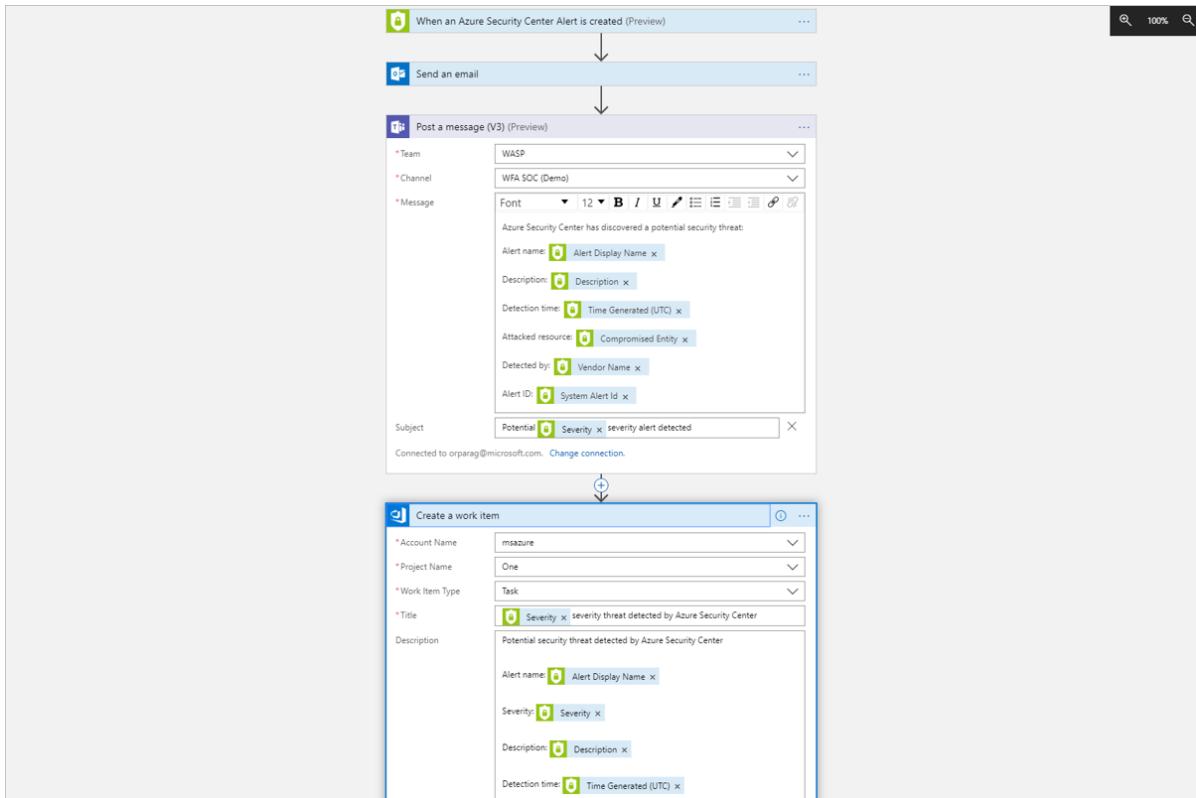
5. In your new Logic App, you can choose from built-in, predefined templates from the security category. Or you can define a custom flow of events to occur when this process is triggered.

In the Logic App designer the following triggers from the Security Center connectors are supported:

- **When an Azure Security Center Recommendation is created or triggered (Preview)**
- **When an Azure Security Center Alert is created or triggered (Preview)**

NOTE

If you are using the legacy trigger "When a response to an Azure Security Center alert is triggered", your Logic Apps will not be launched by the Workflow Automation feature. Instead, use either of the triggers mentioned above.



- After you've defined your Logic App, return to the workflow automation definition pane ("Add workflow automation"). Click **Refresh** to ensure your new Logic App is available for selection.

Actions
Configure the Logic Apps that will be triggered.
Choose an existing Logic App or
[Create a new one](#)

Logic app name * ⓘ
 ^
[Refresh](#)

- Select your Logic App and save the automation. Note that the Logic App dropdown only shows Logic Apps with supporting Security Center connectors mentioned above.

Manually trigger a Logic App

You can also run Logic Apps manually when viewing a security recommendation.

To manually run a Logic App, open a recommendation and click Trigger Logic App (Preview):

Microsoft Azure

Search resources, services, and docs (G+)

Home > Security Center - Security alerts > PREVIEW - Role binding to the cluster-admin role detected > PREVIEW - Role binding to the cluster-admin role detected

PREVIEW - Role binding to the cluster-admin role detected

ASC-IGNITE-DEMO

[Learn more](#)

General information

| | |
|-------------------|--|
| DESCRIPTION | Kubernetes audit log analysis detected a new binding to the cluster-admin role which gives administrator privileges. Unnecessary administrator privileges might cause privilege escalation in the cluster. |
| ACTIVITY TIME | Tuesday, October 29, 2019, 3:06:26 PM |
| SEVERITY | Low |
| STATE | Active |
| ATTACKED RESOURCE | ASC-IGNITE-DEMO |
| SUBSCRIPTION | ASC DEMO (214bd26) |
| DETECTED BY | Microsoft |
| ACTION TAKEN | Detected |

Was this useful? Yes No

[Trigger Logic App \(Preview\)](#)

Data types schemas

To view the raw event schemas of the security alerts or recommendations events passed to the Logic App instance, visit the [Workflow automation data types schemas](#). This can be useful in cases where you are not using Security Center's built-in Logic App connectors mentioned above, but instead are using Logic App's generic HTTP connector - you could use the event JSON schema to manually parse it as you see fit.

Next steps

In this article, you learned about creating Logic Apps, running them manually in Security Center, and automating their execution.

For other related material, see the following articles:

- [Security recommendations in Azure Security Center](#)
- [Security alerts in Azure Security Center](#)
- [About Azure Logic Apps](#)
- [Logic Apps connectors](#)
- [Workflow automation data types schemas](#)

Export security alerts and recommendations (Preview)

2/19/2020 • 4 minutes to read • [Edit Online](#)

Azure Security Center generates detailed security alerts and recommendations. You can view them in the portal or through programmatic tools. You may also need to export this information or send it to other monitoring tools in your environment.

This article describes the set of (preview) tools that allow you to export alerts and recommendations either manually or in an ongoing, continuous fashion.

Using these tools you can:

- Generate detailed reports as CSV
- Export to Log Analytics workspaces
- Export to Azure Event Hubs (for integrations with third-party SIEMs)

Setting up a continuous export

1. From Security Center's sidebar, click **Pricing & settings**.
2. Select the specific subscription for which you want to configure the data export.
3. From the sidebar of the settings page for that subscription, select **Continuous Export (Preview)**.

The screenshot shows the 'Settings - Continuous Export (Preview)' page in the Microsoft Azure portal. The left sidebar lists 'Pricing tier', 'Data Collection', 'Security playbooks', 'Threat detection', 'Email notifications', and 'Continuous Export (Preview)'. The main content area has a title 'Continuous Export (Preview)' with a sub-instruction: 'Configure streaming export setting of Security alerts and recommendations to multiple export targets. Exporting Security Center's data also enables you to use experiences such as PowerBI reports, Azure Mobile notification and SIEM integration.' Below this are sections for 'Event hub' and 'Log Analytics workspace', with 'Event hub' currently selected. A toggle switch 'Export enabled' is set to 'On'. Under 'Exported data types', there are two checkboxes: 'Security recommendations' and 'Security alerts', each with a dropdown menu for selecting severities. The 'Export configuration' section allows selecting a resource group, with 'AzureAttachDemo' selected. The 'Export target' section includes fields for 'Subscription' (set to 'Nir Winter test subscription'), 'Event hub namespace' ('nir-test2'), 'Event hub name' ('Select event hub'), and 'Event hub policy name' ('Select event hub policy name'). A note states 'Saving data to event hub incurs ingestion charges, as detailed [here](#)'. The 'SIEM Integration' section contains a link 'Integrate with 3rd party SIEM>' and a note 'Connect selected Event Hub to Azure Data Explorer'. Another note says 'Export data from the Event Hub to Data Explorer. [Learn More](#)'.

Here you see the export options. There's a tab for each available export target.

4. Select the data type you'd like to export and choose from the filters on each type (for example, export only high severity alerts).
5. From the "Export target" area, choose where you'd like the data saved. Data can be saved in a target on a different subscription (for example on a Central Event Hub instance or a central Log Analytics workspace).
6. Click **Save**.

Continuous export through Azure Event Hubs

NOTE

The most effective method to stream monitoring data to external tools in most cases is using Azure Event Hubs. [This article](#) provides a brief description for how you can stream monitoring data from different sources to an Event Hub and links to detailed guidance.

NOTE

If you previously exported Security Center alerts to a SIEM using Azure Activity log, the procedure below replaces that methodology.

To view the event schemas of the exported data types, visit the [Event Hub event schemas](#).

To integrate with a SIEM

After you have configured continuous export of your chosen Security Center data to Azure Event Hubs, you can set up the appropriate connector on your SIEM by following the instructions below.

Follow the instructions relevant to your SIEM from [this page](#) and use the relevant connector:

- **Splunk** - Use the [Azure Monitor Add-On for Splunk](#)
- **IBM QRadar** - Use [a manually configured log source](#)
- **ArcSight** – Use [SmartConnector](#)

If you're using **Azure Sentinel**, use the native Azure Security Center alerts [data connector](#) offered there.

Also, if you'd like to move the continuously exported data automatically from your configured Event Hub to Azure Data Explorer, use the instructions in [Ingest data from Event Hub into Azure Data Explorer](#).

Continuous export to a Log Analytics workspace

To export to a Log Analytics workspace, you must have Security Center's free or standard tier Log Analytics solutions enabled on your workspace. If you're using the Azure portal, the Security Center free tier solution is automatically enabled when you enable continuous export. However, if you're configuring your continuous export settings programmatically, you must manually select the free or standard pricing tier for the required workspace from within **Pricing & settings**.

Log Analytics tables and schemas

Security alerts and recommendations are stored in the *SecurityAlert* and *SecurityRecommendations* tables respectively. The name of the Log Analytics solution containing these tables depends on whether you are on the free or standard tier (see [pricing](#)): Security('Security and Audit') or SecurityCenterFree.

The screenshot shows the 'Active' section of the Azure Security Center. It displays a hierarchical list of security features. The 'Security' category is expanded, showing sub-items such as CommonSecurityLog, LinuxAuditLog, ProtectionStatus, SecurityAlert, and SecurityBaseline.

To view the event schemas of the exported data types, visit the [Log Analytics table schemas](#).

View exported security alerts and recommendations in Azure Monitor

In some cases, you may choose to view the exported Security Alerts and/or recommendations in [Azure Monitor](#).

Azure Monitor provides a unified alerting experience for a variety of Azure alerts including Diagnostic Log, Metric alerts, and custom alerts based on Log Analytics workspace queries.

To view alerts and recommendations from Security Center in Azure Monitor, configure an Alert rule based on Log Analytics queries (Log Alert):

- From Azure Monitor's **Alerts** page, click **New alert rule**.

The screenshot shows the Azure Monitor - Alerts page. It includes a search bar, navigation links for Overview, Activity log, and Alerts, and sections for Metrics, Logs, Service Health, and Workbooks. The main area displays summary statistics: Total alerts (639), Smart groups (62), Total alert rules (329), and Action rules (2). Below this is a chart showing the distribution of alerts by severity level (Sev 0 to Sev 4).

| Severity | Total Alerts |
|----------|--------------|
| Sev 0 | 68 |
| Sev 1 | 352 |
| Sev 2 | 54 |
| Sev 3 | 145 |
| Sev 4 | 20 |

- In the create rule page, configure your new rule (in the same way you'd configure a [log alert rule in Azure Monitor](#)):

- For **Resource**, select the Log Analytics workspace to which you exported security alerts and recommendations.
- For **Condition**, select **Custom log search**. In the page that appears, configure the query, lookback period, and frequency period. In the search query, you can type *SecurityAlert* or *SecurityRecommendation* to query the data types that Security Center continuously exports to as you enable the Continuous export to Log Analytics feature.

- Optionally, configure the [Action Group](#) that you'd like to trigger. Action groups can trigger email sending, ITSM tickets, WebHooks, and more.

The screenshot shows the 'Create rule' page in the Azure Security Center. The top navigation bar includes 'Create rule', 'Rules management', and 'Alerts' tabs. The main area is divided into sections: 'RESOURCE' (contosoretail-IT), 'HIERARCHY' (Contoso IT - demo > contosoazur), 'CONDITION' (Whenever the Custom log search is Greater than 0 count), 'Monthly cost in USD (Estimated)' (\$ 1.50), and 'Total \$ 1.50'. Below these are 'ACTIONS' (Action group name: SecurityCenterAlertRule, Contain actions: 2 Email(s)), 'Customize Actions' (Email subject, Include custom Json payload for webhook), and 'ALERT DETAILS' (Alert rule name: SecurityCenterAlertRule, Description: Alert rule for exported data from Azure Security Center, Severity: Warning(Sev 1), Enable rule upon creation: Yes, Suppress Alerts). A note at the bottom states: 'Action rules (preview) allows you to define actions at scale as well as suppress actions. Learn more about this functionality [here](#)'. A 'Create alert rule' button is at the bottom left.

You'll now see new Azure Security Center alerts or recommendations (depending on your configuration) in Azure Monitor alerts, with automatic triggering of an action group (if provided).

Manual one-time export of security alerts

To download a CSV report for alerts or recommendations, open the **Security alerts** or **Recommendations** page and click the **Download CSV report** button.

Microsoft Azure

Home > Security Center - Security alerts

Security Center - Security alerts
Showing subscription 'ASC DEMO'

Search (Ctrl+/
Filter
Download CS report
Download CSV report

Overview
Getting started
Pricing & settings

POLICY & COMPLIANCE
Coverage
Secure score
Security policy
Regulatory compliance

RESOURCE SECURITY HYGIENE

ADVANCED CLOUD DEFENSE

THREAT PROTECTION
Security alerts
Security alerts map (Preview)

AUTOMATION & ORCHESTRATION
Playbooks (Preview)

High severity | Medium severity | Low severity
5 | 6 | 7

13 Sun

| Description | Count | Detected by | Environment |
|--|-------|-------------|-------------|
| Security incident detected | 1 | Microsoft | Azure |
| Azure Security Center test alert (not a threat) | 1 | Microsoft | Azure |
| Potential SQL Injection | 1 | Microsoft | Azure |
| Modified system binary discovered in dump file 5bd767e4- 1 | 1 | Microsoft | Azure |

NOTE

These reports contain alerts and recommendations for resources from the currently selected subscriptions.

Next steps

In this article, you learned how to configure continuous exports of your recommendations and alerts. You also learned how to download your alerts data as a CSV file.

For related material, see the following documentation:

- [Azure Event Hubs documentation](#)
- [Azure Sentinel documentation](#)
- [Azure Monitor documentation](#)
- [Workflow automation and continuous export data types schemas](#)

Data collection in Azure Security Center

2/27/2020 • 15 minutes to read • [Edit Online](#)

Security Center collects data from your Azure virtual machines (VMs), virtual machine scale sets, IaaS containers, and non-Azure (including on-premises) computers to monitor for security vulnerabilities and threats. Data is collected using the Log Analytics Agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis. Examples of such data are: operating system type and version, operating system logs (Windows event logs), running processes, machine name, IP addresses, and logged in user. The Log Analytics Agent also copies crash dump files to your workspace.

Data collection is required to provide visibility into missing updates, misconfigured OS security settings, endpoint protection status, and health and threat protection.

This article describes how to install a Log Analytics Agent and set a Log Analytics workspace in which to store the collected data. Both operations are required to enable data collection.

NOTE

- Data collection is only needed for Compute resources (VMs, virtual machine scale sets, IaaS containers, and non-Azure computers). You can benefit from Azure Security Center even if you don't provision agents; however, you will have limited security and the capabilities listed above are not supported.
- For the list of supported platforms, see [Supported platforms in Azure Security Center](#).
- Storing data in Log Analytics, whether you use a new or existing workspace, might incur additional charges for data storage. For more information, see the [pricing page](#).

Enable automatic provisioning of the Log Analytics Agent

To collect the data from the machines, you should have the Log Analytics Agent installed. Installation of the agent can be done automatically (recommended) or you can install the agent manually.

NOTE

Automatic provisioning is off by default. To set Security Center to install automatic provisioning by default, set it to **On**.

When automatic provisioning is On, Security Center provisions the Log Analytics Agent on all supported Azure VMs and any new ones that are created. Automatic provisioning is strongly recommended but manual agent installation is also available. [Learn how to install the Log Analytics Agent extension](#).

To enable automatic provisioning of the Log Analytics Agent:

1. Under the Security Center main menu, select **Pricing & settings**.
2. Click on the applicable subscription

Security Center - Pricing & settings

Showing 3 subscriptions

Pricing & Settings

Configure pricing, data collection and additional settings of your Azure subscriptions and workspaces.

[Click here to learn more >](#)

10 MANAGEMENT GROUPS 3 SUBSCRIPTIONS 2 WORKSPACES

| NAME | PRICING TIER |
|--|--------------------|
| (3 of 49 subscriptions) | |
| 3 (1 of 1 subscriptions) | |
| ASC DEMO | Standard |
| (1 of 46 subscriptions) | |
| Non Production (1 of 42 subscriptions) | |
| NonProd Outside Ring (1 of 40 subscriptions) | |
| NonProd Ring1 (0 of 2 subscriptions) | Free |
| Production (0 of 4 subscriptions) | |
| Prod Outside Ring (0 of 3 subscriptions) | |
| Prod Ring1 (0 of 1 subscriptions) | |
| (0 of 1 subscriptions) | |
| exportSecurityCenterDataToLogAWorkspaceTest | Standard (partial) |
| | Standard |
| | Free |

Policy & Compliance

- Coverage
- Secure score
- Regulatory compliance
- Security policy

Resource Security Hygiene

- Recommendations
- Compute & apps
- Networking
- IoT hubs & resources (Preview)
- Data & storage
- Identity & access (Preview)
- Security solutions

Advanced Cloud Defense

- Adaptive application controls
- Just in time VM access
- Network hardening (Preview)
- File Integrity Monitoring

Threat Protection

- Security alerts
- Custom alert rules (Preview)
- Security alerts map (Preview)

Automation & Orchestration

- Playbooks (Preview)

Logs

- Events
- Search

3. Select **Data Collection**.

4. Under **Auto Provisioning**, select **On** to enable automatic provisioning.

5. Select **Save**.

Security policy - Data Collection

Contoso IT - demo

Save

POLICY COMPONENTS

- Data Collection**
- Security policy
- Email notifications
- Pricing tier
- Edit security configurations (Pre...)

Security Center collects security data and events from your resources and services to help you prevent, detect, and respond to threats. [Learn more >](#)

Auto Provisioning

This enables the automatic installation of the Microsoft Monitoring Agent on all the VMs in your subscription. If enabled, any new or existing VM without an installed agent will be provisioned. [Learn more >](#)

On **Off**

Default workspace configuration

Data collected by Security Center is stored in Log Analytics workspace(s). You can elect to have data collected from Azure VMs stored in workspace(s) created by Security Center or in an existing workspace you created. [Learn more >](#)

Use workspace(s) created by Security Center (default)

Connect Azure VMs to report to workspaces created by Security Center

Connect Azure VMs to report to workspaces created by Security Center

Use another workspace

Connect Azure VMs to report to selected user workspace

contosoretail-IT

i Any other solutions enabled on the selected workspace will be applied to Azure VMs that are connected to it. For paid solutions, this could result in additional charges. For data privacy considerations, please make sure your selected workspace is in your desired region.

NOTE

- For instructions on how to provision a pre-existing installation, see [Automatic provisioning in cases of a preexisting agent installation](#).
- For instructions on manual provisioning, see [Install the Log Analytics Agent extension manually](#).
- For instructions on turning off automatic provisioning, see [Turn off automatic provisioning](#).
- For instructions on how to onboard Security Center using PowerShell, see [Automate onboarding of Azure Security Center using PowerShell](#).

Workspace configuration

Data collected by Security Center is stored in Log Analytics workspace(s). You can select to have data collected from Azure VMs stored in workspaces created by Security Center or in an existing workspace you created.

Workspace configuration is set per subscription, and many subscriptions may use the same workspace.

Using a workspace created by Security Center

Security center can automatically create a default workspace in which to store the data.

To select a workspace created by Security Center:

1. Under **Default workspace configuration**, select Use workspace(s) created by Security center.

Home > Security Center - Security policy > Settings - Data Collection

Settings - Data Collection
Contoso IT - demo

Save

Security Center collects security data and events from your resources and services to help you prevent, detect, and respond to threats. [Learn more >](#)

Auto Provisioning

This enables the automatic installation of the Microsoft Monitoring Agent on all the VMs in your subscription. If enabled, any new or existing VM without an installed agent will be provisioned. [Learn more >](#)

On Off

Default workspace configuration

Data collected by Security Center is stored in Log Analytics workspace(s). You can elect to have data collected from Azure VMs stored in workspace(s) created by Security Center or in an existing workspace you created. [Learn more >](#)

Use workspace(s) created by Security Center (default)
Connect Azure VMs to report to workspaces created by Security Center

Use another workspace
Connect Azure VMs to report to selected user workspace
contosoretail-IT

i Any other solutions enabled on the selected workspace will be applied to Azure VMs that are connected to it. For paid solutions, this could result in additional charges. For data privacy considerations, please make sure your selected workspace is in your desired region.

Security Events

Data collection configuration for security events
[For additional details](#)

All Events
All Windows security and AppLocker events will be collected and stored.

Common
A standard set of events will be collected and stored to enable security and audit capabilities.

Minimal
Security Center will collect the minimal set of events that are required for threat detection. By enabling this option, you won't be able to have a full audit trail.

None
No security or AppLocker events will be collected. Data presented in Security Center will be based on agent assessment such as Endpoint protection, OS Configuration and Updates.

2. Click **Save**.

Security Center creates a new resource group and default workspace in that geolocation, and connects the agent to that workspace. The naming convention for the workspace and resource group is:

Workspace: DefaultWorkspace-[subscription-ID]-[geo]

Resource Group: DefaultResourceGroup-[geo]

If a subscription contains VMs from multiple geolocations, then Security Center creates multiple workspaces. Multiple workspaces are created to maintain data privacy rules.

3. Security Center will automatically enable a Security Center solution on the workspace per the pricing tier set for the subscription.

NOTE

The Log Analytics pricing tier of workspaces created by Security Center does not affect Security Center billing. Security Center billing is always based on your Security Center security policy and the solutions installed on a workspace. For the Free tier, Security Center enables the *SecurityCenterFree* solution on the default workspace. For the Standard tier, Security Center enables the *Security* solution on the default workspace. Storing data in Log Analytics might incur additional charges for data storage. For more information, see the [pricing page](#).

For more information about existing log analytics accounts, see [Existing log analytics customers](#).

Using an existing workspace

If you already have an existing Log Analytics workspace, you might want to use the same workspace.

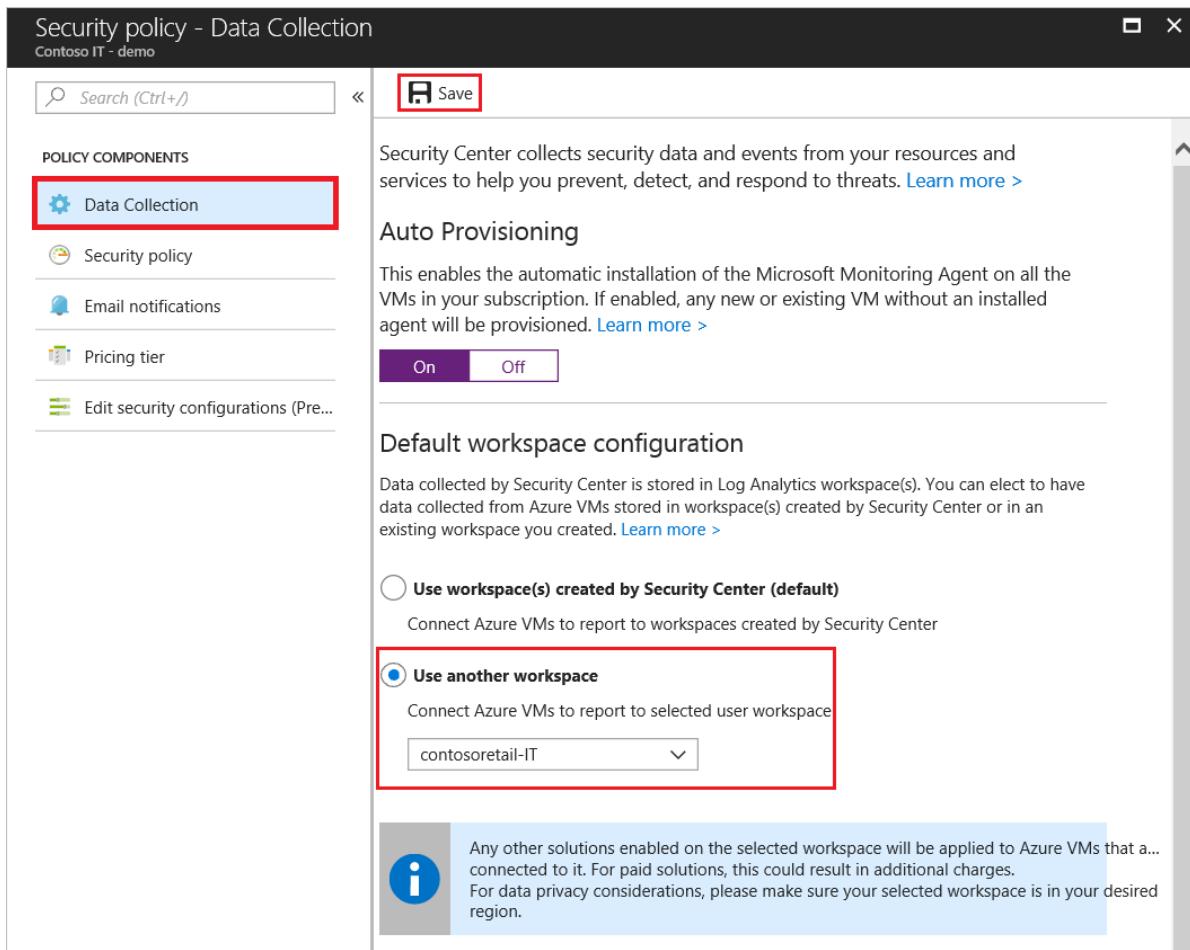
To use your existing Log Analytics workspace, you must have read and write permissions on the workspace.

NOTE

Solutions enabled on the existing workspace will be applied to Azure VMs that are connected to it. For paid solutions, this could result in additional charges. For data privacy considerations, make sure your selected workspace is in the right geographic region. Storing data in log analytics might incur additional charges for data storage. For more information, see the [pricing page](#).

To select an existing Log Analytics workspace:

1. Under **Default workspace configuration**, select **Use another workspace**.



- From the pull-down menu, select a workspace to store collected data.

NOTE

In the pull down menu, all the workspaces across all of your subscriptions are available. See [cross subscription workspace selection](#) for more information. You must have permission to access the workspace.

- Select **Save**.
- After selecting **Save**, you will be asked if you would like to reconfigure monitored VMs that were previously connected to a default workspace.
 - Select **No** if you want the new workspace settings to apply on new VMs only. The new workspace settings only apply to new agent installations; newly discovered VMs that do not have the Log Analytics Agent installed.
 - Select **Yes** if you want the new workspace settings to apply on all VMs. In addition, every VM connected to a Security Center created workspace is reconnected to the new target workspace.

NOTE

If you select Yes, you must not delete the workspace(s) created by Security Center until all VMs have been reconnected to the new target workspace. This operation fails if a workspace is deleted too early.

- Select **Cancel** to cancel the operation.

Would you like to reconfigure monitored VMs?

To apply the default workspace setting on already monitored VMs reporting to Security Center managed workspaces, click Yes. To apply only on new agent installations click No. To cancel operation click Cancel. Please note this process may take up to few hours.

Yes

No

Cancel

5. Select the pricing tier for the desired workspace you intend to set the Log Analytics Agent.

To use an existing workspace, set the pricing tier for the workspace. This will install a security Center solution on the workspace if one is not already present.

a. In the Security Center main menu, select **Pricing & settings**.

b. Select the desired Workspace in which you intend to connect the agent.

Security Center - Pricing & settings

The screenshot shows the 'Pricing & Settings' page in the Azure Security Center. On the left, there's a navigation sidebar with sections like Overview, Getting started, Pricing & settings (which is selected), Policy & Compliance, Resource Security Hygiene, Threat Protection, Automation & Orchestration, and Logs. The main area displays '10 MANAGEMENT GROUPS', '3 SUBSCRIPTIONS', and '2 WORKSPACES'. A table lists workspaces with their names, counts of subscriptions, and pricing tiers. The workspaces include 'ASC DEMO' (Standard), 'Non Production' (Free), 'Production' (Free), 'Prod Outside Ring' (Free), 'Prod Ring1' (Standard), 'exportSecurityCenterDataToLogAWorkspaceTest' (Standard), and another workspace with 49 subscriptions (Standard).

| NAME | PRICING TIER |
|---|--------------|
| ASC DEMO (1 of 1 subscriptions) | Standard |
| Non Production (1 of 46 subscriptions) | Free |
| Production (0 of 4 subscriptions) | Free |
| Prod Outside Ring (0 of 3 subscriptions) | Free |
| Prod Ring1 (0 of 1 subscriptions) | Standard |
| exportSecurityCenterDataToLogAWorkspaceTest | Standard |
| (3 of 49 subscriptions) | |

c. Set the pricing tier.

Home > Security Center - Pricing & settings > Settings - Pricing tier

Settings - Pricing tier
APEX C+L - Aquent Vendor Subscriptions

Search (Ctrl+)/<> Save

The Standard tier provides enhanced security. Learn more >

| Free (for Azure resources only) | Standard |
|--|--|
| ✓ Continuous assessment and security recommendations | ✓ Continuous assessment and security recommendations |
| ✓ Azure Secure Score | ✓ Azure Secure Score |
| ✗ Just in time VM Access | ✓ Just in time VM Access |
| ✗ Adaptive application controls and network hardening | ✓ Adaptive application controls and network hardening |
| ✗ Regulatory compliance dashboard and reports | ✓ Regulatory compliance dashboard and reports |
| ✗ Threat protection for Azure VMs and non-Azure servers (including Server EDR) | ✓ Threat protection for Azure VMs and non-Azure servers (including Server EDR) |
| ✗ Threat protection for supported PaaS services | ✓ Threat protection for supported PaaS services |

Pricing will apply to: 20 resources in this subscription

^ Select pricing tier by resource type

NOTE

If the workspace already has a **Security** or **SecurityCenterFree** solution enabled, the pricing will be set automatically.

Cross-subscription workspace selection

When you select a workspace in which to store your data, all the workspaces across all your subscriptions are available. Cross-subscription workspace selection allows you to collect data from virtual machines running in different subscriptions and store it in the workspace of your choice. This selection is useful if you are using a centralized workspace in your organization and want to use it for security data collection. For more information on how to manage workspaces, see [Manage workspace access](#).

Data collection tier

Selecting a data collection tier in Azure Security Center will only affect the storage of security events in your Log Analytics workspace. The Log Analytics agent will still collect and analyze the security events required for Azure Security Center's threat protection, regardless of which tier of security events you choose to store in your Log Analytics workspace (if any). Choosing to store security events in your workspace will enable investigation, search, and auditing of those events in your workspace.

NOTE

Storing data in log analytics might incur additional charges for data storage. For more information, see the [pricing page](#).

You can choose the right filtering policy for your subscriptions and workspaces from four sets of events to be stored in your workspace:

- **None** – Disable security event storage. This is the default setting.
- **Minimal** – A smaller set of events for customers who want to minimize the event volume.
- **Common** – This is a set of events that satisfies most customers and allows them a full audit trail.
- **All events** – For customers who want to make sure all events are stored.

NOTE

These security events sets are available only on Security Center's Standard tier. See [Pricing](#) to learn more about Security Center's pricing tiers. These sets were designed to address typical scenarios. Make sure to evaluate which one fits your needs before implementing it.

To determine the events that will belong to the **Common** and **Minimal** event sets, we worked with customers and industry standards to learn about the unfiltered frequency of each event and their usage. We used the following guidelines in this process:

- **Minimal** - Make sure that this set covers only events that might indicate a successful breach and important events that have a very low volume. For example, this set contains user successful and failed login (event IDs 4624, 4625), but it doesn't contain sign out which is important for auditing but not meaningful for detection and has relatively high volume. Most of the data volume of this set is the login events and process creation event (event ID 4688).
- **Common** - Provide a full user audit trail in this set. For example, this set contains both user logins and user sign outs (event ID 4634). We include auditing actions like security group changes, key domain controller Kerberos operations, and other events that are recommended by industry organizations.

Events that have very low volume were included in the Common set as the main motivation to choose it over all the events is to reduce the volume and not to filter out specific events.

Here is a complete breakdown of the Security and App Locker event IDs for each set:

| DATA TIER | COLLECTED EVENT INDICATORS |
|-----------|--|
| Minimal | 1102,4624,4625,4657,4663,4688,4700,4702,4719,4720,4722,4723,4724,4727,4728,4732,4735,4737,4739,4740,4754,4755, |
| | 4756,4767,4799,4825,4946,4948,4956,5024,5033,8001,8002,8003,8004,8005,8006,8007,8222 |
| Common | 1,299,300,324,340,403,404,410,411,412,413,431,500,501,1100,1102,1107,1108,4608,4610,4611,4614,4622, |
| | 4624,4625,4634,4647,4648,4649,4657,4661,4662,4663,4665,4666,4667,4688,4670,4672,4673,4674,4675,4689,4697, |
| | 4700,4702,4704,4705,4716,4717,4718,4719,4720,4722,4723,4724,4725,4726,4727,4728,4729,4733,4732,4735,4737, |
| | 4738,4739,4740,4742,4744,4745,4746,4750,4751,4752,4754,4755,4756,4757,4760,4761,4762,4764,4767,4768,4771, |
| | 4774,4778,4779,4781,4793,4797,4798,4799,4800,4801,4802,4803,4825,4826,4870,4886,4887,4888,4893,4898,4902, |
| | 4904,4905,4907,4931,4932,4933,4946,4948,4956,4985,5024,5033,5059,5136,5137,5140,5145,5632,6144,6145,6272, |
| | 6273,6278,6416,6423,6424,8001,8002,8003,8004,8005,8006,8007,8222,26401,30004 |

NOTE

- If you are using Group Policy Object (GPO), it is recommended that you enable audit policies Process Creation Event 4688 and the *CommandLine* field inside event 4688. For more information about Process Creation Event 4688, see Security Center's [FAQ](#). For more information about these audit policies, see [Audit Policy Recommendations](#).
- To enable data collection for [Adaptive Application Controls](#), Security Center configures a local AppLocker policy in Audit mode to allow all applications. This will cause AppLocker to generate events which are then collected and leveraged by Security Center. It is important to note that this policy will not be configured on any machines on which there is already a configured AppLocker policy.
- To collect Windows Filtering Platform [Event ID 5156](#), you need to enable [Audit Filtering Platform Connection](#) (Auditpol /set /subcategory:"Filtering Platform Connection" /Success:Enable)

To choose your filtering policy:

1. On the **Data Collection** page, select your filtering policy under **Security Events**.
2. Select **Save**.

The screenshot shows the 'Data Collection' page in the Microsoft Security Center. At the top, there is a 'Save' button. Below it, a section titled 'Auto Provisioning' has a switch set to 'On'. Under 'Default workspace configuration', the 'Use workspace(s) created by Security Center (default)' option is selected. A note indicates that Azure VMs will report to workspaces created by Security Center. Below this, there are two other options: 'Use another workspace' (selected) and a dropdown menu labeled 'Choose a workspace'. A informational callout box states that other solutions enabled on the selected workspace will be applied to Azure VMs connected to it, and advises selecting a workspace in the desired region. At the bottom, a red box highlights the 'Security Events' section. This section allows selecting the type of events to collect: 'All Events' (selected), 'Common', 'Minimal', or 'None'. A note for 'Common' specifies that a standard set of events will be collected for security and audit purposes. The 'Minimal' note states that Security Center collects the minimal set required for threat detection, noting it won't provide a full audit trail. The 'None' note states that no security or AppLocker events will be collected, with data from agent assessments like Endpoint protection, OS Configuration and Updates used instead.

Automatic provisioning in cases of a pre-existing agent installation

The following use cases specify how automatic provision works in cases when there is already an agent or extension installed.

- Log Analytics Agent is installed on the machine, but not as an extension (Direct agent)
If the Log Analytics Agent is installed directly on the VM (not as an Azure extension), Security Center will install the Log Analytics Agent extension, and may upgrade the Log Analytics Agent to the latest version. The agent installed will continue to report to its already configured workspace(s), and additionally will report to the workspace configured in Security Center (Multi-homing is supported on Windows machines). If the configured workspace is a user workspace (not Security Center's default workspace), then you will need to install the "security"/"securityFree" solution on it for Security Center to start processing events from VMs and computers reporting to that workspace.

For Linux machines, Agent multi-homing is not yet supported - hence, if an existing agent installation is detected, automatic provisioning will not occur and the machine's configuration will not be altered.

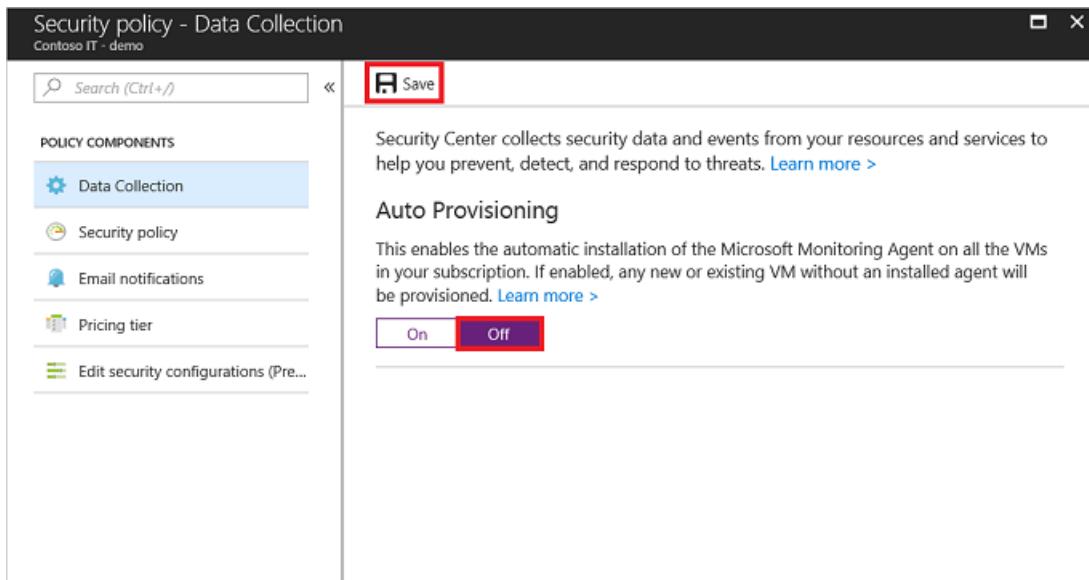
For existing machines on subscriptions onboarded to Security Center before 2019-03-17, when an existing agent will be detected, the Log Analytics Agent extension will not be installed and the machine will not be affected. For these machines, see to the "Resolve monitoring agent health issues on your machines" recommendation to resolve the agent installation issues on these machines.

- System Center Operations Manager agent is installed on the machine
Security center will install the Log Analytics Agent extension side-by-side to the existing Operations Manager. The existing Operations Manager agent will continue to report to the Operations Manager server normally. Note that the Operations Manager agent and Log Analytics Agent share common run-time libraries, which will be updated to the latest version during this process. Note - If Operations Manager agent version 2012 is installed, **do not** turn automatic provisioning On.
- A pre-existing VM extension is present
 - When the Monitoring Agent is installed as an extension, the extension configuration allows reporting to only a single workspace. Security Center does not override existing connections to user workspaces. Security Center will store security data from the VM in the workspace already connected, provided that the "security" or "securityFree" solution has been installed on it. Security Center may upgrade the extension version to the latest version in this process.
 - To see to which workspace the existing extension is sending data to, run the test to [Validate connectivity with Azure Security Center](#). Alternatively, you can open Log Analytics workspaces, select a workspace, select the VM, and look at the Log Analytics agent connection.
 - If you have an environment where the Log Analytics agent is installed on client workstations and reporting to an existing Log Analytics workspace, review the list of [operating systems supported by Azure Security Center](#) to make sure your operating system is supported. For more information, see [Existing log analytics customers](#).

Turn off automatic provisioning

You can turn off automatic provisioning from resources at any time by turning off this setting in the security policy.

1. Return to the Security Center main menu and select the Security policy.
2. Click **Edit settings** in the row of the subscription for which you want to disable automatic provisioning.
3. On the **Security policy – Data Collection** blade, under **Auto provisioning** select **Off**.
4. Select **Save**.



When auto provisioning is disabled (turned off), the default workspace configuration section is not displayed.

If you switch off auto provision after it was previously on:

- Agents will not be provisioned on new VMs.
- Security Center stops collecting data from the default workspace.

NOTE

Disabling automatic provisioning does not remove the Log Analytics Agent from Azure VMs where the agent was provisioned. For information on removing the OMS extension, see [How do I remove OMS extensions installed by Security Center](#).

Manual agent provisioning

There are several ways to install the Log Analytics Agent manually. When installing manually, make sure you disable auto provisioning.

Operations Management Suite VM extension deployment

You can manually install the Log Analytics Agent, so Security Center can collect security data from your VMs and provide recommendations and alerts.

1. Select Auto provision – OFF.
2. Create a workspace and set the pricing tier for the workspace you intend to set the Log Analytics Agent:
 - a. In the Security Center main menu, select **Security policy**.
 - b. Select the Workspace in which you intend to connect the agent. Make sure the workspace is in the same subscription you use in Security Center and that you have read/write permissions on the workspace.

The screenshot shows the Azure Security Center - Security policy interface. On the left, there's a navigation pane with sections like General, Policy & Compliance, Resource Security Hygiene, and Threat Protection. Under Policy & Compliance, the 'Security policy' option is highlighted with a red box. The main area is titled 'Policy Management' and displays a table of '3 SUBSCRIPTIONS' and '9 WORKSPACES'. One subscription, 'contoso-1', is listed with a preview note: '[Preview]: Enable Monitoring in Azure Secu 50% Standard'. There's a 'Edit settings >' button next to it.

3. Set the pricing tier.

The screenshot shows the 'Settings - Pricing tier' page for 'APEX C+L - Aquent Vendor Subscriptions'. The left sidebar lists settings: Pricing tier, Data Collection, Email notifications, Threat detection, Workflow automation (Preview), and Continuous export (Preview). The main area compares two tiers:

- Free (for Azure resources only):**
 - ✓ Continuous assessment and security recommendations
 - ✓ Azure Secure Score
 - ✗ Just in time VM Access
 - ✗ Adaptive application controls and network hardening
 - ✗ Regulatory compliance dashboard and reports
 - ✗ Threat protection for Azure VMs and non-Azure servers (including Server EDR)
 - ✗ Threat protection for supported PaaS services
- Standard:**
 - ✓ Continuous assessment and security recommendations
 - ✓ Azure Secure Score
 - ✓ Just in time VM Access
 - ✓ Adaptive application controls and network hardening
 - ✓ Regulatory compliance dashboard and reports
 - ✓ Threat protection for Azure VMs and non-Azure servers (including Server EDR)
 - ✓ Threat protection for supported PaaS services

A note at the bottom states: 'Pricing will apply to: 20 resources in this subscription'.

NOTE

If the workspace already has a **Security** or **SecurityCenterFree** solution enabled, the pricing will be set automatically.

4. If you want to deploy the agents on new VMs using a Resource Manager template, install the OMS virtual machine extension:
 - a. [Install the OMS virtual machine extension for Windows](#)
 - b. [Install the OMS virtual machine extension for Linux](#)
5. To deploy the extensions on existing VMs, follow the instructions in [Collect data about Azure Virtual](#)

Machines.

NOTE

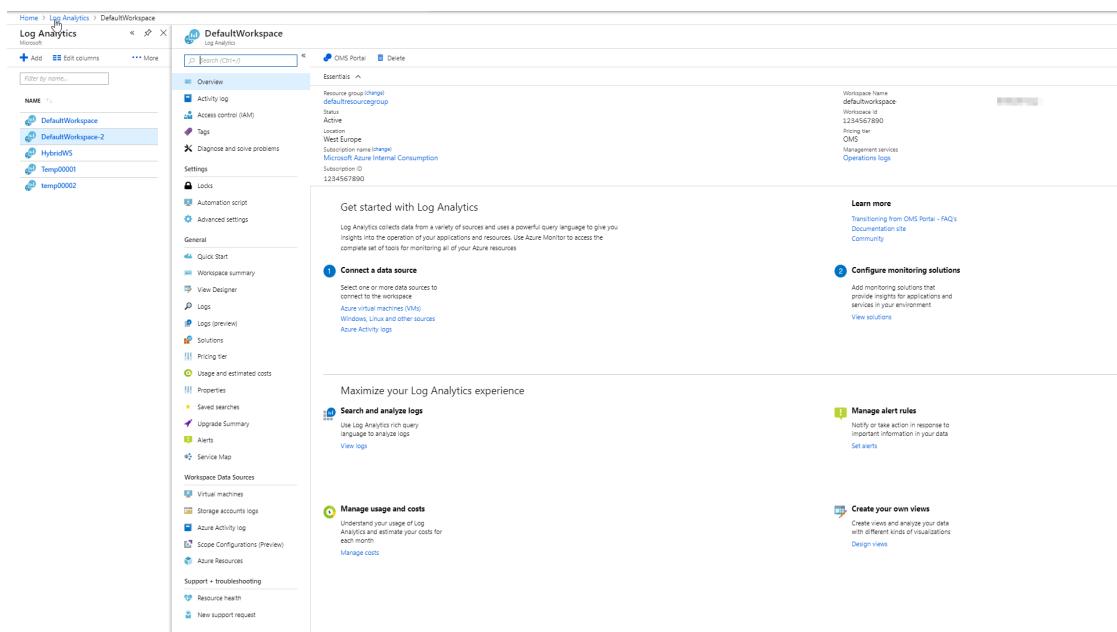
The section **Collect event and performance data** is optional.

6. To use PowerShell to deploy the extension, use the following PowerShell example:

NOTE

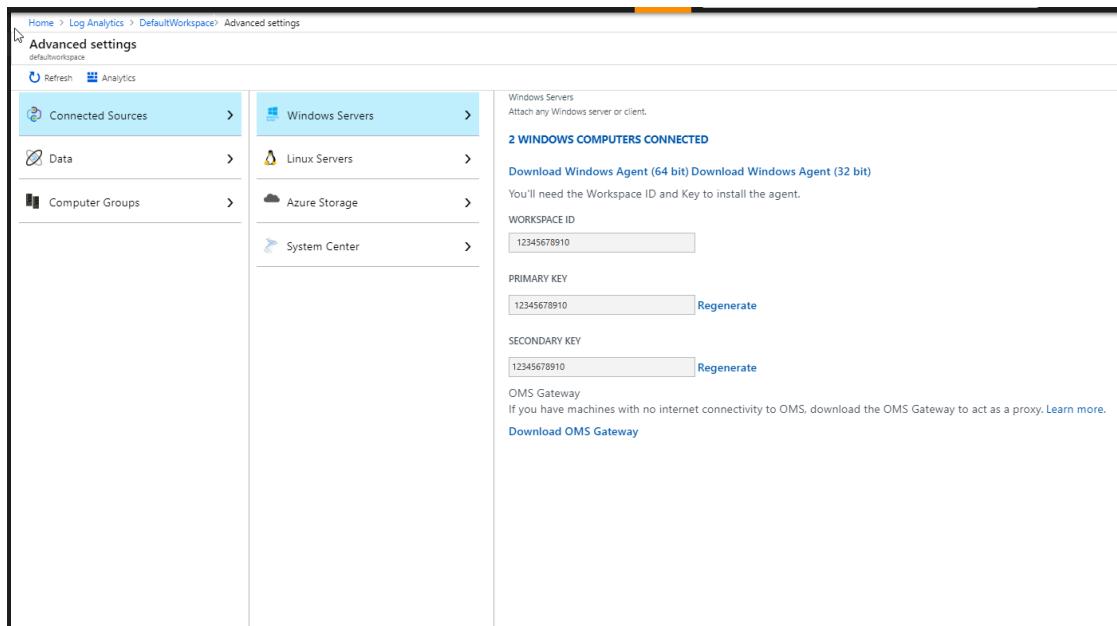
This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

- Go to **Log Analytics** and click on **Advanced settings**.



The screenshot shows the Azure Log Analytics workspace overview page for 'DefaultWorkspace'. On the left, there's a sidebar with 'NAME' and a list of workspaces: DefaultWorkspace, DefaultWorkspace-2, HybridWS, Temp00001, and temp0002. The main area has sections like 'Overview', 'Essentials', 'Get started with Log Analytics', 'Maximize your Log Analytics experience', 'Configure monitoring solutions', 'Manage alert rules', and 'Create your own views'. A prominent blue link labeled 'Advanced settings' is located in the 'Overview' section. On the right, there's a summary card with workspace details: Name (defaultworkspace), Resource group (hengel), Location (West Europe), Subscription name (hengel), and Management services (Operations logs). Below the card, there are links to 'Learn more', 'Configure monitoring solutions', 'Manage alert rules', and 'Create your own views'.

- Copy the values out of **WorkspaceID** and **Primary key**.



The screenshot shows the 'Advanced settings' page for the 'DefaultWorkspace'. On the left, there's a sidebar with 'Connected Sources' (Connected Sources, Data, Computer Groups) and 'Analytics' (Refresh, Analytics). The main area has sections for 'Windows Servers', '2 WINDOWS COMPUTERS CONNECTED', 'Download Windows Agent (64 bit)', 'Download Windows Agent (32 bit)', 'WORKSPACE ID' (input field: 12345678910), 'PRIMARY KEY' (input field: 12345678910, Regenerate button), 'SECONDARY KEY' (input field: 12345678910, Regenerate button), 'OMS Gateway' (text: If you have machines with no internet connectivity to OMS, download the OMS Gateway to act as a proxy. [Learn more](#)), and 'Download OMS Gateway'.

- Populate the public config and the private config with these values:

```
$PublicConf = @{
    "workspaceId"= "<WorkspaceID value>"
}

$PrivateConf = @{
    "workspaceKey"= "<Primary key value>"
}
```

- When installing on a Windows VM:

```
Set-AzVMExtension -ResourceGroupName $vm.ResourceGroupName -VMName $vm.Name -Name
"MicrosoftMonitoringAgent" -Publisher "Microsoft.EnterpriseCloud.Monitoring" -
ExtensionType "MicrosoftMonitoringAgent" -TypeHandlerVersion '1.0' -Location $vm.Location
-settings $PublicConf -ProtectedSettingString $PrivateConf -ForceRerun True
```

- When installing on a Linux VM:

```
Set-AzVMExtension -ResourceGroupName $vm1.ResourceGroupName -VMName $vm1.Name -Name
"OmsAgentForLinux" -Publisher "Microsoft.EnterpriseCloud.Monitoring" -ExtensionType
"OmsAgentForLinux" -TypeHandlerVersion '1.0' -Location $vm.Location -Settingstring
$PublicConf -ProtectedSettingString $PrivateConf -ForceRerun True`
```

NOTE

For instructions on how to onboard Security Center using PowerShell, see [Automate onboarding of Azure Security Center using PowerShell](#).

Troubleshooting

- To identify automatic provision installation issues, see [Monitoring agent health issues](#).
- To identify monitoring agent network requirements, see [Troubleshooting monitoring agent network requirements](#).
- To identify manual onboarding issues, see [How to troubleshoot Operations Management Suite onboarding issues](#).
- To identify Unmonitored VMs and computers issues:

A VM or computer is unmonitored by Security Center if the machine is not running the Microsoft Monitoring Agent extension. A machine may have a local agent already installed, for example the OMS direct agent or the System Center Operations Manager agent. Machines with these agents are identified as unmonitored because these agents are not fully supported in Security Center. To fully benefit from all of Security Center's capabilities, the Microsoft Monitoring Agent extension is required.

For more information about the reasons Security Center is unable to successfully monitor VMs and computers initialized for automatic provisioning, see [Monitoring agent health issues](#).

Next steps

This article showed you how data collection and automatic provisioning in Security Center works. To learn more about Security Center, see the following:

- [Azure Security Center FAQ](#)--Find frequently asked questions about using the service.
- [Security health monitoring in Azure Security Center](#)--Learn how to monitor the health of your Azure

resources.

Threat protection for Azure Key Vault (preview)

2/27/2020 • 2 minutes to read • [Edit Online](#)

Advanced threat protection for Azure Key Vault provides an additional layer of security intelligence. This tool detects potentially harmful attempts to access or exploit Key Vault accounts. Using the native advanced threat protection in Azure Security Center, you can address threats without being a security expert, and without learning additional security monitoring systems.

When Security Center detects anomalous activity, it displays alerts. It also emails the subscription administrator with details of the suspicious activity and recommendations for how to investigate and remediate the identified threats.

Configuring threat protection from Security Center

By default, advanced threat protection is enabled for all of your Key Vault accounts when you subscribe to Security Center's standard pricing tier. For more information, see [Pricing](#).

To enable or disable the protection for a specific subscription:

1. From the left pane in Security Center, select **Pricing & settings**.
2. Select the subscription with the storage accounts for which you want to enable or disable threat protection.
3. Select **Pricing tier**.
4. From the **Select pricing tier by resource type** group, find the **Key Vaults** row and select **Enabled** or **Disabled**.

The screenshot shows the 'Settings - Pricing tier' page for a subscription named 'QA-RomeCore GEO Test1-CoreDev1'. The 'Pricing tier' section is selected in the left sidebar. A callout box highlights the 'Standard' tier, which includes continuous assessment, security recommendations, Azure Secure Score, Just in time VM Access, Adaptive application controls, network hardening, regulatory compliance dashboard, threat protection for Azure VMs and non-Azure servers (including Server EDR), and threat protection for supported PaaS services. Below this, a note states 'Pricing will apply to: 27 resources in this subscription'. A table lists the resource types and their current status: Virtual machines (Enabled, Disabled), PaaS SQL servers (Enabled, Disabled), App Service (Enabled, Disabled), Storage accounts (Enabled, Disabled), Kubernetes Services (Enabled, Disabled), Container Registries (Enabled, Disabled), and Key Vaults (Enabled, Disabled). At the bottom, a note states: 'By clicking Save, the standard tier will be enabled on selected resource types. The first 30 days are free. Virtual machines, SQL servers and App Service instances are billed hourly, only for running resources. For more information on Security Center pricing, visit the [pricing page](#)'.

| RESOURCE TYPE | RESOURCE QUANTITY | PRICING | PLAN |
|----------------------|--------------------------------|-------------------------|--|
| Virtual machines | 7 VMs and VMSS instances | \$15/Server/Month | Enabled Disabled |
| PaaS SQL servers | 2 resources | \$15/Server/Month | Enabled Disabled |
| App Service | 1 instances | \$15/Instance/Month | Enabled Disabled |
| Storage accounts | 11 Storage accounts | \$0.02/10K Transactions | Enabled Disabled |
| Kubernetes Services | 0 Kubernetes services VM cores | \$1/VM Core | Enabled Disabled |
| Container Registries | 3 Container registries | \$0.29/Scan | Enabled Disabled |
| Key Vaults | 3 Key vaults | | Enabled Disabled |

5. Select **Save**.

Next steps

In this article, you learned how to enable and disable advanced threat protection for Azure Key Vault.

For related material, see the following articles:

- [Threat protection in Azure Security Center](#)--This article describes the sources of security alerts in Azure Security Center.
- [Key Vault security alerts](#)--The Key Vault section of the reference table for all Azure Security Center alerts

Provide security contact details in Azure Security Center

2/25/2020 • 2 minutes to read • [Edit Online](#)

Azure Security Center will recommend that you provide security contact details for your Azure subscription if you haven't already. This information will be used by Microsoft to contact you if the Microsoft Security Response Center (MSRC) discovers that your customer data has been accessed by an unlawful or unauthorized party. MSRC performs select security monitoring of the Azure network and infrastructure and receives threat intelligence and abuse complaints from third parties.

An email notification is sent on the first daily occurrence of an alert and only for high severity alerts. Email preferences can only be configured for subscription policies. Resource groups within a subscription will inherit these settings. Alerts are available only in the Standard tier of Azure Security Center.

Alert email notifications are sent:

- Only for high severity alerts
- To a single email recipient per alert type per day
- No more than 3 email messages are sent to a single recipient in a single day
- Each email message contains a single alert, not an aggregation of alerts

For example, if an email message was already sent to alert you about an RDP attack, you will not receive another email message about an RDP attack on the same day, even if another alert is triggered.

NOTE

This document introduces the service by using an example deployment. This is not a step-by-step guide.

Set up email notifications for alerts

1. From the portal, select **Pricing & settings**.
2. Click on the subscription.
3. Click **Email notifications**.

NOTE

If you are implementing a recommendation, then Under **Recommendations**, select **Provide security contact details**, select the Azure subscription to provide contact information on. This opens **Email notifications**.

Email notifications

 Save

 Please provide security contact details below. We will use them to contact you in case our security team finds that your resources are compromised.

Security contact emails 

Phone number 

Send me emails

Send me emails about alerts  On Off

Send email also to subscription owners On Off

 Notice that emails are sent from a US-based service regardless of the affected resource region.

- Enter the security contact email address or addresses separated by commas. There is not a limit to the number of email addresses that you can enter.
- Enter one security contact international phone number.
- To receive emails about high severity alerts, turn on the option **Send me emails about alerts**.
- You have the option to send email notifications to subscription owners (classic Service Administrator and Co-Administrators, plus RBAC Owner role at the subscription scope).
- Select **Save** to apply the security contact information to your subscription.

See also

To learn more about Security Center, see the following:

- [Setting security policies in Azure Security Center](#) -- Learn how to configure security policies for your Azure subscriptions and resource groups.
- [Managing security recommendations in Azure Security Center](#) -- Learn how recommendations help you protect your Azure resources.
- [Security health monitoring in Azure Security Center](#) -- Learn how to monitor the health of your Azure resources.
- [Managing and responding to security alerts in Azure Security Center](#) -- Learn how to manage and respond to security alerts.
- [Monitoring partner solutions with Azure Security Center](#) -- Learn how to monitor the health status of your partner solutions.

Upgrade to Standard tier for enhanced security

2/27/2020 • 3 minutes to read • [Edit Online](#)

Azure Security Center provides unified security management and advanced threat protection for workloads running in Azure, on-premises, and in other clouds. It delivers visibility and control over hybrid cloud workloads, active defenses that reduce your exposure to threats, and intelligent detection to help you keep pace with rapidly evolving cyber attacks.

Pricing tiers

Security Center is offered in two tiers:

- The **Free** tier is enabled on all your Azure subscriptions once you visit the Azure Security Center dashboard in the Azure portal for the first time, or if enabled programmatically via API. The free tier provides security policy, continuous security assessment, and actionable security recommendations to help you protect your Azure resources.
- The **Standard** tier extends the capabilities of the Free tier to workloads running in private and other public clouds, providing unified security management and threat protection across your hybrid cloud workloads. The standard tier also adds threat protection capabilities, which use built-in behavioral analytics and machine learning to identify attacks and zero-day exploits, access and application controls to reduce exposure to network attacks and malware, and more. In addition, standard tier adds vulnerability scanning for your virtual machines. You can try the standard tier for free. Security Center standard supports Azure resources including VMs, Virtual machine scale sets, App Service, SQL servers, and Storage accounts. If you have Azure Security Center standard, you can opt out of support based on resource type.

Most of the free tier security assessments for VMs, as well many of the standard tier security alerts, require the installation of the Microsoft Monitoring Agent (MMA) capability. You can enable Auto Provision on Security Center to automatically deploy the agent for your Azure VMs.

Try standard tier free for 30 days

The standard tier is free for the first 30 days. At the end of 30 days, should you choose to continue using the service, we will automatically start charging for usage.

You can upgrade an entire Azure subscription to the standard tier, which is inherited by all resources within the subscription.

To get the standard tier:

1. Select **Pricing & settings** on the **Security Center** main menu.
2. Select the subscription that you want to upgrade to standard.
3. Select **Pricing tier**.
4. Select **Standard** to upgrade.
5. Click **Save**.

Settings - Pricing tier

Test 4

Save

The Standard tier provides enhanced security. Learn more >

| Free (for Azure resources only) | Standard |
|--|--|
| ✓ Continuous assessment and security recommendations | ✓ Continuous assessment and security recommendations |
| ✓ Azure Secure Score | ✓ Azure Secure Score |
| ✗ Just in time VM Access | ✓ Just in time VM Access |
| ✗ Adaptive application controls and network hardening | ✓ Adaptive application controls and network hardening |
| ✗ Regulatory compliance dashboard and reports | ✓ Regulatory compliance dashboard and reports |
| ✗ Threat protection for Azure VMs and non-Azure servers (including Server EDR) | ✓ Threat protection for Azure VMs and non-Azure servers (including Server EDR) |
| ✗ Threat protection for supported PaaS services | ✓ Threat protection for supported PaaS services |

Pricing will apply to: 22 resources in this subscription

Select pricing tier by resource type

| Resource Type | Resource Quantity | Pricing | Plan |
|--------------------------------|--------------------------------|--------------------------|------------------|
| Virtual machines | 5 VMs and VMSS instances | (Price)/Server/Month | Enabled Disabled |
| PaaS SQL servers | 0 resources | (Price)/Server/Month | Enabled Disabled |
| App Service | 2 instances | (Price)/Instance/Month | Enabled Disabled |
| Storage accounts | 15 Storage accounts | (Price)/10K Transactions | Enabled Disabled |
| Kubernetes Services | 0 Kubernetes services VM cores | (Price)/VM Core/Month | Enabled Disabled |
| Container Registries (Preview) | 0 Container registries | (Price)/Image | Enabled Disabled |
| Key Vaults (Preview) | 0 Key vaults | (Price)/10K Transactions | Enabled Disabled |
| SQL servers on VMs (Preview) | 0 SQL servers on VMs | FREE during preview | Enabled Disabled |

By clicking Save, the standard tier will be enabled on selected resource types. The first 30 days are free. Virtual machines, SQL servers, App Service instances and Kubernetes Service instances are billed hourly, only for running resources. For more information on Security Center pricing, visit the [pricing page](#).

NOTE

To enable all Security Center features, you must apply the standard pricing tier to the subscription containing the applicable virtual machines. Configuring pricing for a workspace does not enable just-in-time VM access, adaptive application controls, and network detections for Azure resources.

Why upgrade to standard?

Security Center offers enhanced security and threat protection for your hybrid cloud workloads, including:

- **Hybrid security** – Get a unified view of security across all of your on-premises and cloud workloads. Apply security policies and continuously assess the security of your hybrid cloud workloads to ensure compliance with security standards. Collect, search, and analyze security data from multiple sources, including firewalls and other partner solutions.
- **Security alerts** - Use advanced analytics and the Microsoft Intelligent Security Graph to get an edge over evolving cyber-attacks. Leverage built-in behavioral analytics and machine learning to identify attacks and zero-day exploits. Monitor networks, machines, and cloud services for incoming attacks and post-breach activity. Streamline investigation with interactive tools and contextual threat intelligence.
- **Vulnerability scanning for virtual machines** - Easily deploy a scanner to all of your virtual machines that provides the industry's most advanced solution for vulnerability management. View, investigate, and remediate the findings directly within Security Center.
- **Access and application controls** - Block malware and other unwanted applications by applying machine learning powered whitelisting recommendations adapted to your specific workloads. Reduce the network attack surface with just-in-time, controlled access to management ports on Azure VMs. This drastically reduces exposure to brute force and other network attacks.

- **Container security features** - Benefit from vulnerability management and real-time threat protection on your containerized environments. When enabling the container registries resource, it may take up to 12hrs until all the features are enabled.

Next steps

In this article, you were introduced to pricing for Security Center. To learn more about the Standard tier's enhanced security and advanced threat protection, see:

- [Threat protection in Azure Security Center](#)
- [Just-in-time VM access control](#)
- [Container security overview](#)
- [Pricing details in your currency of choice, and according to your region](#)

Gain tenant-wide visibility for Azure Security Center

11/27/2019 • 7 minutes to read • [Edit Online](#)

This article explains how to manage your organization's security posture at scale by applying security policies to all Azure subscriptions linked to your Azure Active Directory tenant.

NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

Management groups

Azure management groups provide the ability to efficiently manage access, policies, and reporting on groups of subscriptions, as well as effectively manage the entire Azure estate by performing actions on the root management group. Each Azure AD tenant is given a single top-level management group called the root management group. This root management group is built into the hierarchy to have all management groups and subscriptions fold up to it. This group allows global policies and RBAC assignments to be applied at the directory level.

The root management group is created automatically when you do any of the following actions:

1. Opt in to use Azure management groups by navigating to **Management Groups** in the [Azure portal](#).
2. Create a management group via an API call.
3. Create a management group with PowerShell.

For a detailed overview of management groups, see the [Organize your resources with Azure management groups](#) article.

Create a management group in the Azure portal

You can organize subscriptions into management groups and apply your governance policies to the management groups. All subscriptions within a management group automatically inherit the policies applied to the management group. While management groups aren't required to onboard Security Center, it's highly recommended that you create at least one management group so the root management group is created. After the group is created, all subscriptions under your Azure AD tenant will be linked to it. For instructions for PowerShell and more information, see [Create management groups for resource and organization management](#).

1. Sign in to the [Azure portal](#).
2. Select **All services > Management groups**.
3. On the main page, select **New Management group**.

Management groups

contoso - PREVIEW

Root Management G... > Contoso Redmond

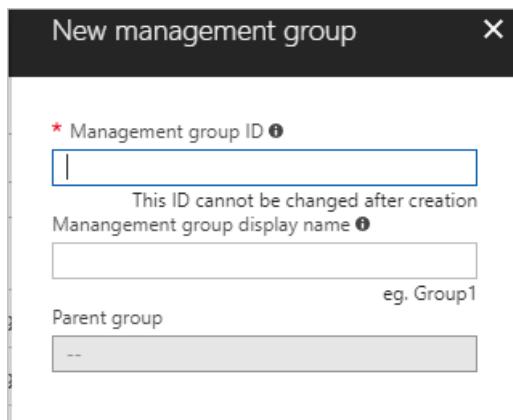
Search by name or ID

Using management groups helps you manage access, policy, and compliance by grouping multiple subscriptions together. [Learn more.](#)

| NAME | ID | TYPE | MY ROLE |
|-----------------------|-------------|------------------|---------|
| Azure Policy | azurepolicy | Management Group | Owner |
| Contoso IT | fabsub | Management Group | Owner |
| Contoso Marketing | Newgroup | Management Group | Owner |
| Global | Test123 | Management Group | Owner |
| Storefront | Storefront | Management Group | Owner |
| Azure Test Sub | | Subscription | Owner |
| BillNotifications | | Subscription | Owner |
| Groups | | Subscription | Owner |
| Legacy Groups Classic | | Subscription | Owner |
| mye2esubprod1-C | | Subscription | Owner |

4. Fill in the management group ID field.

- The **Management Group ID** is the directory unique identifier that is used to submit commands on this management group. This identifier isn't editable after creation as it is used throughout the Azure system to identify this group.
- The display name field is the name that is displayed within the Azure portal. A separate display name is an optional field when creating the management group and can be changed at any time.



5. Select **Save**

View management groups in the Azure portal

- Sign in to the [Azure portal](#).
- To view management groups, select **All services** under the Azure main menu.
- Under **General**, select **Management Groups**.

The screenshot shows the Microsoft Azure portal interface. On the left, there's a navigation bar with a 'Create a resource' button, a 'All services' button (which is highlighted with a red box), and a 'FAVORITES' section containing 'Dashboard'. The main area is titled 'All services' and shows a list of services under 'GENERAL (14)'. One service, 'Management Groups', is highlighted with a red box. To its right is a 'PREVIEW' status with a star icon.

Grant tenant-level visibility and the ability to assign policies

To get visibility into the security posture of all subscriptions registered in the Azure AD tenant, an RBAC role with sufficient read permissions is required to be assigned on the root management group.

Elevate access for a global administrator in Azure Active Directory

An Azure Active Directory tenant administrator doesn't have direct access to Azure subscriptions. However, as a directory administrator, they have the right to elevate themselves to a role that does have access. An Azure AD tenant administrator needs to elevate itself to user access administrator at the root management group level so they can assign RBAC roles. For PowerShell instructions and additional information, see [Elevate access for a Global administrator in Azure Active Directory](#).

1. Sign in to the [Azure portal](#) or the [Azure Active Directory admin center](#).
2. In the navigation list, click **Azure Active Directory** and then click **Properties**.

The screenshot shows the 'Default Directory - Properties' page in the Azure Active Directory admin center. The left sidebar has 'Azure Active Directory' selected (highlighted with a red box). The main pane shows the 'Properties' tab selected (also highlighted with a red box). Under the 'Access management for Azure resources' section, there's a note: 'John can manage access to all Azure subscriptions and management groups in this directory.' Below this is a switch with two options: 'Yes' (highlighted with a blue box) and 'No'.

3. Under **Access management for Azure resources**, set the switch to **Yes**.

Save Discard

* Name
Default Directory

Country or region
United States

Location
United States datacenters

Notification language
English

Directory ID
 

Technical contact

Global privacy contact

Privacy statement URL

Access management for Azure resources

John can manage access to all Azure subscriptions and management groups in this directory. [Learn more](#)

Yes No

- When you set the switch to Yes, you are assigned the User Access Administrator role in Azure RBAC at the root scope (/). This grants you permission to assign roles in all Azure subscriptions and management groups associated with this Azure AD directory. This switch is only available to users who are assigned the Global Administrator role in Azure AD.
- When you set the switch to No, the User Access Administrator role in Azure RBAC is removed from your user account. You can no longer assign roles in all Azure subscriptions and management groups that are associated with this Azure AD directory. You can view and manage only the Azure subscriptions and management groups to which you have been granted access.

4. Click **Save** to save your setting.

- This setting isn't a global property and applies only to the currently logged in user.

5. Perform the tasks you need to make at the elevated access. When you're done, set the switch back to **No**.

Assign RBAC roles to users

To gain visibility to all subscriptions, tenant administrators need to assign the appropriate RBAC role to any users they wish to grant tenant-wide visibility, including themselves, at the root management group level. The recommended roles to assign are either **Security Admin** or **Security Reader**. Generally, the Security Admin role is required to apply policies on the root level, while Security Reader will suffice to provide tenant-level visibility. For more information about the permissions granted by these roles, see the [Security Admin built-in role description](#) or the [Security Reader built-in role description](#).

Assign RBAC roles to users through the Azure portal:

- Sign in to the [Azure portal](#).
- To view management groups, select **All services** under the Azure main menu then select **Management Groups**.

3. Select a management group and click **details**.

The screenshot shows the Azure Management Groups interface. At the top, it says "Management groups" and "microsoft - PREVIEW". Below that, there's a search bar with "Search by name or ID" and a refresh button. A "New management group" button is also present. The main area shows a single management group named "MyTopMG" with a "details" link highlighted with a red box. Below the group name, there are sections for "NAME" and "ID", both of which show "No results".

4. Click **Access control (IAM)** then **Role assignments**.

5. Click **Add role assignment**.

6. Select the role to assign and the user, then click **Save**.

The screenshot shows the "MyTopMG - Access control (IAM)" page. On the left, there's a sidebar with "Overview", "Access control (IAM)" (which is selected and highlighted in blue), "Policies", "Cost Management", and "Cost analysis". The main area has a search bar and a "Add role assignment" button highlighted with a red box. Below that, there are tabs for "Check access" and "Role assignments" (which is selected). It shows a list of "33 items (32 Users, 1 Service Principals)". One item is listed: "BILLING CONTRIBUTOR" for "AK Ashish" (User type). To the right, an "Add role assignment" dialog box is open. It has a "Role" dropdown set to "Security Reader" (highlighted with a red box). Below it, "Assign access to" is set to "Azure AD user, group, or service principal". Under "Select", "admin" is chosen. A "Selected members" section says "No members selected. Search for and add one or more members you want to assign the role for this resource." At the bottom of the dialog are "Save" and "Discard" buttons.

Assign RBAC roles to users with PowerShell:

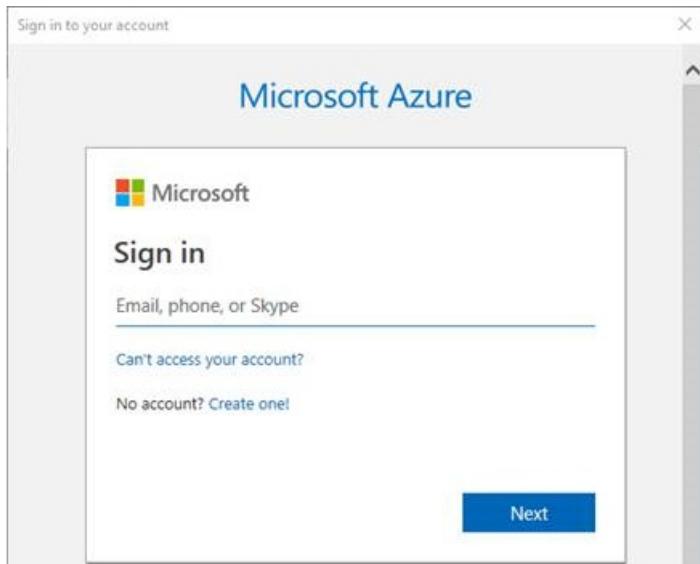
NOTE

This article has been updated to use the new Azure PowerShell Az module. You can still use the AzureRM module, which will continue to receive bug fixes until at least December 2020. To learn more about the new Az module and AzureRM compatibility, see [Introducing the new Azure PowerShell Az module](#). For Az module installation instructions, see [Install Azure PowerShell](#).

1. Install [Azure PowerShell](#).
2. Run the following commands:

```
# Login to Azure as a Global Administrator user
Connect-AzAccount
```

3. When prompted, sign in with global admin credentials.



4. Grant reader role permissions by running the following command:

```
# Add Reader role to the required user on the Root Management Group  
# Replace "user@domian.com" with the user to grant access to  
New-AzRoleAssignment -SignInName "user@domain.com" -RoleDefinitionName "Reader" -Scope "/"
```

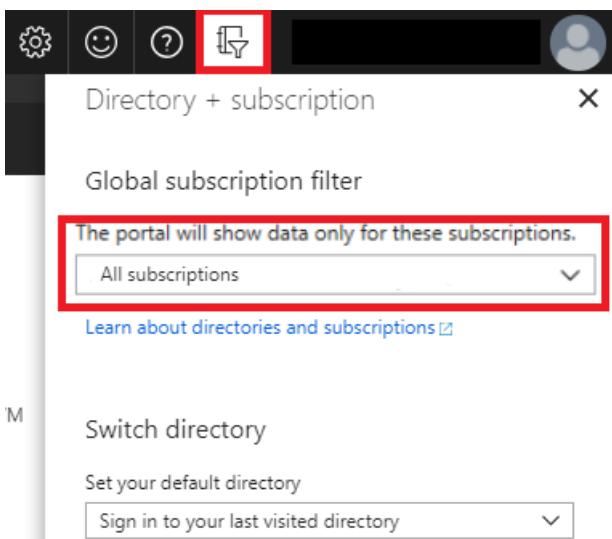
5. To remove the role, use the following command:

```
Remove-AzRoleAssignment -SignInName "user@domain.com" -RoleDefinitionName "Reader" -Scope "/"
```

Open or refresh Security Center

Once you have elevated access, open or refresh Azure Security Center to verify you have visibility into all subscriptions under your Azure AD tenant.

1. Sign in to the [Azure portal](#).
2. Make sure you select all the subscriptions in the subscription selector that you would like to view in Security Center.



3. Select **All services** under the Azure main menu then select **Security Center**.
4. In the **Overview**, there's a subscription coverage chart.

Subscription coverage

| Covered (Standard) | Covered (Free) | Not Covered |
|--------------------|----------------|-------------|
| 3 | 15 | 0 |

Policy compliance

- Overall compliance: 44%
- Least compliant subscriptions:
 - QA-Hybrid-Unification-Demo-Prod: 17%
 - Contoso IT - demo: 34%

- Click on **Coverage** to see the list of subscriptions covered.

| NAME | MY ROLE | OWNER | RESOURCES |
|------------------------------------|----------------|-------|-----------|
| Rome Core Scale Simulator 16 | ResourceAccess | | 40 |
| QA-RomeCore-Unification-Test3-prod | ResourceAccess | | 31 |
| QA-RomeCore-Unification-Test2-prod | ResourceAccess | | 23 |
| QA-RomeCore-Unification-Test1-prod | ResourceAccess | | 17 |
| QA-Test-Subscription-2 | ResourceAccess | | 16 |
| QA-Hybrid-Unification-Demo-Prod | ResourceAccess | | 14 |
| Rome Core Scale Simulator 15 | ResourceAccess | | 12 |

Remove elevated access

Once the RBAC roles have been assigned to the users, the tenant administrator should remove itself from the user access administrator role.

- Sign in to the [Azure portal](#) or the [Azure Active Directory admin center](#).
- In the navigation list, click **Azure Active Directory** and then click **Properties**.
- Under **Global admin can manage Azure Subscriptions and Management Groups**, set the switch to **No**.
- Click **Save** to save your setting.

Adding subscriptions to a management group

You can add subscriptions to the management group that you created. These steps aren't mandatory for gaining tenant-wide visibility and global policy and access management.

- Under **Management Groups**, select a management group to add your subscription to.

Home > Management Groups

Management Groups

New management group Refresh

Expand all

Search by name or text

| NAME | ID | TYPE | MY ROLE |
|----------------------|---------------------------------------|------------------|---------|
| ▼ [?] ACME Worldwide | 6b53f999-b591-4a71-b9f7-aa09b36884ef | Management Group | Owner |
| ▶ [?] Test1 | 6b53f999-b591-4a71-b9f7-aa09b36880re | Management Group | Owner |
| ▼ [?] RnD | 6b53f999-b591-4a71-b9f7-aa09b3688444 | Management Group | Owner |
| [?] QA | 6b53f999-b591-4a71-b9f7-aa09b3688443 | Management Group | Owner |
| [?] Test3 | 19031f08-5e3e-48f2-bbff-0e8fec34fe5a | Subscription | Owner |
| ▼ [?] Sales | 6b53f999-b591-448d-a4a2-ef70f6d3d580 | Management Group | Owner |
| [?] Global | 6b815b0a-7cc1-45ce-9db1-a7458d86f3b40 | Management Group | Owner |
| [?] Regional | 41abb2b6-f76e-473d-ac58-f49b64b3f492 | Management Group | Owner |
| [?] Test1 | e3662a89-b340-448d-a4a2-ef70f6d3d580 | Subscription | Owner |
| [?] Test2 | 6b815b0a-7cc1-45ce-9db1-a7458d86f3b4 | Subscription | Owner |

2. Select Add existing.

The screenshot shows the Azure portal interface for managing a management group named 'MyTopMG'. On the left, there's a sidebar with navigation links: 'Overview', 'Access control (IAM)', and 'Policies'. The main area displays basic information about the management group: Name (MyTopMG), ID (MyTopMG), and Access Level (Owner). Below this is a search bar and a table with one row labeled 'No result'. On the right, a modal window titled 'Add existing resource' is open. It has a 'PREVIEW' tab selected. Inside, there's a dropdown menu labeled 'Existing resource type' which is currently set to 'Subscription'. A note below it says 'Existing resource list' followed by a dropdown menu that is currently empty.

3. Enter subscription under Add existing resource and click Save.

4. Repeat steps 1 through 3 until you've added all the subscriptions in the scope.

NOTE

Management groups can contain both subscriptions and child management groups. When you assign a user an RBAC role to the parent management group, the access is inherited by the child management group's subscriptions. Policies set at the parent management group are also inherited by the children.

Next steps

In this article, you learned how to gain tenant-wide visibility for Azure Security Center. To learn more about Security Center, see the following articles:

[Security health monitoring in Azure Security Center](#)

[Manage and respond to security alerts in Azure Security Center](#)

Security recommendations in Azure Security Center

2/25/2020 • 2 minutes to read • [Edit Online](#)

This topic explains how to view and understand the recommendations in Azure Security Center to help you protect your Azure resources.

NOTE

This document introduces the service by using an example deployment. This document is not a step-by-step guide.

What are security recommendations?

Recommendations are actions for you to take in order to secure your resources.

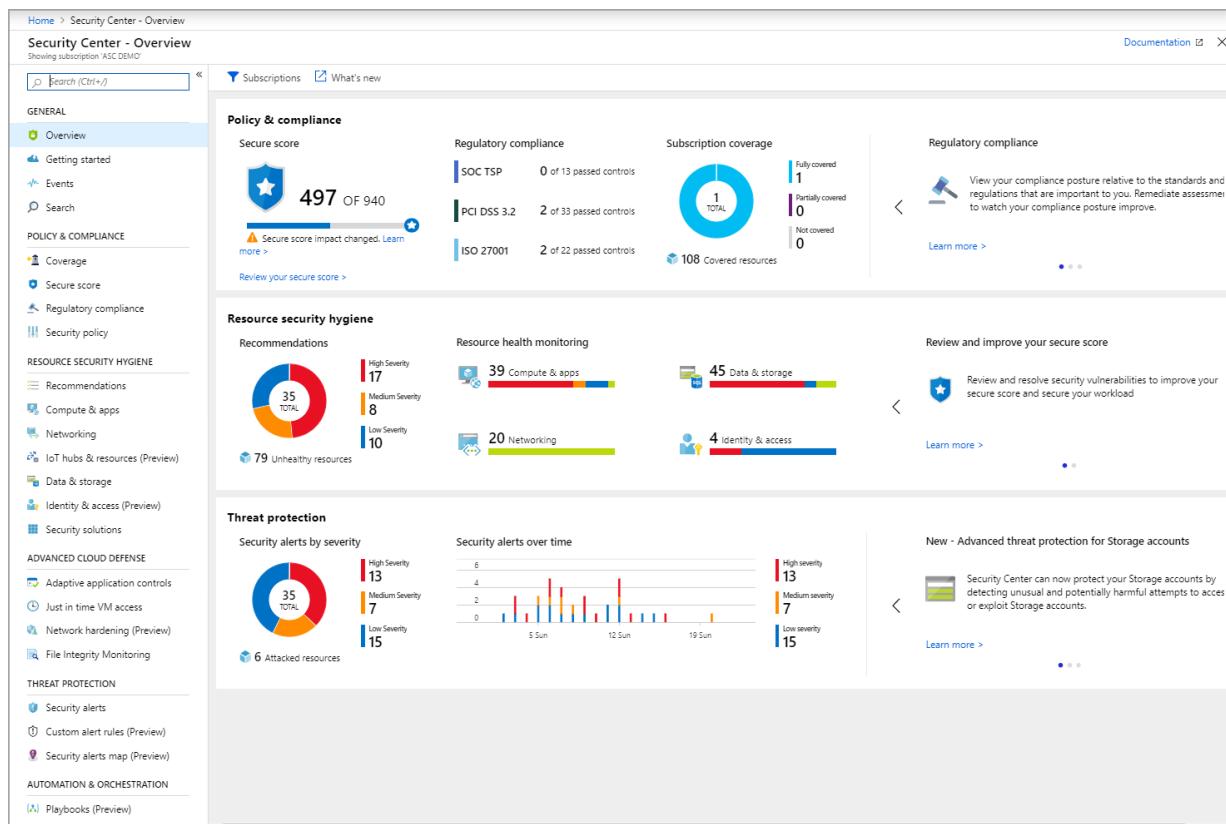
Security Center periodically analyzes the security state of your Azure resources to identify potential security vulnerabilities. It then provides you with recommendations on how to remove them.

Each recommendation provides you with:

- A short description of what is being recommended.
- The remediation steps to carry out in order to implement the recommendation.
- Which resources are in need of you performing the recommended action on them.
- The **Secure Score impact**, which is the amount that your Secure Score will go up if you implement this recommendation.

Monitor recommendations

Security Center analyzes the security state of your resources to identify potential vulnerabilities. The **Recommendations** tile under **Overview** shows the total number of recommendations identified by Security Center.



1. Select the **Recommendations tile** under **Overview**. The **Recommendations** list opens.

The screenshot shows the Recommendations blade. It has a header with a search bar and a table of recommendations. The table columns are RECOMMENDATION, SECURE SCORE IMPACT, FAILED RESOURCES, and SEVERITY. The table data includes:

| RECOMMENDATION | SECURE SCORE IMPACT | FAILED RESOURCES | SEVERITY |
|---|---------------------|-----------------------------------|----------|
| MFA should be enabled on accounts with owner permissions on your subscription (Preview) | +50 | 1 of 1 subscriptions | High |
| Install monitoring agent on virtual machine scale sets | +30 | 2 of 2 virtual machine scale s... | High |
| External accounts with write permissions should be removed from your subscription (Preview) | +30 | 1 of 1 subscriptions | Medium |
| MFA should be enabled on accounts with write permissionson your subscription (Preview) | +30 | 1 of 1 subscriptions | Medium |
| Vulnerabilities in security configuration on your machines should be remediated | +30 | 11 of 21 VMs & computers | Medium |
| MFA should be enabled on accounts with read permissions on your subscription (Preview) | +30 | 1 of 1 subscriptions | Medium |
| Install a vulnerability assessment solution on your virtual machines | +26 | 12 of 20 virtual machines | Medium |
| Web Application should only be accessible over HTTPS | +20 | 4 of 4 web applications | Medium |
| Secure transfer to storage accounts should be enabled | +18 | 30 of 33 storage accounts | High |
| Enable vulnerability assessment on your SQL servers | +15 | 4 of 4 SQL servers | High |
| Provision an Azure AD administrator for SQL server | +15 | 3 of 4 SQL servers | Medium |

You can filter recommendations. To filter the recommendations, select **Filter** on the **Recommendations** blade. The **Filter** blade opens and you select the severity and state values you wish to see.

- **RECOMMENDATIONS:** The recommendation.
- **SECURE SCORE IMPACT:** A score generated by Security Center using your security recommendations, and applying advanced algorithms to determine how crucial each recommendation is. For more information, see [Secure Score calculation](#).
- **RESOURCE:** Lists the resources to which this recommendation applies.
- **STATUS BARS:** Describes the severity of that particular recommendation:
 - **High (Red):** A vulnerability exists with a meaningful resource (such as an application, a VM,

or a network security group) and requires attention.

- **Medium (Orange):** A vulnerability exists and non-critical or additional steps are required to eliminate it or to complete a process.
- **Low (Blue):** A vulnerability exists that should be addressed but does not require immediate attention. (By default, low recommendations aren't presented, but you can filter on low recommendations if you want to see them.)
- **Healthy (Green):**
- **Not Available (Grey):**

2. To view each recommendation's details, click on the recommendation.

The screenshot shows the Azure Security Center - Overview > Recommendations section. A specific recommendation titled "MFA should be enabled on accounts with owner permissions on your subscription (Preview)" is selected. The recommendation details include:

- Description:** Multi-Factor Authentication (MFA) should be enabled for all subscription accounts with owner permissions to prevent a breach of accounts or resources. (Azure AD classic conditional access policies were not analyzed)
- General Information:**
 - Recommendation score: 0/50
 - Recommendation impact: +50
 - User impact: High
 - Implementation cost: Moderate
- Threats:**
 - Account breach
 - Elevation of privilege
- Remediation steps:** A link to "Enable MFA for accounts with owner permissions" is highlighted with a red box.
- Resource Summary:** 1 Unhealthy resource, 0 Healthy resources.
- Learn More:** Links to "Learn more about recommendations" and "Learn how to disable the recommendation".
- Subscription Details:** Shows "ASC DEMO" under the "SUBSCRIPTION" column.

NOTE

See [classic and Resource Manager deployment models](#) for Azure resources.

Next steps

In this document, you were introduced to security recommendations in Security Center. To learn how to remediate the recommendations:

- **Remediate recommendations** — Learn how to configure security policies for your Azure subscriptions and resource groups.

Remediate recommendations in Azure Security Center

2/25/2020 • 6 minutes to read • [Edit Online](#)

Recommendations give you suggestions on how to better secure your resources. You implement a recommendation by following the remediation steps provided in the recommendation.

Remediation steps

After reviewing all the recommendations, decide which one to remediate first. We recommend that you use the [Secure Score impact](#) to help prioritize what to do first.

1. From the list, click the recommendation.
2. Follow the instructions in the **Remediation steps** section. Each recommendation has its own set of instructions. The following screenshot shows remediation steps for configuring applications to only allow traffic over HTTPS.

The screenshot shows the Azure Security Center - Overview > Recommendations > Secure transfer to storage accounts should be enabled page. It includes sections for Description, General Information, Threats, and Remediation steps. The Remediation steps section is highlighted with a red border.

Description:
Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking.

General Information:

| Recommendation score | 10/20 | LEARN MORE |
|-----------------------|-------|---|
| Recommendation impact | +10 | Learn more about recommendations |
| User impact | Low | Learn how to disable the recommendation |
| Implementation effort | Low | |

Threats:

- Data exfiltration
- Data spillage
- Threat resistance

Remediation steps:

1-click fix remediation:
To remediate with a single click, in the Unhealthy resources tab (below), select the resources, and click "Remediate".
Read the remediation details in the confirmation box, insert the relevant parameters if required and approve the remediation.

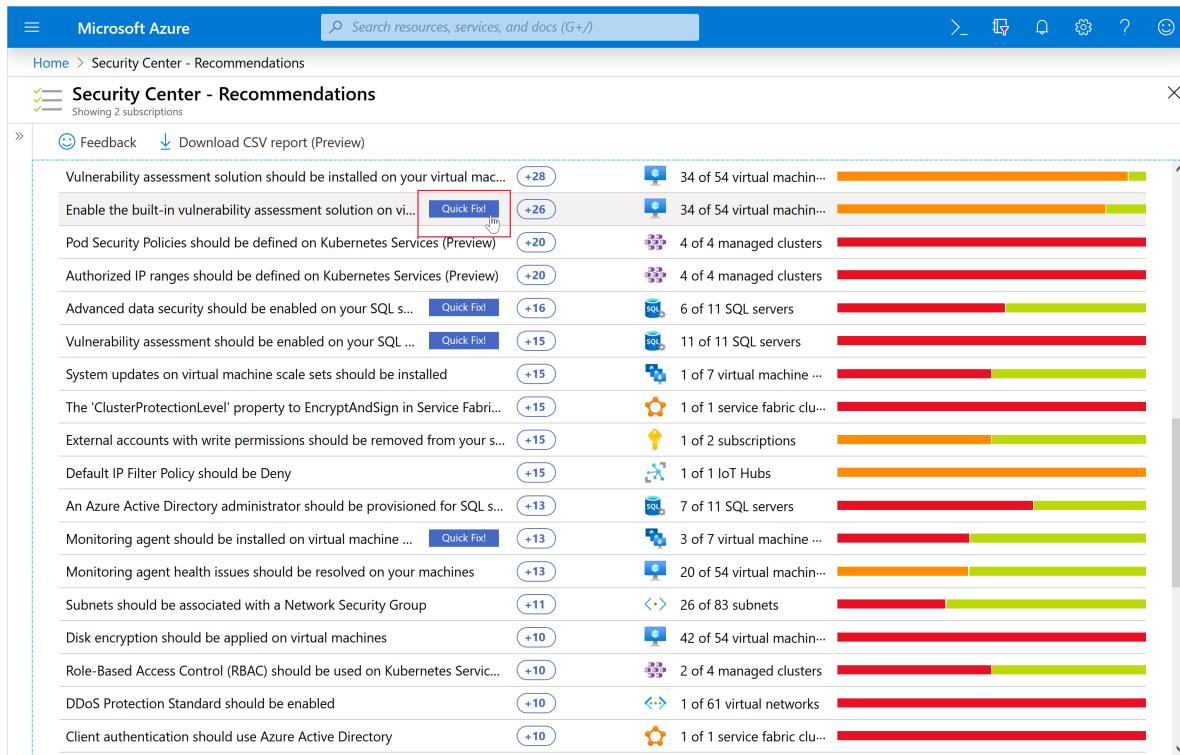
- Once completed, a notification appears informing you if the remediation succeeded.

Quick Fix remediation

Quick Fix enables you to quickly remediate a recommendation on multiple resources. It's only available for specific recommendations. Quick Fix simplifies remediation and enables you to quickly increase your Secure Score, improving your environment's security.

To implement Quick Fix remediation:

- From the list of recommendations that have the **Quick Fix!** label, click on the recommendation.



The screenshot shows the Microsoft Azure Security Center - Recommendations page. The left sidebar shows 'Home > Security Center - Recommendations' and 'Showing 2 subscriptions'. The main area lists various remediation tasks with their respective scores and progress bars. One task, 'Enable the built-in vulnerability assessment solution on vi...', has a 'Quick Fix!' button highlighted with a red box. The tasks listed include:

- Vulnerability assessment solution should be installed on your virtual mac... (+28)
- Enable the built-in vulnerability assessment solution on vi... **Quick Fix!** (+26)
- Pod Security Policies should be defined on Kubernetes Services (Preview) (+20)
- Authorized IP ranges should be defined on Kubernetes Services (Preview) (+20)
- Advanced data security should be enabled on your SQL s... **Quick Fix!** (+16)
- Vulnerability assessment should be enabled on your SQL ... **Quick Fix!** (+15)
- System updates on virtual machine scale sets should be installed (+15)
- The 'ClusterProtectionLevel' property to EncryptAndSign in Service Fabri... (+15)
- External accounts with write permissions should be removed from your s... (+15)
- Default IP Filter Policy should be Deny (+15)
- An Azure Active Directory administrator should be provisioned for SQL s... (+13)
- Monitoring agent should be installed on virtual machine ... **Quick Fix!** (+13)
- Monitoring agent health issues should be resolved on your machines (+13)
- Subnets should be associated with a Network Security Group (+11)
- Disk encryption should be applied on virtual machines (+10)
- Role-Based Access Control (RBAC) should be used on Kubernetes Servic... (+10)
- DDoS Protection Standard should be enabled (+10)
- Client authentication should use Azure Active Directory (+10)

Each task includes a progress bar indicating the number of resources affected. For example, 'Enable the built-in vulnerability assessment solution on vi...' has 34 of 54 virtual machines remediated, while 'Client authentication should use Azure Active Directory' has 1 of 1 service fabric clusters remediated.

- From the **Unhealthy resources** tab, select the resources that you want to implement the recommendation on, and click **Remediate**.

NOTE

Some of the listed resources might be disabled, because you don't have the appropriate permissions to modify them.

- In the confirmation box, read the remediation details and implications.

The screenshot shows the Azure Security Center interface for remediating a recommendation titled "Secure transfer to storage accounts should be enabled".

Secure transfer to storage accounts should be enabled

- Threat resistance

Remediation steps

1-click fix remediation: To remediate with a single click, in the Unhealthy resources tab (below), select the resources, and click "Remediate". Read the remediation details in the confirmation box, insert the relevant parameters if required and approve the remediation.

Note: It can take several minutes after remediation completes to see the resources in the 'healthy resources' tab.

Manual remediation: To enable secure transfer required:

- In your storage account, go to the 'Configuration' page.
- Enable 'Secure transfer required'.

Affected resources

Unhealthy resources (19) Healthy resources (19) Unscanned resources (0)

| NAME | SUBSCRIPTION |
|-----------------------|--------------|
| vm2nicwaf8426 | ASC D |
| vm2nicwaf9911 | ASC D |
| vm4nicwaf1394 | ASC D |
| vm4nicwaf7106 | ASC D |
| cleanupservicediag912 | ASC D |

Remediate

Was this recommendation useful? Yes No

Remediate resources

This action updates your storage account security to only allow requests by secure connections. (HTTPS).

SELECTED RESOURCES

- cleanupservicediag912
- vm4nicwaf1394
- vm2nicwaf426

Review the implications

Select resources to remediate and then click Remediate.

Run one-click remediation on the selected resource(s)

Remediate 3 resources **Cancel**

NOTE

The implications are listed in the grey box in the **Remediate resources** window that opens after clicking **Remediate**. They list what changes happen when proceeding with the Quick Fix remediation.

- Insert the relevant parameters if necessary, and approve the remediation.

NOTE

It can take several minutes after remediation completes to see the resources in the **Healthy resources** tab. To view the remediation actions, check the [activity log](#).

- Once completed, a notification appears informing you if the remediation succeeded.

Quick Fix remediation logging in the activity log

The remediation operation uses a template deployment or REST PATCH API call to apply the configuration on the resource. These operations are logged in [Azure activity log](#).

Recommendations with Quick Fix remediation

| RECOMMENDATION | IMPLICATION |
|----------------|-------------|
|----------------|-------------|

| RECOMMENDATION | IMPLICATION | |
|--|---|--|
| Auditing on SQL servers should be enabled | <p>This action will enable SQL auditing on these servers and their databases.</p> <p>Note:</p> <ul style="list-style-type: none"> For each region of the selected SQL servers, a storage account for saving audit logs will be created and shared by all the servers in that region. To ensure proper auditing, do not delete or rename the resource group or the storage accounts. | |
| Advanced data security should be enabled on your SQL managed instances | <p>This action will enable SQL Advanced Data Security (ADS) on the selected SQL managed instances.</p> <p>Note:</p> <ul style="list-style-type: none"> For each region and resource group of the selected SQL managed instances, a storage account for saving scan results will be created and shared by all the instances in that region. ADS is charged at \$15 per SQL managed instance. | |
| Vulnerability assessment should be enabled on your SQL managed instances | <p>This action will enable SQL Vulnerability Assessment on the selected SQL managed instances.</p> <p>Note:</p> <ul style="list-style-type: none"> SQL Vulnerability Assessment is part of the SQL Advanced Data Security (ADS) package. If ADS is not enabled already, it will automatically be enabled on the managed instance. For each region and resource group of the selected SQL managed instances, a storage account for storing scan results will be created and shared by all the instances in that region. ADS is charged at \$15 per SQL server. | |

| RECOMMENDATION | IMPLICATION | |
|--|--|--|
| Advanced Data Security should be enabled on your SQL servers | <p>This action will enable Advanced Data Security (ADS) on these selected servers and their databases.</p> <p>Note:</p> <ul style="list-style-type: none"> For each region and resource group of the selected SQL servers, a storage account for storing scan results will be created and shared by all the servers in that region.< ADS is charged at \$15 per SQL server. | |
| Vulnerability Assessment should be enabled on your SQL servers | <p>This action will enable SQL Vulnerability Assessment on these selected servers and their databases.</p> <p>Note:</p> <ul style="list-style-type: none"> SQL Vulnerability Assessment is part of the SQL Advanced Data Security (ADS) package. If ADS isn't enabled already, it will automatically be enabled on the SQL server. For each region and resource group of the selected SQL servers, a storage account for storing scan results will be created and shared by all the instances in that region. ADS is charged at \$15 per SQL server. | |
| Transparent data encryption on SQL databases should be enabled | <p>This action enables SQL Database Transparent Data Encryption (TDE) on the selected databases.</p> <p>Note: By default, service-managed TDE keys will be used.</p> | |
| Secure transfer to storage accounts should be enabled | <p>This action updates your storage account security to only allow requests by secure connections. (HTTPS).</p> <p>Note:</p> <ul style="list-style-type: none"> Any requests using HTTP will be rejected. When you're using the Azure files service, connection without encryption will fail, including scenarios using SMB 2.1, SMB 3.0 without encryption, and some flavors of the Linux SMB client. Learn more. | |

| RECOMMENDATION | IMPLICATION | |
|---|---|--|
| Web Application should only be accessible over HTTPS | <p>This action will redirect all traffic from HTTP to HTTPS, on the selected resources.</p> <p>Note:</p> <ul style="list-style-type: none"> • An HTTPS endpoint that doesn't have an SSL certificate will show up in the browser with a 'Privacy Error'. So users who have a custom domain need to verify they have set up an SSL certificate. • Make sure packet and web application firewalls protecting the app service, allow HTTPS sessions forwarding. | |
| Function App should only be accessible over HTTPS | <p>This action will redirect all traffic from HTTP to HTTPS, on the selected resources.</p> <p>Note:</p> <ul style="list-style-type: none"> • An HTTPS endpoint that doesn't have an SSL certificate will show up in the browser with a 'Privacy Error'. So users who have a custom domain need to verify they have set up an SSL certificate. • Make sure packet and web application firewalls protecting the app service, allow HTTPS sessions forwarding. | |
| API App should only be accessible over HTTPS | <p>This action will redirect all traffic from HTTP to HTTPS, on the selected resources.</p> <p>Note:</p> <ul style="list-style-type: none"> • An HTTPS endpoint that doesn't have an SSL certificate will show up in the browser with a 'Privacy Error'. So users who have a custom domain need to verify they have set up an SSL certificate. • Make sure packet and web application firewalls protecting the app service, allow HTTPS sessions forwarding. | |
| Remote debugging should be turned off for Web Application | This action disables remote debugging. | |
| Remote debugging should be turned off for Function App | This action disables remote debugging. | |
| Remote debugging should be turned off for API App | This action disables remote debugging. | |

| RECOMMENDATION | IMPLICATION | |
|---|---|--|
| CORS should not allow every resource to access your Web Application | <p>This action blocks other domains from accessing your Web Application. To allow specific domains, enter them in the Allowed origins field (separated by commas).</p> <p>Note: Leaving the field empty will block all cross-origin calls.'Param field title: 'Allowed origins'</p> | |
| CORS should not allow every resource to access your Function App | <p>This action blocks other domains from accessing your Function Application. To allow specific domains, enter them in the Allowed origins field (separated by commas).</p> <p>Note: Leaving the field empty will block all cross-origin calls.'Param field title: 'Allowed origins'</p> | |
| CORS should not allow every resource to access your API App | <p>This action blocks other domains from accessing your API Application. To allow specific domains, enter them in the Allowed origins field (separated by commas).</p> <p>Note: Leaving the field empty will block all cross-origin calls.'Param field title: 'Allowed origins'</p> | |
| Monitoring agent should be enabled on your virtual machines | <p>This action installs a monitoring agent on the selected virtual machines. Select a workspace for the agent to report to.</p> <ul style="list-style-type: none"> If your update policy is set to automatic, it will deploy on new existing instances. If your update policy is set to manual and you would like to install the agent on existing instances, select the check box option. Learn more | |
| Diagnostic logs in Key Vault should be enabled | This action enables diagnostic logs on key vaults. Diagnostic logs and metrics are saved in the selected workspace. | |
| Diagnostic logs in Service bus should be enabled | This action enables diagnostic logs on the service bus. Diagnostic logs and metrics are saved in the selected workspace. | |

Next steps

In this document, you were shown how to remediate recommendations in Security Center. To learn more about Security Center, see the following topics:

- [Setting security policies in Azure Security Center](#) - Learn how to configure security policies for your Azure subscriptions and resource groups.
- [Security health monitoring in Azure Security Center](#) - Learn how to monitor the health of your Azure

resources.

Strengthen your security posture with Azure Security Center

2/25/2020 • 2 minutes to read • [Edit Online](#)

This article helps you strengthen your security posture. Use the monitoring capabilities in Azure Security Center to make sure your resource security is as tight as possible and monitor compliance with policies.

How do you strengthen your security posture?

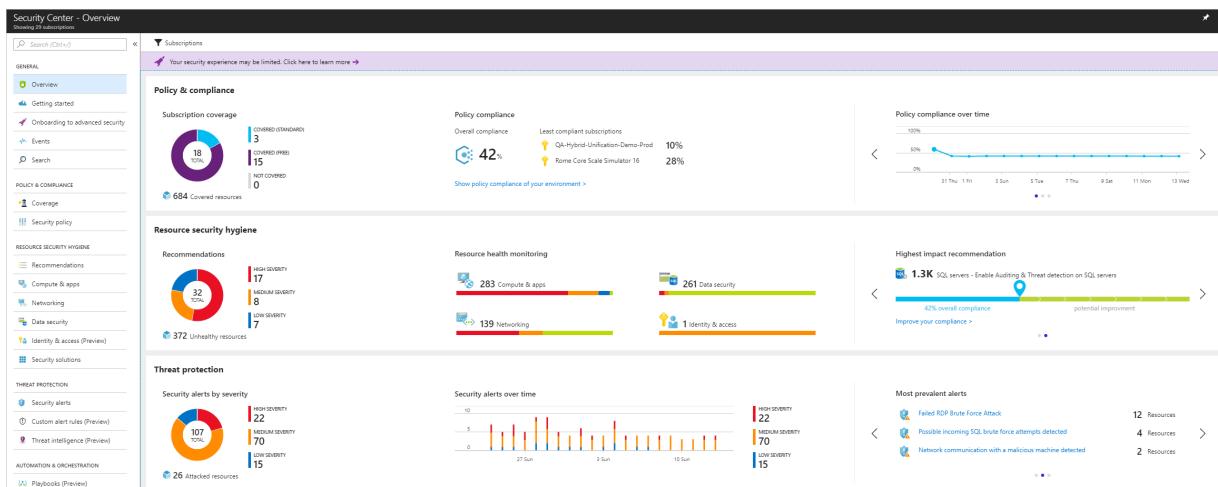
We often think of monitoring as watching and waiting for an event to occur so that we can react to the situation. Strengthening your security posture refers to having a proactive strategy that audits your resources to identify systems that do not meet organizational standards or best practices.

After you enable [security policies](#) for a subscription's resources, Security Center analyzes the security of your resources to identify potential vulnerabilities. Information about your network configuration is available instantly. Depending on the number of VMs and computers that you have with the agent installed, it may take an hour or more to collect information about VMs and computer's configuration, such as security update status and operating system configuration, to become available. You can view a full list of issues and ways to harden your network and remediate risk in the **Recommendations** tile.

You can view the security state of your resources and any issues per resource type:

- To monitor the health of your computer resources and your apps, and receive recommendations for improving their security, see [Protecting your machines and applications in Azure Security Center](#)
- To monitor your network resources, such as virtual machines, network security groups and endpoints, and receive recommendations for improving their security, see [Protecting your network in Azure Security Center](#) for more information.
- To monitor your data and storage resources, such as SQL servers and storage accounts, and receive recommendations for improving their security, see [Protecting Azure SQL service and data in Azure Security Center](#) for more information.
- To monitor your identity and access resources, including MFA and account permissions, and receive recommendations for improving their security, see [Monitor identity and access in Azure Security Center](#) for more information.
- To monitor just-in-time access to your resources, see [Manage virtual machine access using just-in-time](#) for more information.

For more information about how to apply recommendations, read [Implementing security recommendations in Azure Security Center](#).



See also

In this article, you learned how to use monitoring capabilities in Azure Security Center. To learn more about Azure Security Center, see the following:

- [Setting security policies in Azure Security Center](#): Learn how to configure security settings in Azure Security Center.
- [Managing and responding to security alerts in Azure Security Center](#): Learn how to manage and respond to security alerts.
- [Monitoring partner solutions with Azure Security Center](#): Learn how to monitor the health status of your partner solutions.

Security recommendations - a reference guide

2/25/2020 • 21 minutes to read • [Edit Online](#)

This article lists the recommendations you might see in Azure Security Center. The recommendations shown in your environment depend on the resources you're protecting and your customized configuration.

To learn about how to respond to these recommendations, see [Remediate recommendations in Azure Security Center](#).

Your Secure Score is based on how many Security Center recommendations you have mitigated. To prioritize the recommendations to resolve first, consider the severity of each.

Network recommendations

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|---|--------------|---|-----------------|
| Just-in-time network access control should be applied on virtual machines | Apply just-in-time (JIT) virtual machine (VM) access control to permanently lock down access to selected ports, and enable authorized users to open them, via JIT, for a limited amount of time only. (Related policy: Just-In-Time network access control should be applied on virtual machines) | High | N | Virtual machine |
| Network security groups on the subnet level should be enabled | Enable network security groups to control network access of resources deployed in your subnets. (Related policy: Subnets should be associated with a Network Security Group. This policy is disabled by default) | High/ Medium | N | Subnet |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|---|--|--------------|---|-----------------|
| Internet-facing virtual machines should be protected with Network Security Groups | <p>Enable Network Security Groups to control network access of your virtual machines.</p> <p>(Related policy: Internet-facing virtual machines should be protected with Network Security Groups)</p> | High/ Medium | N | Virtual machine |
| All network ports should be restricted on NSG associated to your VM | <p>Harden the network security groups of your Internet-facing VMs by restricting the access of your existing allow rules.</p> <p>This recommendation is triggered when any port is opened to <i>all</i> sources (except for ports 22, 3389, 5985, 5986, 80, and 1443).</p> <p>(Related policy: Access through internet facing endpoint should be restricted)</p> | High | N | Virtual machine |
| Adaptive Network Hardening recommendations should be applied on internet facing virtual machines | <p>Customers on the standard pricing tier will see this recommendation when the Adaptive Network Hardening feature finds an overly-permissive NSG rule.</p> <p>(Related policy: Adaptive Network Hardening recommendations should be applied on internet facing virtual machines)</p> | High | N | Virtual machine |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|--|----------|---|-----------------|
| The rules for web applications on IaaS NSGs should be hardened (DEPRECATED) | Harden the network security group (NSG) of your virtual machines that are running web applications, with NSG rules that are overly permissive with regards to web application ports. (Related policy: The NSGs rules for web applications on IaaS should be hardened) | High | N | Virtual machine |
| Access to App Services should be restricted (DEPRECATED) | Restrict access to your App Services by changing the networking configuration, to deny inbound traffic from ranges that are too broad. (Related policy: [Preview]: Access to App Services should be restricted) | High | N | App service |
| Management ports should be closed on your virtual machines | Harden the network security group of your virtual machines to restrict access to management ports. (Related policy: Management ports should be closed on your virtual machines) | High | N | Virtual machine |
| DDoS Protection Standard should be enabled | Protect virtual networks containing applications with public IPs by enabling DDoS protection service standard. DDoS protection enables mitigation of network volumetric and protocol attacks. (Related policy: DDoS Protection Standard should be enabled) | High | N | Virtual network |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|---|---|----------|---|-----------------|
| IP forwarding on your virtual machine should be disabled | Disable IP forwarding. When IP forwarding is enabled on a virtual machine's NIC, the machine can receive traffic addressed to other destinations. IP forwarding is rarely required (for example, when using the VM as a network virtual appliance), and therefore, this should be reviewed by the network security team. (Related policy: [Preview]: IP Forwarding on your virtual machine should be disabled) | Medium | N | Virtual machine |
| Web Application should only be accessible over HTTPS | Enable "HTTPS only" access for web applications. Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks. (Related policy: Web Application should only be accessible over HTTPS) | Medium | Y | Web application |
| Function App should only be accessible over HTTPS | Enable "HTTPS only" access for function apps. Use of HTTPS ensures server/service authentication and protects data in transit from network layer eavesdropping attacks. (Related policy: Function App should only be accessible over HTTPS) | Medium | Y | Function app |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|--|----------|---|-----------------|
| Secure transfer to storage accounts should be enabled | Enable secure transfer to storage accounts. Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). Use of HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks, such as man-in-the-middle, eavesdropping, and session-hijacking. (Related policy: Secure transfer to storage accounts should be enabled) | High | Y | Storage account |
| | | | | |

Container recommendations

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|---|----------|---|--------------------------------|
| Role-Based Access Control should be used to restrict access to a Kubernetes Service Cluster | To provide granular filtering of the actions that users can perform, use Role-Based Access Control (RBAC) to manage permissions in Kubernetes Service Clusters and configure relevant authorization policies. For more information see Azure role-based access control . (Related policy: [Preview]: Role-Based Access Control (RBAC) should be used on Kubernetes Services) | Medium | N | Compute resources (Containers) |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|---|---|----------|---|--------------------------------|
| The Kubernetes Service should be upgraded to the latest Kubernetes version | <p>Upgrade Azure Kubernetes Service clusters to the latest Kubernetes version in order to benefit from up-to-date vulnerability patches. For details regarding specific Kubernetes vulnerabilities see Kubernetes CVEs.</p> <p>(Related policy: [Preview]: Kubernetes Services should be upgraded to a non-vulnerable Kubernetes version)</p> | High | N | Compute resources (Containers) |
| Pod Security Policies should be defined to reduce the attack vector by removing unnecessary application privileges (Preview) | <p>Define Pod Security Policies to reduce the attack vector by removing unnecessary application privileges. It is recommended to configure pod security policies so pods can only access resources which they are allowed to access.</p> <p>(Related policy: [Preview]: Pod Security Policies should be defined on Kubernetes Services)</p> | Medium | N | Compute resources (Containers) |
| Access to a Kubernetes service management API should be limited by authorizing specific IP ranges only | <p>Restrict access to the Kubernetes service management API by granting API access only to IP addresses in specific ranges. It is recommended to configure authorized IP ranges so only applications from allowed networks can access the cluster.</p> <p>(Related policy: [Preview]: Authorized IP ranges should be defined on Kubernetes Services)</p> | High | N | Compute resources (Containers) |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|---|----------|---|--------------------------------|
| Vulnerabilities in Azure Container Registry images should be remediated (powered by Qualys) | Container image vulnerability assessment scans your registry for security vulnerabilities on each pushed container image and exposes detailed findings per image. Resolving the vulnerabilities can greatly improve your containers' security posture and protect them from attacks. (No related policy) | High | N | Compute resources (Containers) |
| | | | | |

App Service recommendations

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|---|--|----------|---|---------------|
| Web Application should only be accessible over HTTPS | Limit access of Web Applications over HTTPS only. (Related policy:) | Medium | N | App service |
| Function App should only be accessible over HTTPS | Limit access of Function Apps over HTTPS only. (Related policy:) | Medium | N | App service |
| API App should only be accessible over HTTPS | Limit access of API Apps over HTTPS only. (Related policy:) | Medium | N | App service |
| Remote debugging should be turned off for Web Applications | Turn off debugging for Web Applications if you no longer need to use it. Remote debugging requires inbound ports to be opened on a Web App. (Related policy: Remote debugging should be turned off for Web Application) | Low | Y | App service |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|---|--|----------|---|---------------|
| Remote debugging should be turned off for Function App | Turn off debugging for Function App if you no longer need to use it. Remote debugging requires inbound ports to be opened on a Function App. (Related policy: Remote debugging should be turned off for Function App) | Low | Y | App service |
| Remote debugging should be turned off for API App | Turn off debugging for API App if you no longer need to use it. Remote debugging requires inbound ports to be opened on an API App. (Related policy: Remote debugging should be turned off for API App) | Low | Y | App service |
| CORS should not allow every resource to access your Web Applications | Allow only required domains to interact with your web application. Cross origin resource sharing (CORS) should not allow all domains to access your web application. (Related policy: CORS should not allow every resource to access your Web Application) | Low | Y | App service |
| CORS should not allow every resource to access your Function App | Allow only required domains to interact with your function application. Cross origin resource sharing (CORS) should not allow all domains to access your function application. (Related policy: CORS should not allow every resource to access your Function App) | Low | Y | App service |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|---|----------|---|---------------|
| CORS should not allow every resource to access your API App | Allow only required domains to interact with your API application. Cross origin resource sharing (CORS) should not allow all domains to access your API application. (Related policy: CORS should not allow every resource to access your API App) | Low | Y | App service |
| Diagnostic logs in App Services should be enabled | Enable logs and retain them up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised. (Related policy: Diagnostic logs in App Services should be enabled) | Low | N | App service |
| | | | | |

Compute and app recommendations

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|---|----------|---|--------------------------------------|
| Diagnostic logs in Azure Stream Analytics should be enabled | Enable logs and retain them up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised. (Related policy: Diagnostic logs in Azure Stream Analytics should be enabled) | Low | Y | Compute resources (stream analytics) |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|---|--|----------|---|--------------------------------|
| Diagnostic logs in Batch accounts should be enabled | Enable logs and retain them up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised. (Related policy: Diagnostic logs in Batch accounts should be enabled) | Low | Y | Compute resources (batch) |
| Diagnostic logs in Event Hub should be enabled | Enable logs and retain them up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised. (Related policy: Diagnostic logs in Event Hub should be enabled) | Low | Y | Compute resources (event hub) |
| Diagnostic logs in Logic Apps should be enabled | Enable logs and retain them up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised. (Related policy: Diagnostic logs in Logic Apps should be enabled) | Low | Y | Compute resources (logic apps) |
| Diagnostic logs in Search services should be enabled | Enable logs and retain them up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised. (Related policy: Diagnostic logs in Search services should be enabled) | Low | Y | Compute resources (search) |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|---|----------|---|------------------------------------|
| Diagnostic logs in Service Bus should be enabled | <p>Enable logs and retain them up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised.</p> <p>(Related policy: Diagnostic logs in Service Bus should be enabled)</p> | Low | Y | Compute resources (service bus) |
| Service Fabric clusters should only use Azure Active Directory for client authentication | <p>Perform Client authentication only via Azure Active Directory in Service Fabric.</p> <p>(Related policy: Service Fabric clusters should only use Azure Active Directory for client authentication)</p> | High | N | Compute resources (service fabric) |
| Service Fabric clusters should have the ClusterProtectionLevel property set to EncryptAndSign | <p>Service Fabric provides three levels of protection (None, Sign, and EncryptAndSign) for node-to-node communication using a primary cluster certificate. Set the protection level to ensure that all node-to-node messages are encrypted and digitally signed.</p> <p>(Related policy: The ClusterProtectionLevel property to EncryptAndSign in Service Fabric should be set)</p> | High | N | Compute resources (service fabric) |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|--|----------|---|---------------------------------|
| All authorization rules except RootManageSharedAccessKey should be removed from Service Bus namespace | Service Bus clients should not use a namespace level access policy that provides access to all queues and topics in a namespace. To align with the least privilege security model, you should create access policies at the entity level for queues and topics to provide access to only the specific entity. (Related policy: All authorization rules except RootManageSharedAccessKey should be removed from Service Bus namespace) | Low | N | Compute resources (service bus) |
| All authorization rules except RootManageSharedAccessKey should be removed from Event Hub namespace | Event Hub clients should not use a namespace level access policy that provides access to all queues and topics in a namespace. To align with the least privilege security model, you should create access policies at the entity level for queues and topics to provide access to only the specific entity. (Related policy: All authorization rules except RootManageSharedAccessKey should be removed from Event Hub namespace) | Low | N | Compute resources (event hub) |
| Authorization rules on the Event Hub entity should be defined | Audit authorization rules on the Event Hub entity to grant least-privileged access. (Related policy: Authorization rules on the Event Hub entity should be defined) | Low | N | Compute resources (event hub) |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|--|----------|---|---------------|
| Install monitoring agent on your virtual machines | Install the Monitoring agent to enable data collection, updates scanning, baseline scanning, and endpoint protection on each machine. (Related policy: Monitoring agent should be enabled on your virtual machines) | High | Y | Machine |
| Monitoring agent health issues should be resolved on your machines | For full Security Center protection, resolve monitoring agent issues on your machines by following the instructions in the Troubleshooting guide (No related policy - dependent upon "Install monitoring agent on your virtual machines") | Medium | N | Machine |
| Adaptive Application Controls should be enabled on virtual machines | Enable application control to control which applications can run on your VMs located in Azure. This will help harden your VMs against malware. Security Center uses machine learning to analyze the applications running on each VM and helps you apply allow rules using this intelligence. This capability simplifies the process of configuring and maintaining application allow rules. (Related policy: Adaptive Application Controls should be enabled on virtual machines) | High | N | Machine |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|---|----------|---|---------------|
| Install endpoint protection solution on your machines | Install an endpoint protection solution on your Windows and Linux machines, to protect them from threats and vulnerabilities. (Related policy: Monitor missing Endpoint Protection in Azure Security Center) | Medium | N | Machine |
| Install endpoint protection solution on virtual machines | Install an endpoint protection solution on your virtual machines, to protect them from threats and vulnerabilities. (No related policy) | Medium | N | Machine |
| OS version should be updated for your cloud service roles | Update the operating system (OS) version for your cloud service roles to the most recent version available for your OS family. (No related policy) | High | N | Machine |
| System updates should be installed on your machines | Install missing system security and critical updates to secure your Windows and Linux virtual machines and computers (Related policy: System updates should be installed on your machines) | High | N | Machine |
| Your machines should be restarted to apply system updates | Restart your machines to apply the system updates and secure the machine from vulnerabilities. (No related policy - dependent upon "System updates should be installed on your machines") | Medium | N | Machine |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|---|---|----------|--|--|
| Automation account variables should be encrypted | Enable encryption of Automation account variable assets when storing sensitive data. (Related policy: Encryption should be enabled on Automation account variables) | High | N | Compute resources (automation account) |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|---|----------|---|---------------|
| Disk encryption should be applied on virtual machines | <p>Encrypt your virtual machine disks using Azure Disk Encryption both for Windows and Linux virtual machines. Azure Disk Encryption (ADE) leverages the industry standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide OS and data disk encryption to help protect and safeguard your data and help meet your organizational security and compliance commitments in customer Azure key vault. When your compliance and security requirement requires you to encrypt the data end to end using your encryption keys, including encryption of the ephemeral (locally attached temporary) disk, use Azure disk encryption. Alternatively, by default, Managed Disks are encrypted at rest by default using Azure Storage Service Encryption where the encryption keys are Microsoft-managed keys in Azure. If this meets your compliance and security requirements, you can leverage the default Managed disk encryption to meet your requirements.</p> <p>(Related policy: Disk encryption should be applied on virtual machines)</p> | High | N | Machine |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|---|---|----------|---|---------------|
| Virtual machines should be migrated to new Azure Resource Manager resources | <p>Use Azure Resource Manager for your virtual machines to provide security enhancements such as: stronger access control (RBAC), better auditing, Resource Manager-based deployment and governance, access to managed identities, access to key vault for secrets, Azure AD-based authentication and support for tags and resource groups for easier security management.</p> <p>(Related policy: Virtual machines should be migrated to new Azure Resource Manager resources)</p> | Low | N | Machine |
| Vulnerability assessment solution should be installed on your virtual machines | <p>Install a vulnerability assessment solution on your virtual machines</p> <p>(Related policy: Vulnerability assessment should be installed on virtual machines)</p> | Medium | N | Machine |
| Vulnerabilities should be remediated by a Vulnerability Assessment solution | <p>Virtual machines for which a vulnerability assessment 3rd party solution is deployed are being continuously assessed against application and OS vulnerabilities.</p> <p>Whenever such vulnerabilities are found, these are available for more information as part of the recommendation.</p> <p>(Related policy: Vulnerabilities should be remediated by a Vulnerability Assessment solution)</p> | High | N | Machine |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|---|----------|---|---------------|
| Vulnerabilities in security configuration on your machines should be remediated | Remediate vulnerabilities in security configuration on your machines to protect them from attacks. (Related policy: Vulnerabilities in security configuration on your machines should be remediated) | Low | N | Machine |
| Vulnerabilities in container security configurations should be remediated | Remediate vulnerabilities in security configuration on machines with Docker installed to protect them from attacks. (Related policy: Vulnerabilities in container security configurations should be remediated) | High | N | Machine |
| Endpoint protection health issues should be resolved on your machines | For full Security Center protection, resolve monitoring agent issues on your machines by following the instructions in the Troubleshooting guide. (No related policy - dependent upon "Install endpoint protection solution on your machines") | Medium | N | Machine |
| | | | | |

Virtual machine scale set recommendations

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|----------------|------------------------------|----------|---|---------------|
| | | | | |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|---|---|----------|---|---------------------------|
| Diagnostic logs in Virtual Machine Scale Sets should be enabled | Enable logs and retain them for up to a year. This enables you to recreate activity trails for investigation purposes. This is useful when a security incident occurs, or your network is compromised. (Related policy: Diagnostic logs in Virtual Machine Scale Sets should be enabled) | Low | N | Virtual machine scale set |
| Endpoint protection health failures should be remediated on virtual machine scale sets | Remediate endpoint protection health failures on your virtual machine scale sets to protect them from threats and vulnerabilities. (No related policy - dependent upon "Endpoint protection solution should be installed on virtual machine scale sets") | Low | N | Virtual machine scale set |
| Endpoint protection solution should be installed on virtual machine scale sets | Install an endpoint protection solution on your virtual machine scale sets, to protect them from threats and vulnerabilities. (Related policy: Endpoint protection solution should be installed on virtual machine scale sets) | High | N | Virtual machine scale set |
| System updates on virtual machine scale sets should be installed | Install missing system security and critical updates to secure your Windows and Linux virtual machine scale sets. (Related policy: System updates on virtual machine scale sets should be installed) | High | N | Virtual machine scale set |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|---|----------|---|---------------------------|
| Vulnerabilities in security configuration on your virtual machine scale sets should be remediated | Remediate vulnerabilities in security configuration on your virtual machine scale sets to protect them from attacks. (Related policy: Vulnerabilities in security configuration on your virtual machine scale sets should be remediated) | High | N | Virtual machine scale set |
| | | | | |

Data and storage recommendations

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|---|---|----------|---|-----------------|
| Access to storage accounts with firewall and virtual network configurations should be restricted | Audit unrestricted network access in your storage account firewall settings. Instead, configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific Internet or on-premises clients, you can grant access to traffic from specific Azure virtual networks or to public Internet IP address ranges. (Related policy: Audit unrestricted network access to storage accounts) | Low | N | Storage account |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|--|----------|---|-----------------|
| An Azure Active Directory administrator should be provisioned for SQL servers | <p>Provision an Azure AD administrator for your SQL server to enable Azure AD authentication. Azure AD authentication enables simplified permission management and centralized identity management of database users and other Microsoft services.</p> <p>(Related policy: Audit provisioning of an Azure Active Directory administrator for SQL server)</p> | High | N | SQL |
| Auditing on SQL server should be enabled | <p>Enable auditing for Azure SQL servers. (Azure SQL service only. Doesn't include SQL running on your virtual machines.)</p> <p>(Related policy: Auditing should be enabled on advanced data security settings on SQL Server)</p> | Low | Y | SQL |
| Diagnostic logs in Azure Data Lake Store should be enabled | <p>Enable logs and retain them up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised.</p> <p>(Related policy: Diagnostic logs in Azure Data Lake Store should be enabled)</p> | Low | Y | Data lake store |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|--|----------|---|---------------------|
| Diagnostic logs in Data Lake Analytics should be enabled | Enable logs and retain them up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised. (Related policy: Diagnostic logs in Data Lake Analytics should be enabled) | Low | Y | Data lake analytics |
| Only secure connections to your Redis Cache should be enabled | Enable only connections via SSL to Azure Cache for Redis. Use of secure connections ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking. (Related policy: Only secure connections to your Redis Cache should be enabled) | High | N | Redis |
| Secure transfer to storage accounts should be enabled | Secure transfer is an option that forces your storage account to accept requests only from secure connections (HTTPS). HTTPS ensures authentication between the server and the service and protects data in transit from network layer attacks such as man-in-the-middle, eavesdropping, and session-hijacking. (Related policy: Secure transfer to storage accounts should be enabled) | High | N | Storage account |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|---|----------|---|-----------------|
| Storage accounts should be migrated to new Azure Resource Manager resources | <p>Use new Azure Resource Manager for your storage accounts to provide security enhancements such as: stronger access control (RBAC), better auditing, Resource Manager-based deployment and governance, access to managed identities, access to key vault for secrets, and Azure AD-based authentication and support for tags and resource groups for easier security management.</p> <p>(Related policy: Storage accounts should be migrated to new Azure Resource Manager resources)</p> | Low | N | Storage account |
| Transparent Data Encryption on SQL databases should be enabled | <p>Enable transparent data encryption to protect data-at-rest and meet compliance requirements.</p> <p>(Related policy: Transparent Data Encryption on SQL databases should be enabled)</p> | Low | Y | SQL |
| Vulnerability assessment should be enabled on your SQL servers | <p>Vulnerability assessment can discover, track, and help you remediate potential database vulnerabilities.</p> <p>(Related policy: Vulnerability assessment should be enabled on your SQL servers)</p> | High | Y | SQL |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|---|---|----------|---|---------------|
| Vulnerabilities on your SQL databases should be remediated | SQL Vulnerability Assessment scans your database for security vulnerabilities and exposes any deviations from best practices such as misconfigurations, excessive permissions, and unprotected sensitive data. Resolving the vulnerabilities found can greatly improve your database security stature. (Related policy: Vulnerabilities on your SQL databases should be remediated) | High | N | SQL |
| | | | | |

Identity and access recommendations

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|--|----------|---|---------------|
| MFA should be enabled on accounts with read permissions on your subscription | Enable Multi-Factor Authentication (MFA) for all subscription accounts with read privileges to prevent a breach of accounts or resources. (Related policy: MFA should be enabled on accounts with read permissions on your subscription) | High | N | Subscription |
| MFA should be enabled on accounts with write permissions on your subscription | Enable Multi-Factor Authentication (MFA) for all subscription accounts with write privileges to prevent a breach of accounts or resources. (Related policy: MFA should be enabled on accounts with write permissions on your subscription) | High | N | Subscription |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|---|----------|---|---------------|
| MFA should be enabled on accounts with owner permissions on your subscription | Enable Multi-Factor Authentication (MFA) for all subscription accounts with owner privileges to prevent a breach of accounts or resources. (Related policy: MFA should be enabled on accounts with owner permissions on your subscription) | High | N | Subscription |
| External accounts with read permissions should be removed from your subscription | Remove external accounts with read privileges from your subscription in order to prevent unmonitored access. (Related policy: External accounts with read permissions should be removed from your subscription) | High | N | Subscription |
| External accounts with write permissions should be removed from your subscription | Remove external accounts with write privileges from your subscription in order to prevent unmonitored access. (Related policy: External accounts with write permissions should be removed from your subscription) | High | N | Subscription |
| External accounts with owner permissions should be removed from your subscription | Remove external accounts with owner privileges from your subscription in order to prevent unmonitored access. (Related policy: External accounts with owner permissions should be removed from your subscription) | High | N | Subscription |

| RECOMMENDATION | DESCRIPTION & RELATED POLICY | SEVERITY | QUICK FIX ENABLED? (LEARN MORE) | RESOURCE TYPE |
|--|---|----------|---|---------------|
| Deprecated accounts with owner permissions should be removed from your subscription | Remove deprecated accounts with owner permissions from your subscriptions. (Related policy: Deprecated accounts with owner permissions should be removed from your subscription) | High | N | Subscription |
| Deprecated accounts should be removed from your subscription | Remove deprecated accounts from your subscriptions to enable access to only current users. (Related policy: Deprecated accounts should be removed from your subscription) | High | N | Subscription |
| There should be more than one owner assigned to your subscription | Designate more than one subscription owner in order to have administrator access redundancy. (Related policy: There should be more than one owner assigned to your subscription) | High | N | Subscription |
| A maximum of 3 owners should be designated for your subscription | Designate fewer than three subscription owners in order to reduce the potential for breach by a compromised owner. (Related policy: A maximum of 3 owners should be designated for your subscription) | High | N | Subscription |
| Diagnostic logs in Key Vault should be enabled | Enable logs and retain them up to a year. This enables you to recreate activity trails for investigation purposes when a security incident occurs or your network is compromised. (Related policy: Diagnostic logs in Key Vault should be enabled) | Low | Y | Key Vault |
| | | | | |

Next steps

To learn more about recommendations, see the following:

- [Security recommendations in Azure Security Center](#)
- [Protecting your machines and applications](#)
- [Protecting your network in Azure Security Center](#)

Protect your machines and applications

2/18/2020 • 6 minutes to read • [Edit Online](#)

When Azure Security Center identifies potential security vulnerabilities, it creates recommendations that guide you through the process of configuring the needed controls to harden and protect your resources.

This article explains the **Compute and Apps** page of Security Center's resource security section.

For a full list of the recommendations you might see on this page, see [Compute and apps recommendations](#).

View the security of your compute and apps resources

The screenshot shows the Azure Security Center - Compute & apps dashboard. On the left, there's a sidebar with links like Overview, Getting started, Pricing & settings, Community, Workflow automation, Policy & Compliance, Resource Security Hygiene, and Compute & apps (which is selected). The main area has tabs for Overview, VMs and Servers, VM scale sets, Cloud services, App services, Containers, and Compute resources. The Overview tab is active, displaying a list of security recommendations. Each recommendation includes a title, a 'Quick Fix' button, a change count (+30), the number of failed resources (e.g., 7 of 7 Container hosts), and a severity bar (red for high, yellow for medium, green for low).

| Recommendation | Secure Score Impact | Failed Resources | Severity |
|--|---------------------|--------------------------------|----------|
| Vulnerabilities in container security configurations should be remediated | +30 | 7 of 7 Container hosts | High |
| Remediate vulnerabilities found on your virtual machines (powered by Qualys) | +30 | 9 of 9 virtual machines | Medium |
| Vulnerability assessment solution should be installed on your virtual machines | +30 | 92 of 237 virtual machines | Medium |
| Vulnerabilities in security configuration on your machines should be remediated | +29 | 51 of 239 VMs & servers | Low |
| Enable the built-in vulnerability assessment solution on virtual machines | +23 | 28 of 238 virtual machines | Medium |
| Just-In-Time network access control should be applied on virtual machines | +21 | 122 of 237 virtual machines | Medium |
| Pod Security Policies should be defined on Kubernetes Services (Preview) | +20 | 18 of 18 managed clusters | High |
| Authorized IP ranges should be defined on Kubernetes Services (Preview) | +20 | 18 of 18 managed clusters | High |
| Vulnerabilities in Azure Container Registry images should be remediated (powered ... | +20 | 2 of 3 container registries | Medium |
| Vulnerabilities in security configuration on your virtual machine scale sets should be ... | +20 | 4 of 26 virtual machine sc... | Low |
| Adaptive Application Controls should be enabled on virtual machines | +15 | 52 of 237 virtual machines | Medium |
| The 'ClusterProtectionLevel' property to EncryptAndSign in Service Fabric should be ... | +15 | 1 of 1 service fabric clust... | High |

To view the status of your compute and apps resources, from the left pane in Security Center, select **Compute & apps**. The following tabs are available:

- **Overview:** lists the recommendations for all the compute and apps resources as well as their current security status
- **VMs and Servers:** lists the recommendations for your VMs, computers, and current security state of each
- **VM scale sets:** lists the recommendations for your scale sets,
- **Cloud services:** lists the recommendations for your web and worker roles monitored by Security Center
- **App services:** lists the recommendations for your App service environments and the current security state of each
- **Containers:** lists the recommendations for your containers and security assessment of their configurations
- **Compute resources:** lists the recommendations for your compute resources, such as Service Fabric clusters and Event hubs

What's in each tab?

Each tab has multiple sections, and in each section, you can drill down to see additional details about the item shown.

In each tab, you will also see recommendations for the relevant resources in your monitored environment. The first column lists the recommendation, the second shows the total number of resources affected, and the third shows the severity of the issue.

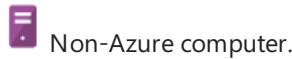
Each recommendation has a set of actions that you can perform after you select it. For example, if you select **Missing system updates**, the number of VMs and computers that are missing patches, and the severity of the missing update appears.

NOTE

The security recommendations are the same as those on the [Recommendations](#) page, but here they're filtered to the specific resource type you've selected. For more information about how to resolve recommendations, see [Implementing security recommendations in Azure Security Center](#).

VMs and Servers

The VMs and computers section gives you an overview of all security recommendations for your VMs and computers. Four types of machines are included:



Non-Azure computer.



Azure Resource Manager VM.



Azure Classic VM.



VMs that are identified only from the workspace that is part of the viewed subscription. This includes VMs from other subscriptions that report to the workspace in this subscription, and VMs that were installed with Operations Manager direct agent, and have no resource ID.

The icon that appears under each recommendation helps you to quickly identify the VM and computer that needs attention, and the type of recommendation. You can also use the filters to search the list by **Resource type** and by **Severity**.

To drill down into the security recommendations for each VM, click on the VM. Here you see the security details for the VM or computer. At the bottom, you can see the recommended action and the severity of each issue.

Vm2
Virtual machine security health

| Resource health | Total recommendations | Recommendations summary | | | | | | | | | |
|---|-----------------------|--|------|---|--|--------|---|--|-----|---|--|
|  Vm2 | 5 | <table border="1"> <tr> <td>High</td> <td>3</td> <td><div style="width: 60%; background-color: #c0392b;"></div></td> </tr> <tr> <td>Medium</td> <td>1</td> <td><div style="width: 20%; background-color: #e6a231;"></div></td> </tr> <tr> <td>Low</td> <td>1</td> <td><div style="width: 20%; background-color: #1f78b4;"></div></td> </tr> </table> | High | 3 | <div style="width: 60%; background-color: #c0392b;"></div> | Medium | 1 | <div style="width: 20%; background-color: #e6a231;"></div> | Low | 1 | <div style="width: 20%; background-color: #1f78b4;"></div> |
| High | 3 | <div style="width: 60%; background-color: #c0392b;"></div> | | | | | | | | | |
| Medium | 1 | <div style="width: 20%; background-color: #e6a231;"></div> | | | | | | | | | |
| Low | 1 | <div style="width: 20%; background-color: #1f78b4;"></div> | | | | | | | | | |

^ Virtual machine information

| | |
|-------------------------|--|
| RESOURCE NAME | Vm2 |
| RESOURCE GROUP | CONTOSO |
| SUBSCRIPTION | Contoso IT - |
| VERSION | Compute |
| WORKSPACE | contosoretail |
| MONITORING STATE | Monitored by Azure Security Center |
| OPERATING SYSTEM | Windows |
| SYSTEM UPDATES | Microsoft (Last scan time - 12/11/2018 12:44 PM) |
| SECURITY CONFIGURATIONS | Microsoft (Last scan time - No recent data) |
| ENDPOINT PROTECTION | Windows Defender |

^ Recommendation list

Recommendations (5) Passed assessments (5) Unavailable assessments (2)

| DESCRIPTION | STATUS |
|--|----------|
| Install system updates on your machines | ● High |
| Enable Adaptive Application Controls | ● High |
| Apply disk encryption on your virtual machines | ● High |
| Install a vulnerability assessment solution on your virtual machines | ▲ Medium |
| Troubleshoot missing scan data on your machines | ● Low |

Virtual machine scale sets

Security Center automatically discovers whether you have scale sets and recommends that you install the Microsoft Monitoring Agent on them.

To install the Microsoft Monitoring Agent:

1. Select the recommendation **Install the monitoring agent on virtual machine scale set**. You get a list of unmonitored scale sets.
2. Select an unhealthy scale set. Follow the instructions to install the monitoring agent using an existing populated workspace or create a new one. Make sure to set the workspace [pricing tier](#) if it's not set.

Install the monitoring agent on virtual machine scale sets (Preview)



Install the Microsoft Monitoring Agent on virtual machine scale sets

Security Center identified several unmonitored virtual machine scale sets. To enhance security and monitor this scale set, it is recommended to install the Microsoft Monitoring Agent.

The agent collects security data and events from the VM scale set instances to help you prevent, detect, and respond to threats.

The data collected by the agent is stored in Log Analytics workspaces. You can set the data collected from Azure VM scale sets to be stored in the same workspaces you defined for VM data collection, or use a different workspace.

Workspace Configuration

WORKSPACE NAME: Workspace-Contoso-1US [edit >](#)

Note: This is the workspace you set for VM data collection.

Your VM scale set installation update policy is set to: Manual. This will deploy the agent on new instances only. To install the agent on existing instances, select the checkbox. [Learn more >](#)

Also install the agent now on existing instances.

Install Agent

To set new scale sets to automatically install the Microsoft Monitoring Agent:

1. Go to Azure Policy and click **Definitions**.
2. Search for the policy **Deploy Log Analytics agent for Windows virtual machine scale sets** and click on it.
3. Click **Assign**.
4. Set the **Scope** and **Log Analytics workspace** and click **Assign**.

If you want to set all existing scale sets to install the Microsoft Monitoring Agent, in Azure Policy, go to **Remediation** and apply the existing policy to existing scale sets.

Cloud services

For cloud services, a recommendation is created when the operating system version is out of date.

The screenshot shows the 'Compute SECURITY HEALTH' dashboard. It has tabs for Overview, Virtual machines, Cloud services (selected), and App services (Preview). Under 'Cloud services', there is a table with columns: NAME, INSTANCES, and OS VERSION. A recommendation is shown for the 'csdemo1' service, indicating that the 'WebRole1' instance is running an outdated OS version (Windows Server 2008 R2) while the 'WorkerRole1' instance is up-to-date (Windows Server 2016).

| NAME | INSTANCES | OS VERSION |
|-------------|-----------|----------------|
| csdemo1 | 2 | ● (Outdated) |
| WebRole1 | 2 | ✓ (Up-to-date) |
| WorkerRole1 | 3 | ✓ (Up-to-date) |

In a scenario where you have a recommendation, follow the steps in the recommendation to update the operating system. When an update is available, you will have an alert (red or orange - depending on the severity of the issue). For a full explanation of this recommendation, click **Update OS version** under the **DESCRIPTION** column.

App services

To view the App Service information, you must be on Security Center's Standard pricing tier and enable App Service in your subscription. For instructions on enabling this feature, see [Protect App Service with Azure Security Center](#).

Under **App services**, you find a list of your App service environments and the health summary based on the assessment Security Center performed.

The screenshot shows the Azure Security Center interface for App services. At the top, there are tabs for Overview, VMs and Computers, Cloud services, App services (Preview), Containers (Preview), VM scale sets (Preview), and Com. Below the tabs are filters for Resource type: All and Severity: All, along with a search bar. A table lists two application environments: HumanResources and NewBilling, each with 4 of 10 recommendations. Each row has a progress bar indicating the status of the recommendations.

| NAME | TOTAL |
|----------------|-------------------------|
| HumanResources | 4 of 10 recommendations |
| NewBilling | 4 of 10 recommendations |

There are three types of application services shown:

- App services environment
- Web application
- Function application

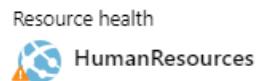
If you select a web application, a summary view opens with three tabs:

- **Recommendations:** based on assessments performed by Security Center that failed.
- **Passed assessments:** list of assessments performed by Security Center that passed.
- **Unavailable assessments:** list of assessments that failed to run due to an error or the recommendation is not relevant for the specific App service

Under **Recommendations** is a list of the recommendations for the selected web application and severity of each recommendation.

HumanResources

Web application security health



Total recommendations

4

Recommendations summary



^ Web application information

RESOURCE NAME [HumanResources](#)RESOURCE GROUP [AppServiceRG](#)SUBSCRIPTION [ASC DEMO](#)

^ Recommendation list

[Recommendations \(4\)](#) [Passed assessments \(4\)](#) [Unavailable assessments \(2\)](#)

| DESCRIPTION | STATUS |
|--|--|
| Web Application should only be accessible over HTTPS (Preview) | ⚠ Medium |
| Configure IP restrictions for Web Application (Preview) | ⚠ Medium |
| Use the latest supported PHP version for Web Application (Preview) | ⓘ Low |
| Use custom domains for Web Application (Preview) | ⓘ Low |

Select a recommendation to see a description of the recommendation and a list of unhealthy resources, healthy resources, and unscanned resources.

- The **Passed assessments** column shows a list of passed assessments. Severity of these assessments is always green.
- Select a passed assessment from the list for a description of the assessment, a list of unhealthy and healthy resources, and a list of unscanned resources. There is a tab for unhealthy resources but that list is always empty since the assessment passed.

Containers

When you open the **Containers** tab, depending on your environment, you might see any of three types of resources:



Container hosts - VMs running docker



Azure Kubernetes Service (AKS) clusters



Azure Container Registry (ACR) registries - Shown only when you're on the standard pricing tier and when you have the Azure Container Registry bundle enabled.

For instructions on how to use the container security features, see [Monitoring the security of your containers](#).

Benefits of the Azure Container Registry bundle are explained [here](#)

Benefits of the Kubernetes Services bundle are explained [here](#)

The screenshot shows the Azure Security Center interface. At the top, there are several navigation icons: Overview, VMs and Servers, VM scale sets, Cloud services, App services, Containers (which is highlighted with a blue dashed border), and Compute resources. Below these are two dropdown filters: 'Resource type: All' and 'Severity: All'. A search bar labeled 'Search resources' is also present. The main content area is a table with columns for 'Name', 'Total', and 'Severity'. The data rows are:

| Name | Total | Severity |
|------------|-------------------------|--|
| asc-demo | 4 of 5 recommendations | <div style="width: 80%; background-color: red;"></div> |
| imagesca | 2 of 2 recommendations | <div style="width: 100%; background-color: red;"></div> |
| contoso | 2 of 14 recommendations | <div style="width: 15%; background-color: green;"></div> |
| k8s-ma | 1 of 1 recommendations | <div style="width: 100%; background-color: red;"></div> |
| ga-k8clter | 1 of 1 recommendations | <div style="width: 100%; background-color: red;"></div> |

To see the recommendations for a specific resource in the list, click that resource.

Visibility into container registries

For example, clicking the asc-demo ACR registry from the list shown in the graphic above leads to this details page:

The screenshot shows the details page for the 'ascdemo' container registry. The top navigation bar includes 'Dashboard', 'Security Center - Compute & apps', and the current resource name 'ascdemo'. The main section is titled 'ascdemo' and 'Container registry security health'. It displays the following information:

- Resource health:** Shows a total of 2 recommendations. The 'Recommendations summary' table shows:

| Severity | Count |
|----------|-------|
| High | 2 |
| Medium | 0 |
| Low | 0 |
- Container registry information:** Includes details such as Resource Name (ascdemo), Resource Group (ASC-Demo), Subscription (ASC DEMO), Login server (ascdemo), Repository count (7), and Image count (9).
- Recommendation list:** Shows a list of recommendations with the following details:

| Recommendation | Status |
|---|---|
| Vulnerabilities in Azure Container Registry images should be remediated (powered by Qualys) | ! High |
| Audit diagnostic setting Custom | ! High |

Visibility into containers hosted on IaaS Linux machines

When you click one of the VMs running docker, you'll see the details page with information related to the containers on the machine, such as Docker version and the number of images running on the host.

ascdockercontainer

Container host security health

| Resource health | Total recommendations | Recommendations summary |
|--|-----------------------|--|
|  ascdockercontainer | 1 | High 1 <div style="width: 100%; background-color: red; height: 10px;"></div> Medium 0 Low 0 |

Container host information

| | |
|--------------------------|--------------------|
| RESOURCE NAME | ascdockercontainer |
| RESOURCE GROUP | Containers |
| SUBSCRIPTION | ASC DEMO |
| DOCKER VERSION | 18.06.1-ce |
| ORCHESTRATOR | None |
| OPERATING SYSTEM | Ubuntu 16.04.5 LTS |
| IMAGE COUNT | 1 |
| RUNNING CONTAINERS COUNT | 1 |

Recommendation list

| Recommendations (1) | Passed assessments (0) | Unavailable assessments (0) |
|--|--|-----------------------------|
|  Remediate vulnerabilities in container security configurations |  High | |

Security recommendations based on CIS benchmark for Docker

Security Center scans your Docker configurations and gives you visibility into misconfigurations by providing a list of all failed rules that were assessed. Security Center provides guidelines to help you resolve these issues quickly and save time. Security Center continuously assesses the Docker configurations and provides you with their latest state.

Logs (classic)
defaultworkspace-contoso

Refresh Saved Searches Analytics New Alert Rule Export PowerBI

Data based on last 1 day

1 bar = 1hr

12:00:00 PM Oct 28, 2018

TYPE (1)

- SecurityBaseline 20

RESOURCE (1)

- ascdockercontainer 20

OSNAME (1)

- Linux 20

```
SecurityBaseline
| where BaselineType == "Docker"
| where Computer == "ascdockercontainer" and AnalyzeResult == "Failed"
| summarize arg_max(TimeGenerated, *) by Cceld
| order by RuleSeverity asc nulls last
```

11 Results [List](#) [Table](#) [Security Baseline Rules](#)

10/28/2018 1:16:59.607 PM | SecurityBaseline

| | |
|----------------------|---|
| ... Cceld | : CIS-CE-2-1 |
| ... TimeGenerated | : 10/28/2018 1:16:59.607 PM |
| ... Resource | : ascdockercontainer |
| ... Computer | : ascdockercontainer |
| ... BaselineType | : Docker |
| ... OSName | : Linux |
| ... RuleSeverity | : Critical |
| ... BaselineRuleType | : Command |
| ... Description | : Ensure network traffic is restricted between containers on the default bridge |
| ... AnalyzeResult | : Failed |

[+] show more

Next steps

To learn more about recommendations that apply to other Azure resource types, see the following articles:

- [Full reference list of Azure Security Center's security recommendations](#)
- [Monitor identity and access in Azure Security Center](#)
- [Protecting your network in Azure Security Center](#)
- [Protecting your Azure SQL service in Azure Security Center](#)

Protect your network resources

2/18/2020 • 6 minutes to read • [Edit Online](#)

Azure Security Center continuously analyzes the security state of your Azure resources for network security best practices. When Security Center identifies potential security vulnerabilities, it creates recommendations that guide you through the process of configuring the needed controls to harden and protect your resources.

This article explains the **Networking** page of the resource security section of Security Center.

For a full list of the recommendations for Networking, see [Networking recommendations](#).

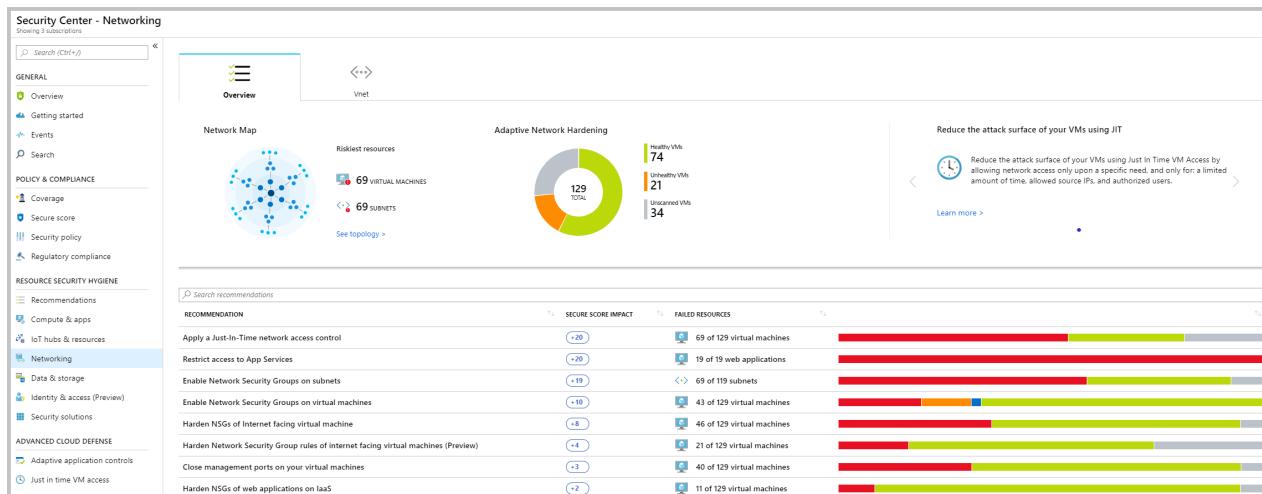
This article addresses recommendations that apply to your Azure resources from a network security perspective. Networking recommendations center around next generation firewalls, Network Security Groups, JIT VM access, overly permissive inbound traffic rules, and more. For a list of networking recommendations and remediation actions, see [Managing security recommendations in Azure Security Center](#).

NOTE

The **Networking** page lets you deep dive into your Azure resource health from a network perspective. The Network map and Adaptive Network Controls are available for the Azure Security Center standard tier only. If you use the free tier, you can click the button to [View legacy networking](#) and receive networking resource recommendations.

The **Networking** page provides an overview of the sections you can deep dive into, to get more information about the health of your network resources:

- Network map (Azure Security Center Standard tier only)
- Adaptive Network Hardening
- Networking security recommendations.
- Legacy **Networking** blade (the previous networking blade)



Network map

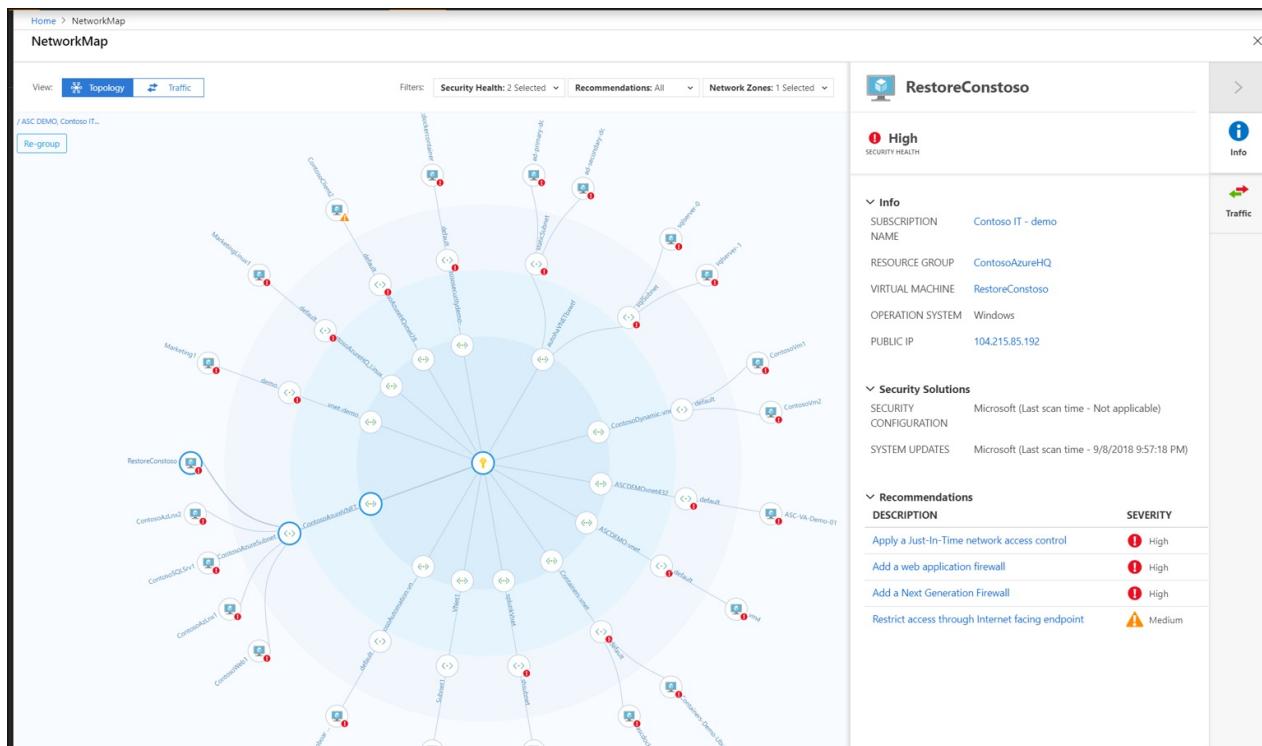
The interactive network map provides a graphical view with security overlays giving you recommendations and insights for hardening your network resources. Using the map you can see the network topology of your Azure workloads, connections between your virtual machines and subnets, and the capability to drill down from the map into specific resources and the recommendations for those resources.

To open the Network map:

1. In Security Center, under Resource Security Hygiene, select **Networking**.
 2. Under **Network map** click **See topology**.

The default view of the topology map displays:

- Subscriptions you selected in Azure. The map supports multiple subscriptions.
 - VMs, subnets, and VNets of the Resource Manager resource type (Classic Azure resources are not supported)
 - Peered VNets
 - Only resources that have [network recommendations](#) with a high or medium severity
 - Internet facing resources
 - The map is optimized for the subscriptions you selected in Azure. If you modify your selection, the map is recalculated and re-optimized based on your new settings.



Understanding the Network map

The Network map can show you your Azure resources in a **Topology** view and a **Traffic** view.

The topology view

In the **Topology** view of the networking map, you can view the following insights about your networking resources:

- In the inner circle, you can see all the Vnets within your selected subscriptions, the next circle is all the subnets, the outer circle is all the virtual machines.
 - The lines connecting the resources in the map let you know which resources are associated with each other, and how your Azure network is structured.
 - Use the severity indicators to quickly get an overview of which resources have open recommendations from Security Center.
 - You can click any of the resources to drill down into them and view the details of that resource and its recommendations directly, and in the context of the Network map.
 - If there are too many resources being displayed on the map, Azure Security Center uses its proprietary algorithm to smart cluster your resources, highlighting the resources that are in the most critical state, and

have the most high severity recommendations.

Because the map is interactive and dynamic, every node is clickable, and the view can change based on the filters:

1. You can modify what you see on the network map by using the filters at the top. You can focus the map based on:

- **Security health:** You can filter the map based on Severity (High, Medium, Low) of your Azure resources.
- **Recommendations:** You can select which resources are displayed based on which recommendations are active on those resources. For example, you can view only resources for which Security Center recommends you enable Network Security Groups.
- **Network zones:** By default, the map displays only Internet facing resources, you can select internal VMs as well.

2. You can click **Reset** in top left corner at any time to return the map to its default state.

To drill down into a resource:

1. When you select a specific resource on the map, the right pane opens and gives you general information about the resource, connected security solutions if there are any, and the recommendations relevant to the resource. It's the same type of behavior for each type of resource you select.
2. When you hover over a node in the map, you can view general information about the resource, including subscription, resource type, and resource group.
3. Use the link to zoom into the tool tip and refocus the map on that specific node.
4. To refocus the map away from a specific node, zoom out.

The Traffic view

The **Traffic** view provides you with a map of all the possible traffic between your resources. This provides you with a visual map of all the rules you configured that define which resources can communicate with whom. This enables you to see the existing configuration of the network security groups as well as quickly identify possible risky configurations within your workloads.

Uncover unwanted connections

The strength of this view is in its ability to show you these allowed connections together with the vulnerabilities that exist, so you can use this cross-section of data to perform the necessary hardening on your resources.

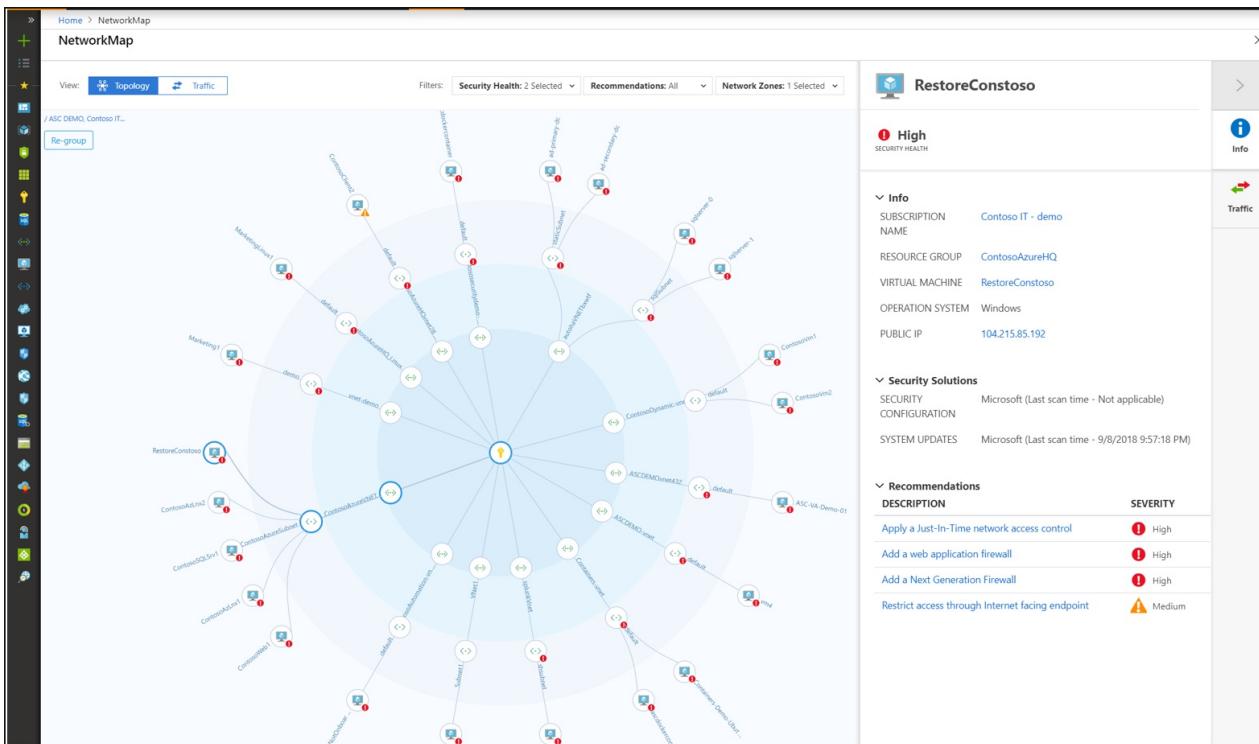
For example, you might detect two machines that you weren't aware could communicate, enabling you to better isolate the workloads and subnets.

Investigate resources

To drill down into a resource:

1. When you select a specific resource on the map, the right pane opens and gives you general information about the resource, connected security solutions if there are any, and the recommendations relevant to the resource. It's the same type of behavior for each type of resource you select.
2. Click **Traffic** to see the list of possible outbound and inbound traffic on the resource - this is a comprehensive list of who can communicate with the resource and who it can communicate with, and through which protocols and ports. For example, when you select a VM, all the VMs it can communicate with are shown, and when you select a subnet, all the subnets which it can communicate with are shown.

This data is based on analysis of the Network Security Groups as well as advanced machine learning algorithms that analyze multiple rules to understand their crossovers and interactions.



Legacy networking

If you don't have Security Center Standard tier, this section explains how to view free Networking recommendations.

To access this information, in the Networking blade, click **View legacy networking**.

The screenshot shows the 'View Legacy Networking' blade. It includes:

- Network Map (Preview)**: Shows a network graph with 47 endpoints and 33 virtual machines.
- Riskiest resources**: Lists 47 endpoints and 33 virtual machines.
- NSG Hardening**: Describes Adaptive Network Hardening and JIT VM Access, with a progress bar showing 4 configured out of 18 total.
- Recommendations** table:

| RECOMMENDATION | RESOURCE TYPE | RESOURCE | STATUS |
|--|------------------|----------|--------|
| Add a Next Generation Firewall | endpoints | 47 of 74 | High |
| Configure Missing Network Security Groups for Subnets | subnets | 14 of 73 | Medium |
| Configure Missing Network Security Groups for virtual machines | virtual machines | 26 of 78 | High |
| Restrict access through Internet facing endpoint | virtual machines | 28 of 78 | Medium |
| Apply a Just-In-Time network access control | virtual machines | 33 of 78 | High |

Internet facing endpoints section

In the **Internet facing endpoints** section, you can see the virtual machines that are currently configured with an Internet facing endpoint and its status.

This table has the endpoint name, the Internet facing IP address, and the current severity status of the network security group and the NGFW recommendations. The table is sorted by severity.

Networking topology section

The **Networking topology** section has a hierarchical view of the resources.

This table is sorted (virtual machines and subnets) by severity.

In this topology view, the first level displays Vnets. The second displays subnets, and the third level displays the virtual machines that belong to those subnets. The right column shows the current status of the network security

group recommendations for those resources.

The third level displays virtual machines, which is similar to what is described previously. You can click any resource to learn more or apply the required security control or configuration.

Next steps

To learn more about recommendations that apply to other Azure resource types, see the following:

- [Protecting your machines and applications in Azure Security Center](#)
- [Protecting your Azure SQL service in Azure Security Center](#)

Protect Azure data and storage services

12/30/2019 • 2 minutes to read • [Edit Online](#)

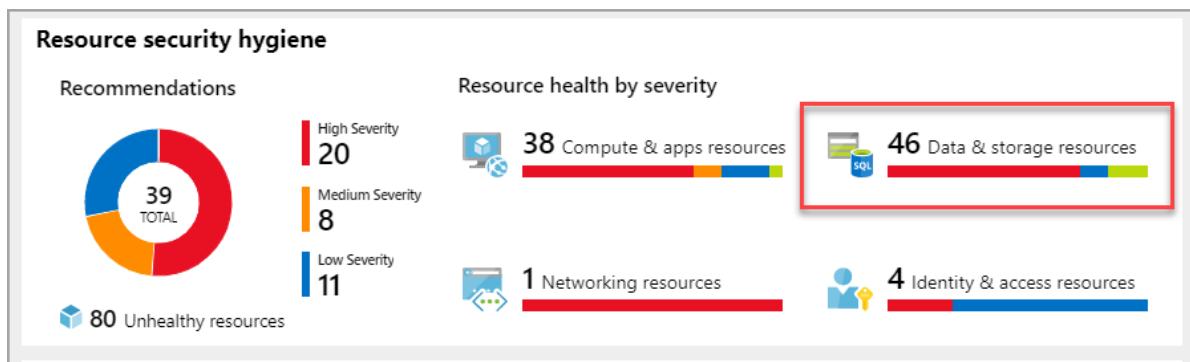
When Azure Security Center identifies potential security vulnerabilities, it creates recommendations that guide you through the process of configuring the needed controls to harden and protect your resources.

This article explains the **Data Security page** of the resource security section of Security Center.

For a full list of the recommendations you might see on this page, see [Data and Storage recommendations](#).

View your data security information

1. In the **Resource security hygiene** section, click **Data and storage resources**.



The **Data security** page opens with recommendations for data resources.

The screenshot shows the 'Data security' page. At the top, there's a navigation bar: Home > Security Center - Overview > Data security. Below it, a 'Data security' section header and a 'SQL Information Protection' tab. A horizontal navigation bar includes 'Overview', 'SQL', 'Storage accounts', 'Redis', 'Data Lake Analytics', and 'Data Lake Store'. Below this is a search bar labeled 'Search recommendations'. A table lists two recommendations:

| RECOMMENDATION | SECURE SCORE IMPACT | FAILED RESOURCES | SEVERITY |
|---|---------------------|---------------------------------|----------|
| Storage accounts should be migrated to new Azure Resource Manager resources | +10 | 2 of 2 classic storage accou... | High |
| Auditing on SQL server should be enabled | +5 | 4 of 4 SQL servers | Medium |

From this page, you can:

- Click the **Overview** tab lists all the data resources recommendations to be remediated.
- Click each tab, and view the recommendations by resource type.

NOTE

For more information about storage encryption, see [Azure Storage encryption for data at rest](#).

Remediate a recommendation on a data resource

1. From any of the resource tabs, click a resource. The information page opens listing the recommendations to be remediated.

sqlserver2ascdemo

SQL server security health

SQL server information



| | |
|----------------|-------------------|
| Resource Name | sqlserver2ascdemo |
| Resource Group | ascdemoRG |
| Subscription | ASC DEMO |
| Version | v12.0 |

Recommendation list

[Recommendations \(5\)](#) [Passed assessments \(2\)](#) [Unavailable assessments \(0\)](#)

| DESCRIPTION | STATUS |
|---|---|
| Vulnerability assessment should be enabled on your SQL servers | ! High |
| Vulnerability assessment should be enabled on your SQL servers | ! High |
| Auditing on SQL server should be enabled | ! High |
| An Azure Active Directory administrator should be provisioned for SQL servers | ! High |
| An Azure Active Directory administrator should be provisioned for SQL servers | ! High |

- Click a recommendation. The Recommendation page opens and displays the **Remediation steps** to implement the recommendation.

Auditing on SQL server should be enabled

^ Description

Enable auditing on your SQL Server to track database activities across all databases on the server and save them in an audit log.

^ General Information

| | |
|---------------------|-----|
| User impact | Low |
| Implementation cost | Low |

^ Threats

- Data exfiltration
- Data spillage
- Malicious insider
- Threat resistance

^ Remediation steps

To enable SQL server auditing:

1. Select the SQL server.
2. Under Auditing, select On.
3. Select Storage details and configure a storage account for the audit log.
4. Click Save.

[Take action](#)

[Go to resource](#)

3. Click **Take action**. The resource settings page appears.

Server settings
sqlserver2ascdemo

Save Discard Feedback

ADVANCED DATA SECURITY

ON **OFF**

 Advanced Data Security costs 15 USD/server/month. It includes Data Discovery & Classification, Vulnerability Assessment and Advanced Threat Protection. We invite you to a trial period for the first 30 days, without charge.

VULNERABILITY ASSESSMENT SETTINGS

Subscription >
ASC DEMO

Storage account  >
Configure required settings

Periodic recurring scans 
ON **OFF**

Send scan reports to 
 

Also send email notification to admins and subscription owners 

ADVANCED THREAT PROTECTION SETTINGS

Send alerts to 

Also send email notification to admins and subscription owners 

Advanced Threat Protection types >
All

 [Enable Auditing for better threats investigation experience](#)

4. Follow the **Remediation steps** and click **Save**.

Next steps

To learn more about recommendations that apply to other Azure resource types, see the following topics:

- [Full reference list of Azure Security Center's security recommendations](#)
- [Protecting your machines and applications in Azure Security Center](#)
- [Protecting your network in Azure Security Center](#)

Monitor identity and access (preview)

12/30/2019 • 3 minutes to read • [Edit Online](#)

When Security Center identifies potential security vulnerabilities, it creates recommendations that guide you through the process of configuring the needed controls to harden and protect your resources.

This article explains the **Identity and Access** page of the resource security section of Azure Security Center.

For a full list of the recommendations you might see on this page, see [Identity and Access recommendations](#).

NOTE

Monitoring identity and access is in preview and available only on the Standard tier of Security Center. See [Pricing](#) to learn more about Security Center's pricing tiers.

Identity should be the control plane for your enterprise, and protecting identities should be your top priority. The security perimeter has evolved from a network perimeter to an identity perimeter. Security becomes less about defending your network and more about defending your data, as well as managing the security of your apps and users. Nowadays, with more data and more apps moving to the cloud, identity becomes the new perimeter.

By monitoring identity activities, you can take proactive actions before an incident takes place or reactive actions to stop an attack attempt. The Identity & Access dashboard provides you with recommendations such as:

- Enable MFA for privileged accounts on your subscription
- Remove external accounts with write permissions from your subscription
- Remove privileged external accounts from your subscription

NOTE

If your subscription has more than 600 accounts, Security Center is unable to run the Identity recommendations against your subscription. Recommendations that are not run are listed under "unavailable assessments" below. Security Center is unable to run the Identity recommendations against a Cloud Solution Provider (CSP) partner's admin agents.

Monitor identity and access

Open the list of identified Identity and Access issues by selecting **Identity & access** from the Security Center sidebar (under **Resources**), or from the overview page.

Under **Identity & Access**, there are two tabs:

- **Overview:** recommendations identified by Security Center.
- **Subscriptions:** list of your subscriptions and current security state of each.

| RECOMMENDATION | TOTAL |
|---|----------------------|
| Remove privileged external accounts from your subscription (Preview) | 1 of 1 subscriptions |
| Designate up to 3 owners on your subscription (Preview) | 1 of 1 subscriptions |
| Remove external accounts with read permissions from your subscription (Preview) | 1 of 1 subscriptions |

Overview section

Under **Overview**, there is a list of recommendations. The first column lists the recommendation. The second column shows the total number of subscriptions that are affected by that recommendation. The third column shows the severity of the issue.

1. Select a recommendation. The recommendations window opens and displays:

- Description of the recommendation
- List of unhealthy and healthy subscriptions
- List of resources that are unscanned due to a failed assessment or the resource is under a subscription running on the Free tier and is not assessed

| UNHEALTHY RESOURCES | HEALTHY RESOURCES |
|---------------------|-------------------|
| 1 🚨 | 0 🌟 |

UNHEALTHY RESOURCES: Contoso IT - demo

LEARN MORE: Learn more about recommendations

2. Select a subscription in the list for additional detail.

Subscriptions section

Under **Subscriptions**, there is a list of subscriptions. The first column lists the subscriptions. The second column shows the total number of recommendations for each subscription. The third column shows the severities of the issues.

| NAME | TOTAL |
|-------------------|-------------------------|
| Contoso IT - demo | 3 of 10 recommendations |

1. Select a subscription. A summary view opens with three tabs:

- **Recommendations:** based on assessments performed by Security Center that failed.
- **Passed assessments:** list of assessments performed by Security Center that passed.
- **Unavailable assessments:** list of assessments that failed to run due to an error or because the subscription has more than 600 accounts.

Under **Recommendations** is a list of the recommendations for the selected subscription and severity of each recommendation.

Contoso IT - demo (Preview)

Subscription security health

Recommendations

8 ! 2 ✓

Recommendations Passed assessments Unavailable assessments

| DESCRIPTION | STATUS |
|--|----------|
| Remove privileged external accounts from your subscription (Preview) | ! High |
| Enable MFA for privileged accounts on your subscription (Preview) | ! High |
| Remove external accounts with write permissions from your subscription (Preview) | ⚠ Medium |
| Enable MFA for accounts with write permissions on your subscription (Preview) | ⚠ Medium |
| Designate up to 3 owners on your subscription (Preview) | ⚠ Medium |

2. Select a recommendation for a description of the recommendation, a list of unhealthy and healthy subscriptions, and a list of unscanned resources.

Designate up to 3 owners on your subscription (Preview)

Description
It is recommended to designate up to 3 subscription owners in order to reduce the potential for breach by a compromised owner.
Remediation steps
To remove accounts with owner permissions from your subscription, we recommend the following steps:
1. Go to the subscription's Access control (IAM) page
2. Select accounts with owner permissions that you would like to remove
3. Change their assigned role or remove them from your subscription

UNHEALTHY RESOURCES HEALTHY RESOURCES

1 🚨 0 🌟

Unhealthy resources Healthy resources Unscanned resources

Search subscriptions

NAME SUBSCRIPTION

Contoso IT - demo e4272367-5645-4c4e-9c67-3b74b59a6982

Under **Passed assessments** is a list of passed assessments. Severity of these assessments is always green.

Contoso IT - demo (Preview)

Subscription security health

Recommendations

8 ! 2 ✓

Recommendations Passed assessments Unavailable assessments

| DESCRIPTION | STATUS |
|--|-----------|
| Remove privileged deprecated accounts from your subscription (Preview) | ✓ Healthy |
| Designate more than one owner on your subscription (Preview) | ✓ Healthy |

3. Select a passed assessment from the list for a description of the assessment and a list of healthy subscriptions. There is a tab for unhealthy subscriptions that lists all the subscriptions that failed.

Remove privileged deprecated accounts from your subscription (Preview) X

Description
Privileged deprecated accounts should be removed from your subscription. Security Center found deprecated accounts with access to your subscription. It is recommended that you renew your keys.

Remediation steps
To remove deprecated accounts from your subscription, we recommend the following steps:
1. Go to the subscription's Access control (IAM) page
2. Select external accounts
3. Select remove

| UNHEALTHY RESOURCES | HEALTHY RESOURCES |
|---------------------|-------------------|
| 0 | 1 |

[Unhealthy resources](#) [Healthy resources](#) [Unscanned resources](#)

Search subscriptions

| NAME | SUBSCRIPTION |
|-------------------|--------------------------------------|
| Contoso IT - demo | e4272367-5645-4c4e-9c67-3b74b59a6982 |

LEARN MORE [Learn more about recommendations](#)

NOTE

If you created a Conditional Access policy that necessitates MFA but has exclusions set, the Security Center MFA recommendation assessment considers the policy non-compliant, because it enables some users to sign in to Azure without MFA.

Next steps

To learn more about recommendations that apply to other Azure resource types, see the following articles:

- [Protecting your machines and applications in Azure Security Center](#)
- [Protecting your network in Azure Security Center](#)
- [Protecting your Azure SQL service and data in Azure Security Center](#)

Secure your management ports with just-in-time access

2/25/2020 • 11 minutes to read • [Edit Online](#)

If you're on Security Center's standard pricing tier (see [pricing](#)), you can lock down inbound traffic to your Azure VMs with just-in-time (JIT) virtual machine (VM) access. This reduces exposure to attacks while providing easy access to connect to VMs when needed.

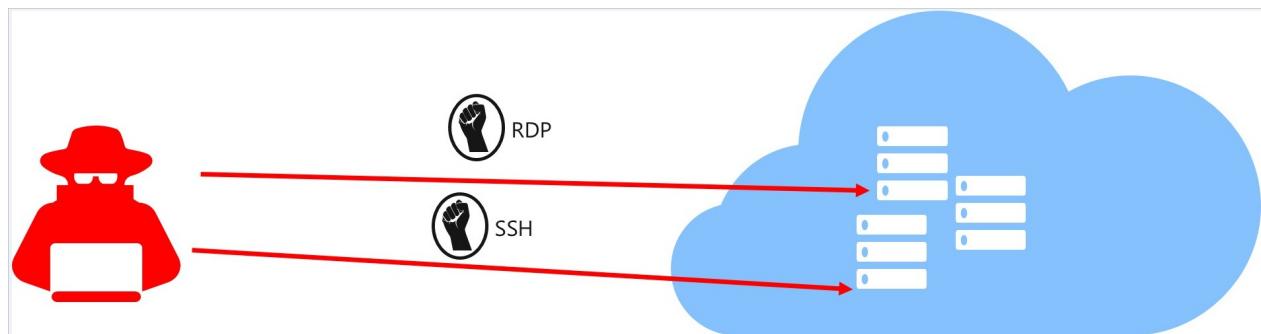
NOTE

Security Center just-in-time VM access currently supports only VMs deployed through Azure Resource Manager. To learn more about the classic and Resource Manager deployment models see [Azure Resource Manager vs. classic deployment](#).

Attack scenario

Brute force attacks commonly target management ports as a means to gain access to a VM. If successful, an attacker can take control over the VM and establish a foothold into your environment.

One way to reduce exposure to a brute force attack is to limit the amount of time that a port is open. Management ports don't need to be open at all times. They only need to be open while you're connected to the VM, for example to perform management or maintenance tasks. When just-in-time is enabled, Security Center uses [network security group](#) (NSG) and Azure Firewall rules, which restrict access to management ports so they cannot be targeted by attackers.



How does JIT access work?

When just-in-time is enabled, Security Center locks down inbound traffic to your Azure VMs by creating an NSG rule. You select the ports on the VM to which inbound traffic will be locked down. These ports are controlled by the just-in-time solution.

When a user requests access to a VM, Security Center checks that the user has [Role-Based Access Control \(RBAC\)](#) permissions for that VM. If the request is approved, Security Center automatically configures the Network Security Groups (NSGs) and Azure Firewall to allow inbound traffic to the selected ports and requested source IP addresses or ranges, for the amount of time that was specified. After the time has expired, Security Center restores the NSGs to their previous states. Those connections that are already established are not being interrupted, however.

NOTE

If a JIT access request is approved for a VM behind an Azure Firewall, then Security Center automatically changes both the NSG and firewall policy rules. For the amount of time that was specified, the rules allow inbound traffic to the selected ports and requested source IP addresses or ranges. After the time is over, Security Center restores the firewall and NSG rules to their previous states.

Permissions needed to configure and use JIT

| TO ENABLE A USER TO: | PERMISSIONS TO SET |
|---|---|
| Configure or edit a JIT policy for a VM | <p><i>Assign these actions to the role:</i></p> <ul style="list-style-type: none"> • On the scope of a subscription or resource group that is associated with the VM: <code>Microsoft.Security/locations/jitNetworkAccessPolicies/write</code> • On the scope of a subscription or resource group of VM: <code>Microsoft.Compute/virtualMachines/write</code> |
| Request JIT access to a VM | <p><i>Assign these actions to the user:</i></p> <ul style="list-style-type: none"> • On the scope of a subscription or resource group that is associated with the VM: <code>Microsoft.Security/locations/jitNetworkAccessPolicies/initiate/*/read</code> • On the scope of a subscription or resource group that is associated with the VM: <code>Microsoft.Security/locations/jitNetworkAccessPolicies/*/read</code> • On the scope of a subscription or resource group or VM: <code>Microsoft.Compute/virtualMachines/read</code> • On the scope of a subscription or resource group or VM: <code>Microsoft.Network/networkInterfaces/*/read</code> |

Configure JIT on a VM

There are three ways to configure a JIT policy on a VM:

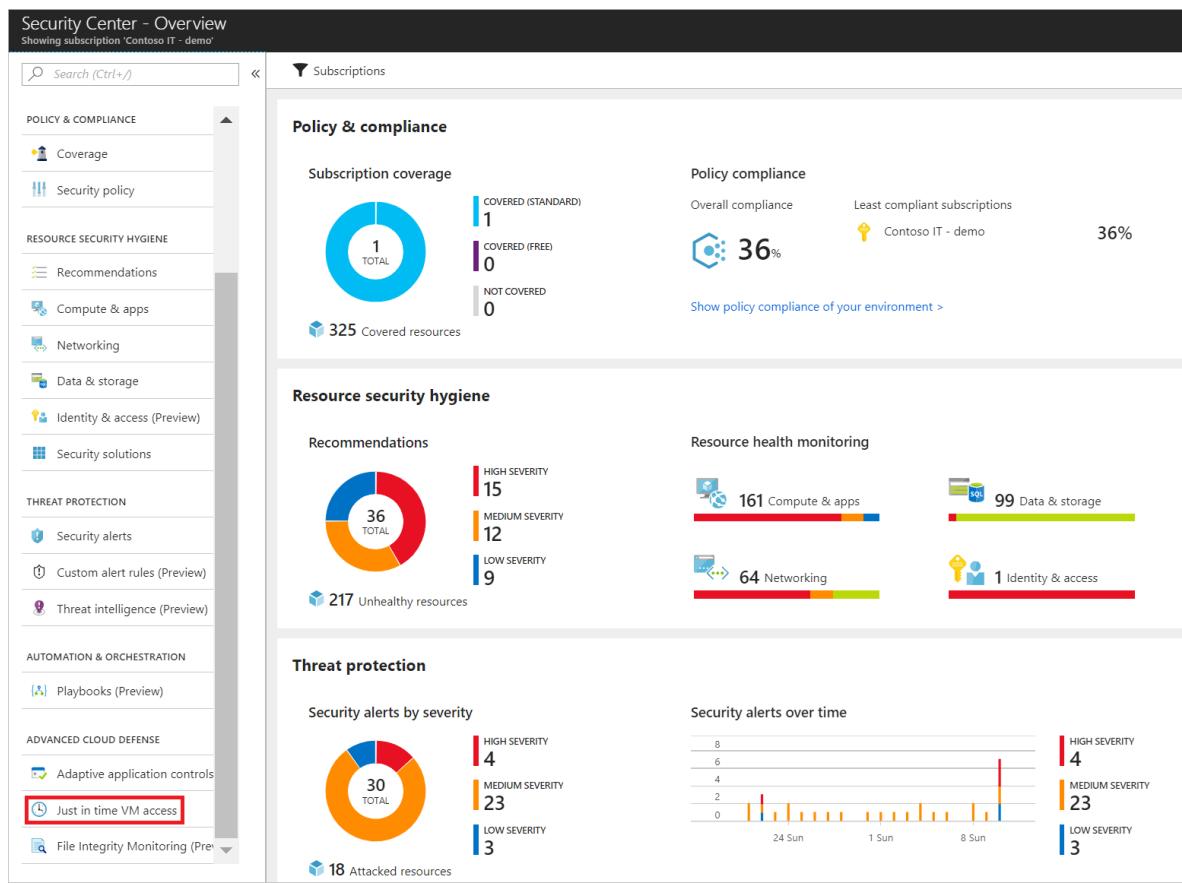
- [Configure JIT access in Azure Security Center](#)
- [Configure JIT access in an Azure VM page](#)
- [Configure a JIT policy on a VM programmatically](#)

Configure JIT in Azure Security Center

From Security Center, you can configure a JIT policy and request access to a VM using a JIT policy

Configure JIT access on a VM in Security Center

1. Open the **Security Center** dashboard.
2. In the left pane, select **Just-in-time VM access**.



The **Just-in-time VM access** window opens and shows information on the state of your VMs:

- **Configured** - VMs that have been configured to support just-in-time VM access. The data presented is for the last week and includes for each VM the number of approved requests, last access date and time, and last user.
- **Recommended** - VMs that can support just-in-time VM access but haven't been configured to. We recommend that you enable just-in-time VM access control for these VMs.
- **No recommendation** - Reasons that can cause a VM not to be recommended are:
 - Missing NSG - The just-in-time solution requires an NSG to be in place.
 - Classic VM - Security Center just-in-time VM access currently supports only VMs deployed through Azure Resource Manager. A classic deployment is not supported by the just-in-time solution.
 - Other - A VM is in this category if the just-in-time solution is turned off in the security policy of the subscription or the resource group, or if the VM is missing a public IP and doesn't have an NSG in place.

3. Select the **Recommended** tab.

4. Under **VIRTUAL MACHINE**, click the VMs that you want to enable. This puts a checkmark next to a VM.

Virtual machines

Configured Recommended No recommendation

VMs for which we recommend you to apply the just in time VM access control.

61 VMs

Enable JIT on 2 VMs

Search to filter items...

| VIRTUAL MACHINE | STATE | SEVERITY |
|---|-------|----------|
| AA-Contoso-01 | Open | ! High |
| <input checked="" type="checkbox"/> App01 | Open | ! High |
| App03 | Open | ! High |
| App04 | Open | ! High |
| App05 | Open | ! High |
| App06 | Open | ! High |
| <input checked="" type="checkbox"/> App07 | Open | ! High |
| App08 | Open | ! High |
| App09 | Open | ! High |

5. Click **Enable JIT on VMs**. A pane opens displaying the default ports recommended by Azure Security Center:

- 22 - SSH
- 3389 - RDP
- 5985 - WinRM
- 5986 - WinRM

6. Optionally, you can add custom ports to the list:

- a. Click **Add**. The **Add port configuration** window opens.
- b. For each port you choose to configure, both default and custom, you can customize the following settings:
 - **Protocol type**- The protocol that is allowed on this port when a request is approved.
 - **Allowed source IP addresses**- The IP ranges that are allowed on this port when a request is approved.
 - **Maximum request time**- The maximum time window during which a specific port can be opened.
- c. Click **OK**.

7. Click **Save**.

NOTE

When JIT VM Access is enabled for a VM, Azure Security Center creates "deny all inbound traffic" rules for the selected ports in the network security groups associated and Azure Firewall with it. If other rules had been created for the selected ports, then the existing rules take priority over the new "deny all inbound traffic" rules. If there are no existing rules on the selected ports, then the new "deny all inbound traffic" rules take top priority in the Network Security Groups and Azure Firewall.

Request JIT access via Security Center

To request access to a VM via Security Center:

1. Under **Just-in-time VM access**, select the **Configured** tab.

2. Under **Virtual Machine**, click the VMs that you want to request access for. This puts a checkmark next to the VM.

- The icon in the **Connection Details** column indicates whether JIT is enabled on the NSG or FW. If it's enabled on both, only the Firewall icon appears.
- The **Connection Details** column provides the information required to connect the VM, and its open ports.

| Virtual machines | | | | | |
|-------------------------------------|------------|------------------|-----------------------|------------------|-----|
| | Configured | Recommended | No recommendation | | |
| VIRTUAL MACHINE | APPROVED | LAST ACCESS | CONNECTION DETAILS | LAST USER | |
| af-vm | 1 Requests | 5/7/19, 11:05 AM | 13.64.24.215:13389 | user@contoso.com | ... |
| srvworkload2 | 1 Requests | 5/7/19, 11:30 AM | 20.185.107.87:10022 | user@contoso.com | ... |
| sc2019 | 2 Requests | 5/7/19, 11:39 AM | 3 Ports | user@contoso.com | ... |
| bengr-jit-mul-1 | 1 Requests | Active now | Ports: 5986, 22, 3389 | user@contoso.com | ... |
| LBWeb0 | 0 Requests | N/A | - | N/A | ... |
| LBWeb1 | 0 Requests | N/A | - | N/A | ... |
| multiport1 | 0 Requests | N/A | - | N/A | ... |
| <input type="checkbox"/> multiport0 | 0 Requests | N/A | - | N/A | ... |
| WebApp1 | 0 Requests | N/A | - | N/A | ... |
| WinVM | 0 Requests | N/A | - | N/A | ... |
| vm2 | 0 Requests | N/A | - | N/A | ... |
| BarWaffT2Jun3 | 0 Requests | N/A | - | N/A | ... |
| bengr-jit-mul-2 | 0 Requests | N/A | - | N/A | ... |
| Chkpln3 | 0 Requests | N/A | - | N/A | ... |

3. Click **Request access**. The **Request access** window opens.

Request access

Please select the ports that you would like to open per virtual machine.

| PORT | TOGGLE | ALLOWED SOURCE IP | IP RANGE | TIMERANGE |
|--------------|--------|-------------------|----------|---------------------------------|
| ▼ vm1 | | | | |
| 22 | On Off | My IP IP Range | No range | <input type="range" value="3"/> |
| 3389 | On Off | My IP IP Range | No range | <input type="range" value="3"/> |
| 5985 | On Off | My IP IP Range | No range | <input type="range" value="3"/> |
| 5986 | On Off | My IP IP Range | No range | <input type="range" value="3"/> |
| ▼ vm2 | | | | |
| 22 | On Off | My IP IP Range | No range | <input type="range" value="3"/> |
| 3389 | On Off | My IP IP Range | No range | <input type="range" value="2"/> |
| 5985 | On Off | My IP IP Range | No range | <input type="range" value="3"/> |
| 5986 | On Off | My IP IP Range | No range | <input type="range" value="3"/> |

Open ports

4. Under **Request access**, for each VM, configure the ports that you want to open and the source IP addresses that the port is opened on and the time window for which the port will be open. It will only be possible to request access to the ports that are configured in the just-in-time policy. Each port has a maximum allowed time derived from the just-in-time policy.

5. Click **Open ports**.

NOTE

If a user who is requesting access is behind a proxy, the option **My IP** may not work. You may need to define the full IP address range of the organization.

Edit a JIT access policy via Security Center

You can change a VM's existing just-in-time policy by adding and configuring a new port to protect for that VM, or by changing any other setting related to an already protected port.

To edit an existing just-in-time policy of a VM:

1. In the **Configured** tab, under **VMs**, select a VM to which to add a port by clicking on the three dots within the row for that VM.
2. Select **Edit**.
3. Under **JIT VM access configuration**, you can either edit the existing settings of an already protected port or add new custom port.

The screenshot shows the JIT VM access configuration interface in the Azure Security Center. On the left, the 'Just in time VM access' page displays a summary and a list of virtual machines. The 'Configured' tab is selected. A red box highlights the 'Configured' tab. On the right, the 'JIT VM access configuration' page for 'vm1' is open, showing two ports (22 and 3389) with their respective settings. A red box highlights the 'Edit' button in the context menu for the 'vm1' row in the list.

Audit JIT access activity in Security Center

You can gain insights into VM activities using log search. To view logs:

1. Under **Just-in-time VM access**, select the **Configured** tab.
2. Under **VMs**, select a VM to view information about by clicking on the three dots within the row for that VM and select **Activity Log** from the menu. The **Activity log** opens.

Just in time VM access

Last week

What is just in time VM access?

Just in time VM access enables you to lock down your VMs in the network level by blocking inbound traffic to specific ports. It enables you to control the access and reduce the attack surface to your VMs, by allowing access only upon a specific need.

How does it work?

Upon a user request, based on Azure RBAC, Security Center will decide whether to grant access. If a request is approved, Security Center automatically configures the NSGs to allow inbound traffic to these ports, for only 3 hours, after which it restores the NSGs to their previous states.

[For more information go to the documentation >](#)

Virtual machines

| Configured | Recommended | No recommendation | | | | | | | | | | | | | | | | | | | | | | | | |
|---|-------------|-------------------|-----------------|----------|-------------|-----------|-----|------------|-----------------|------------|-----|------------|-----------------|--------------|-----|------------|-----|------|-------|------------|-----|--------|-------|------------|-----|-----|
| 5 VMs | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <p>VMs for which the just in time VM access control is already in place. Presented data is for the last week.</p> <table border="1"> <thead> <tr> <th>VIRTUAL MACHINE</th> <th>APPROVED</th> <th>LAST ACCESS</th> <th>LAST USER</th> </tr> </thead> <tbody> <tr> <td>vm1</td> <td>6 Requests</td> <td>17/07/17, 15:27</td> <td>Properties</td> </tr> <tr> <td>vm2</td> <td>4 Requests</td> <td>13/07/17, 17:37</td> <td>Activity Log</td> </tr> <tr> <td>vm3</td> <td>0 Requests</td> <td>N/A</td> <td>Edit</td> </tr> <tr> <td>vm2WL</td> <td>0 Requests</td> <td>N/A</td> <td>Remove</td> </tr> <tr> <td>vm3WL</td> <td>0 Requests</td> <td>N/A</td> <td>...</td> </tr> </tbody> </table> | | | VIRTUAL MACHINE | APPROVED | LAST ACCESS | LAST USER | vm1 | 6 Requests | 17/07/17, 15:27 | Properties | vm2 | 4 Requests | 13/07/17, 17:37 | Activity Log | vm3 | 0 Requests | N/A | Edit | vm2WL | 0 Requests | N/A | Remove | vm3WL | 0 Requests | N/A | ... |
| VIRTUAL MACHINE | APPROVED | LAST ACCESS | LAST USER | | | | | | | | | | | | | | | | | | | | | | | |
| vm1 | 6 Requests | 17/07/17, 15:27 | Properties | | | | | | | | | | | | | | | | | | | | | | | |
| vm2 | 4 Requests | 13/07/17, 17:37 | Activity Log | | | | | | | | | | | | | | | | | | | | | | | |
| vm3 | 0 Requests | N/A | Edit | | | | | | | | | | | | | | | | | | | | | | | |
| vm2WL | 0 Requests | N/A | Remove | | | | | | | | | | | | | | | | | | | | | | | |
| vm3WL | 0 Requests | N/A | ... | | | | | | | | | | | | | | | | | | | | | | | |

Activity log provides a filtered view of previous operations for that VM along with time, date, and subscription.

You can download the log information by selecting [Click here to download all the items as CSV](#).

Modify the filters and click **Apply** to create a search and log.

Configure JIT access from an Azure VM's page

For your convenience, you can connect to a VM using JIT directly from within the VM's page in Security Center.

Configure JIT access on a VM via the Azure VM page

To make it easy to roll out just-in-time access across your VMs, you can set a VM to allow only just-in-time access directly from within the VM.

- From the [Azure portal](#), search for and select **Virtual machines**.
- Select the virtual machine you want to limit to just-in-time access.
- In the menu, select **Configuration**.
- Under **Just-in-time access**, select **Enable just-in-time**.

This enables just-in-time access for the VM using the following settings:

- Windows servers:
 - RDP port 3389
 - Three hours of maximum allowed access
 - Allowed source IP addresses is set to Any
- Linux servers:
 - SSH port 22
 - Three hours of maximum allowed access
 - Allowed source IP addresses is set to Any

If a VM already has just-in-time enabled, when you go to its configuration page you will be able to see that just-in-time is

enabled and you can use the link to open the policy in Azure Security Center to view and change the settings.

The screenshot shows the Azure portal interface for managing virtual machines. On the left, a list of virtual machines is displayed, with 'vm-contoso-us' selected and highlighted by a red box. The main pane shows the 'vm-contoso-us - Configuration' page. A red box highlights the 'Just-in-time access' section, which contains a message: 'To improve security, enable a just-in-time access policy.' Below this is a blue button labeled 'Enable just-in-time policy'. Another red box highlights the 'Configuration' section under 'Settings', which includes options like Networking, Disks, Size, Security, Extensions, Continuous delivery (Preview), Availability set, Configuration (selected), and Identity (Preview). At the bottom right of the configuration pane, there are 'Save' and 'Discard' buttons, along with 'Azure hybrid benefit' and 'Use existing Windows license' options with 'No' and 'Yes' buttons.

Request JIT access to a VM via an Azure VM's page

In the Azure portal, when you try to connect to a VM, Azure checks to see if you have a just-in-time access policy configured on that VM.

- If you have a JIT policy configured on the VM, you can click **Request access** to grant access in accordance with the JIT policy set for the VM.

Connect to virtual machine

X

vm1



This VM has a just-in-time access policy. Select "Request access" before connecting.

RDP

SSH

You need to request access to connect to your virtual machine. Select an IP address, optionally change the port number, and select "Request access". [Learn more](#)

o

* IP address

Public IP address (52.161.18.9)



* Port number

3389

Request access

[Download RDP file anyway](#)

Having trouble connecting to this VM?

- [Diagnose and solve problems](#)
- [Troubleshoot connection](#)
- [Serial console](#)

Access is requested with the following default parameters:

- o **source IP:** 'Any' (*) (cannot be changed)
- o **time range:** Three hours (cannot be changed)
- o **port number** RDP port 3389 for Windows / port 22 for Linux (can be changed)

NOTE

After a request is approved for a VM protected by Azure Firewall, Security Center provides the user with the proper connection details (the port mapping from the DNAT table) to use to connect to the VM.

- If you do not have JIT configured on a VM, you will be prompted to configure a JIT policy on it.

Connect to virtual machine

ContosoAppSrv2

To improve security, enable just-in-time access on this VM.

RDP **SSH**

To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.

* IP address
Public IP address (40.124.37.238)

* Port number
3389

Download RDP File

 Inbound traffic to the Public IP address may be blocked. You can update inbound port rules in the **VM Networking** page.

 You can troubleshoot VM connection issues by opening the **Diagnose and solve problems** page.

Configure a JIT policy on a VM programmatically

You can set up and use just-in-time via REST APIs and via PowerShell.

JIT VM access via REST APIs

The just-in-time VM access feature can be used via the Azure Security Center API. You can get information about configured VMs, add new ones, request access to a VM, and more, via this API. See [Jit Network Access Policies](#), to learn more about the just-in-time REST API.

JIT VM access via PowerShell

To use the just-in-time VM access solution via PowerShell, use the official Azure Security Center PowerShell cmdlets, and specifically `Set-AzJitNetworkAccessPolicy`.

The following example sets a just-in-time VM access policy on a specific VM, and sets the following:

1. Close ports 22 and 3389.
2. Set a maximum time window of 3 hours for each so they can be opened per approved request.
3. Allows the user who is requesting access to control the source IP addresses and allows the user to establish a successful session upon an approved just-in-time access request.

Run the following in PowerShell to accomplish this:

1. Assign a variable that holds the just-in-time VM access policy for a VM:

```
$JitPolicy = (@{  
    id="/subscriptions/SUBSCRIPTIONID/resourceGroups/RESOURCEGROUP/providers/Microsoft.Compute/virtualMachines/VMNAME"  
    E"  
    ports=@{  
        @{
            number=22;  
            protocol="*";  
            allowedSourceAddressPrefix=@("*");  
            maxRequestAccessDuration="PT3H"},  
        @{
            number=3389;  
            protocol="*";  
            allowedSourceAddressPrefix=@("*");  
            maxRequestAccessDuration="PT3H"}})}
```

2. Insert the VM just-in-time VM access policy to an array:

```
$JitPolicyArr=@($JitPolicy)
```

3. Configure the just-in-time VM access policy on the selected VM:

```
Set-AzJitNetworkAccessPolicy -Kind "Basic" -Location "LOCATION" -Name "default" -ResourceGroupName "RESOURCEGROUP" -VirtualMachine $JitPolicyArr
```

Request access to a VM via PowerShell

In the following example, you can see a just-in-time VM access request to a specific VM in which port 22 is requested to be opened for a specific IP address and for a specific amount of time:

Run the following in PowerShell:

1. Configure the VM request access properties

```
$JitPolicyVm1 = (@{  
    id="/SUBSCRIPTIONID/resourceGroups/RESOURCEGROUP/providers/Microsoft.Compute/virtualMachines/VMNAME"  
    ports=@{  
        number=22;  
        endTimeUtc="2018-09-17T17:00:00.3658798Z";  
        allowedSourceAddressPrefix=@("IPV4ADDRESS"))})
```

2. Insert the VM access request parameters in an array:

```
$JitPolicyArr=@($JitPolicyVm1)
```

3. Send the request access (use the resource ID you got in step 1)

```
Start-AzJitNetworkAccessPolicy -ResourceId  
"/subscriptions/SUBSCRIPTIONID/resourceGroups/RESOURCEGROUP/providers/Microsoft.Security/locations/LOCATION/jitNe  
tworkAccessPolicies/default" -VirtualMachine $JitPolicyArr
```

For more information, see the [PowerShell cmdlet documentation](#).

Automatic cleanup of redundant JIT rules

Whenever you update a JIT policy, a cleanup tool automatically runs to check the validity of your entire ruleset. The tool looks for mismatches between rules in your policy and rules in the NSG. If the cleanup tool finds a mismatch, it determines the cause and, when it's safe to do so, removes built-in rules that aren't needed any more. The cleaner never deletes rules that you've created.

Examples scenarios when the cleaner might remove a built-in rule:

- When two rules with identical definitions exist and one has a higher priority than the other (meaning, the lower priority rule will never be used)
- When a rule description includes the name of a VM which doesn't match the destination IP in the rule

Next steps

In this article, you learned how just-in-time VM access in Security Center helps you control access to your Azure virtual machines.

To learn more about Security Center, see the following:

- [Setting security policies](#) — Learn how to configure security policies for your Azure subscriptions and resource groups.
- [Managing security recommendations](#) — Learn how recommendations help you protect your Azure resources.
- [Security health monitoring](#) — Learn how to monitor the health of your Azure resources.

Adaptive application controls

2/25/2020 • 8 minutes to read • [Edit Online](#)

Learn how to configure application control in Azure Security Center using this walkthrough.

What are adaptive application controls in Security Center?

Adaptive application control is an intelligent, automated, end-to-end solution from Azure Security Center which helps you control which applications can run on your Azure and non-Azure machines (Windows and Linux). Among other benefits, this helps harden your machines against malware. Security Center uses machine learning to analyze the applications running on your machines and creates an allow list from this intelligence. This capability greatly simplifies the process of configuring and maintaining application allow list policies, enabling you to:

- Block or alert on attempts to run malicious applications, including those that might otherwise be missed by antimalware solutions.
- Comply with your organization's security policy that dictates the use of only licensed software.
- Avoid unwanted software to be used in your environment.
- Avoid old and unsupported apps to run.
- Prevent specific software tools that are not allowed in your organization.
- Enable IT to control the access to sensitive data through app usage.

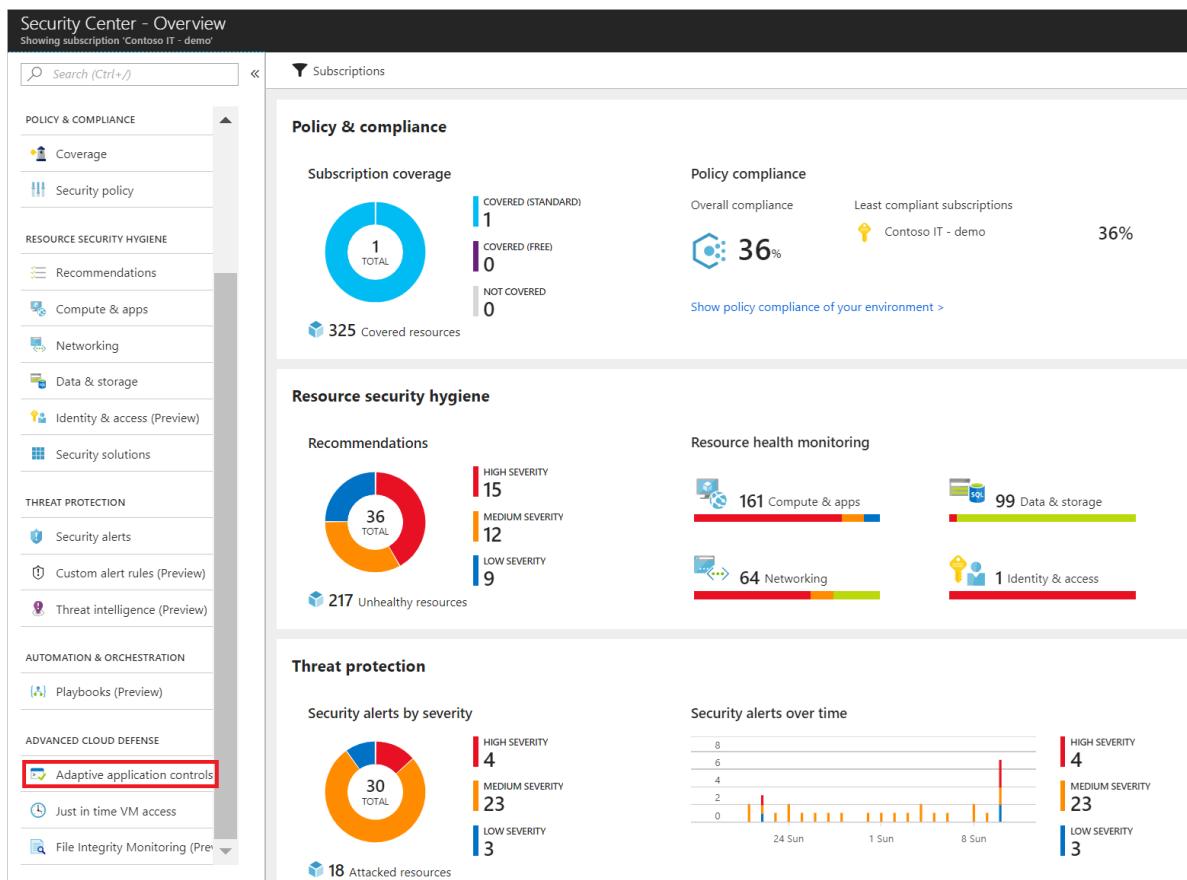
NOTE

For Non-Azure and Linux machines, adaptive application controls are supported in audit mode only.

How to enable adaptive application controls?

Adaptive application controls help you define a set of applications that are allowed to run on configured groups of machines. This feature is available for both Azure and non-Azure Windows (all versions, classic, or Azure Resource Manager) and Linux machines. Use the following steps to configure your application allow lists:

1. Open the **Security Center** dashboard.
2. In the left pane, select **Adaptive application controls** located under **Advanced cloud defense**.



The **Adaptive application controls** page appears.

Security Center - Adaptive application controls

Showing subscription 'Contoso IT - demo'

What is application control?

Application control helps you deal with malicious and/or unauthorized software, by allowing only specific applications to run on your VMs

How does it work?

Security Center analyzes data of applications to find VMs for which there is a constant set of running applications. Security Center creates whitelisting rules for each group and presents the rules in the form of a recommendation. Once the recommendation is resolved, Security Center configures it by leveraging Applocker capabilities.

[For more information go to the documentation >](#)

Groups of VMs

VMS AND COMPUTERS Recommended No recommendation

Groups of VMs in which the set of applications on the associated VMs keeps changing, and thus is not recommended for an application whitelist control.

| NAME | VMS AND COMPUTERS |
|-------------------|-------------------|
| Contoso IT - demo | 11 |
| CONTOSO2ADEMO | 1 |
| CONTOSOAZUREHQ-DR | 1 |
| DRYRUN2 | 3 |
| DRYRUN40 | 3 |
| DRYRUN50 | 3 |

The **Groups of VMs** section contains three tabs:

- **Configured:** list of groups containing the VMs that were configured with application control.
- **Recommended:** list of groups for which application control is recommended. Security Center uses machine

learning to identify VMs that are good candidates for application control based on whether the VMs consistently run the same applications.

- **No recommendation:** list of groups containing VMs without any application control recommendations. For example, VMs on which applications are always changing, and haven't reached a steady state.

NOTE

Security Center uses a proprietary clustering algorithm to create groups of VMs making sure that similar VMs get the optimal recommended application control policy.

Configure a new application control policy

1. Select the **Recommended** tab for a list of groups with application control recommendations:

- What is application control?
- How does it work?

| Configured | Recommended | No recommendation | | | | |
|--|-------------------|-------------------|----|----------|----|----|
| Groups of VMs for which we recommend to apply the application whitelist control. | | | | | | |
| GROUP NAME | VMS AND COMPUTERS | STATE | ↑↓ | SEVERITY | ↑↓ | ↑↓ |
| ▼ 🛡 ASC DEMO | 2 | Open | | | | |
| 🌐 CONTOSOWEB | 1 | Open | | High | | |
| 🌐 WL1 | 1 | Open | | High | | |
| ▼ 🛡 Contoso IT - demo | 10 | Open | | | | |
| 🌐 GROUP1 | 2 | Open | | High | | |
| 🌐 GROUP2 | 2 | Open | | High | | |
| 🌐 GROUP3 | 3 | Open | | High | | |
| 🌐 GROUP1-EU | 2 | Open | | High | | |
| 🌐 GROUP2-EU | 1 | Open | | High | | |

The list includes:

- **Group Name:** The name of the subscription and group
- **VMs and Computers:** The number of virtual machines in the group
- **State:** the state of the recommendations
- **Severity:** the severity level of the recommendations

2. Click on a group to open the **Create application control rules** option.

3. In the **Select VMs**, review the list of recommended VMs and uncheck any you do not want to apply an application whitelisting policy to. Next, you see two lists:
 - **Recommended applications:** a list of applications that are frequent on the VMs within this group, and are recommended to be allowed to run.
 - **More applications:** a list of applications that are either less frequent on the VMs within this group or that are known as Exploitables (see more below), and recommended for review.
4. Review the applications in each of the lists, and uncheck any you do not want to apply. Each list includes:
 - **NAME:** the certificate information or the full path of an application
 - **FILE TYPES:** the application file type. This can be EXE, Script, MSI, or any permutation of these types.
 - **EXPLOITABLE:** a warning icon indicates if a specific application could be used by an attacker to bypass an application allow list. It is recommended to review these applications prior to their approval.
 - **USERS:** users that are recommended to be allowed to run an application
5. Once you finish your selections, select **Create**.

After you select Create, Azure Security Center automatically creates the appropriate rules on top of the built-in application allow list solution available on Windows servers (AppLocker).

NOTE

- Security Center relies on a minimum of two weeks of data in order to create a baseline and populate the unique recommendations per group of VMs. New customers of Security Center standard tier should expect a behavior in which at first their groups of VMs appear under the *no recommendation* tab.
- Adaptive Application Controls from Security Center doesn't support VMs for which an AppLocker policy is already enabled by either a GPO or a local security policy.
- As a security best practice, Security Center will always try to create a publisher rule for applications that are selected to be allowed, and only if an application doesn't have a publisher information (aka not signed), a path rule will be created for the full path of the specific application.

Editing and monitoring a group configured with application control

1. To edit and monitor a group configured with an application allow list policy, return to the **Adaptive application controls** page and select **CONFIGURED** under **Groups of VMs**:

Groups of VMs

Configured Recommended No recommendation

Groups of VMs for which an application whitelist is already applied and can be centrally managed.

| GROUP NAME | VMS AND COMPUTERS | MODE | ISSUES |
|----------------------|-------------------|-------|--------|
| ▼ Contoso IT - demo | 6 | | |
| A-MANAGEMENT | 2 | Audit | |
| CONTOSOONPREMHQ | 3 | Audit | |
| CONTOSORETAILDEV | 1 | Audit | |

The list includes:

- **Group Name:** the name of the subscription and group
- **VMs and Computers:** the number of virtual machines in the group
- **Mode:** Audit mode will log attempts to run applications that aren't on the allow list; Enforce will not allow applications to run unless they are on the allow list
- **Alerts:** any current violations

2. Click on a group to make changes in the **Edit application control policy** page.

The screenshot shows the 'Edit application control policy' page. In the 'Protection mode' section, 'Audit' is selected. The 'Policy extension' section contains a table with three rows, each representing a whitelisted path and its associated file types and users. The 'Save' and 'Discard' buttons are at the bottom.

3. Under **Protection mode**, you have the option to select between the following:

- **Audit:** in this mode, the application control solution does not enforce the rules, and only audits the activity on the protected VMs. This is recommended for scenarios where you want to first observe the overall behavior before blocking an app to run in the target VM.
- **Enforce:** in this mode, the application control solution does enforce the rules, and makes sure that applications that are not allowed to run are blocked.

NOTE

- **Enforce** protection mode is disabled until further notice.
- As previously mentioned, by default a new application control policy is always configured in *Audit* mode.

4. Under **Policy extension**, add any application path that you want to allow. After you add these paths,

Security Center updates the application allow list policy on the VMs within the selected group of VMS and creates the appropriate rules for these applications, in addition to the rules that are already in place.

5. Review the current violations listed in the **Recent alerts** section. Click on each line to be redirected to the **Alerts** page within Azure Security Center, and view all the alerts that were detected by Azure Security Center on the associated VMs.

- **Alerts:** any violations that were logged.
- **No. of VMs:** the number of virtual machines with this alert type.

6. Under **Publisher whitelisting rules**, **Path whitelisting rules**, and **Hash whitelisting rules** you can see which application whitelisting rules are currently configured on the VMs within a group, according to the rule collection type. For each rule you can see:

- **Rule:** The specific parameters according to which an application is examined by AppLocker to determine if an application is allowed to run.
- **File type:** The file types that are covered by a specific rule. This can be any of the following: EXE, Script, MSI, or any permutation of those file types.
- **Users:** Name or number of users who are allowed to run an application that is covered by an application whitelisting rule.

| Publisher whitelisting rules | |
|--|---------------------|
| <input type="text"/> Search to filter items... | |
| RULE | USERS |
|  Vendor: O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US | 5 Users allowed ... |

7. Click on the three dots at the end of each line if you want to delete the specific rule or edit the allowed users.

8. After making changes to an **Adaptive application controls** policy, click **Save**.

Not recommended list

Security Center only recommends application whitelisting policies for virtual machines running a stable set of applications. Recommendations are not created if applications on the associated VMs keep changing.

| Groups of VMs | |
|--|-------------------|
| Configured | Recommended |
| Groups of VMs in which the set of applications on the associated VMs keeps changing, and thus is not recommended for an application whitelist control. | |
| GROUP NAME | VMS AND COMPUTERS |
|  Contoso IT - demo | 11 |
|  CONTOSOA2ADEMO | 1 |
|  CONTOSOAZUREHQ-DR | 1 |
|  DRYRUN2 | 3 |
|  DRYRUN40 | 3 |
|  DRYRUN50 | 3 |

The list contains:

- **Group Name:** the name of the subscription and group
- **VMs and Computers:** the number of virtual machines in the group

Azure Security Center enables you to define an application whitelisting policy on non-recommended groups of VMs as well. Follow the same principles as were previously described, to configure an application whitelisting policy on those groups as well.

Move a VM from one group to another

When you move a VM from one group to another, the application control policy applied to it changes to the settings of the group that you moved it to. You can also move a VM from a configured group to a non-configured group, which results in removing any application control policy that was previously applied to the VM.

1. From the **Adaptive application controls** page, from the **CONFIGURED** tab, click the group which the VM to be moved currently belongs to.
2. Click **Configured VMs and Computers**.
3. Click the three dots in the line of the VM to move and click **Move**. The **Move computer to different group** window opens.

The screenshot shows the Azure Security Center interface for editing application control policies. The top navigation bar includes Home, Security Center - Overview, Security Center - Adaptive application controls, and Edit application control policy. The main area is titled 'Edit application control policy' for 'CONTOSOWEB-DEMO'. Under 'Group settings', there's a search bar labeled 'Search to filter items...'. Below it is a table titled 'MACHINE' with four entries: contosowebdc, contosowebbe2, contosowebfe1, and contosowebbe3. The 'contosowebdc' row has a context menu with options 'Move' and 'Delete', where 'Move' is highlighted with a red box. At the bottom are 'Save' and 'Discard' buttons.

4. Select the group to move the VM to, and click **Move Computer**, and click **Save**.

The screenshot shows the 'Move computer to different group' dialog box. The left side of the dialog is part of the 'Edit application control policy' interface, showing the same machine list as the previous screenshot. The right side of the dialog has a title 'Move computer to different group' and a subtitle 'contosowebdc'. It contains a message: 'Select an application control policy group from the list below to which you wish to move the selected VM or server'. Below this is a list of groups:

- CONFIGURED GROUPS
 - WL1
- GROUPS FOR REVIEW
 - No results

At the bottom are 'Save' and 'Discard' buttons on the left, and 'Move Computer' and 'Cancel' buttons on the right.

NOTE

Be sure to click **Save** after clicking **Move Computer**. If you do not click **Save**, then the computer will not be moved.

Next steps

In this document, you learned how to use adaptive application control in Azure Security Center to whitelist applications running in Azure and non-Azure VMs. To learn more about Azure Security Center, see the following:

- [Managing and responding to security alerts in Azure Security Center](#). Learn how to manage alerts, and respond to security incidents in Security Center.
- [Security health monitoring in Azure Security Center](#). Learn how to monitor the health of your Azure resources.
- [Understanding security alerts in Azure Security Center](#). Learn about the different types of security alerts.
- [Azure Security Center Troubleshooting Guide](#). Learn how to troubleshoot common issues in Security Center.
- [Azure Security Blog](#). Find blog posts about Azure security and compliance.

File Integrity Monitoring in Azure Security Center

2/25/2020 • 7 minutes to read • [Edit Online](#)

Learn how to configure File Integrity Monitoring (FIM) in Azure Security Center using this walkthrough.

What is FIM in Security Center?

File Integrity Monitoring (FIM), also known as change monitoring, examines files and registries of operating system, application software, and others for changes that might indicate an attack. A comparison method is used to determine if the current state of the file is different from the last scan of the file. You can leverage this comparison to determine if valid or suspicious modifications have been made to your files.

Security Center's File Integrity Monitoring validates the integrity of Windows files, Windows registry, and Linux files. You select the files that you want monitored by enabling FIM. Security Center monitors files with FIM enabled for activity such as:

- File and Registry creation and removal
- File modifications (changes in file size, access control lists, and hash of the content)
- Registry modifications (changes in size, access control lists, type, and the content)

Security Center recommends entities to monitor, which you can easily enable FIM on. You can also define your own FIM policies or entities to monitor. This walkthrough shows you how.

NOTE

The File Integrity Monitoring (FIM) feature works for Windows and Linux computers and VMs and is available on the Standard tier of Security Center. See [Pricing](#) to learn more about Security Center's pricing tiers. FIM uploads data to the Log Analytics workspace. Data charges apply, based on the amount of data you upload. See [Log Analytics pricing](#) to learn more.

FIM uses the Azure Change Tracking solution to track and identify changes in your environment. When File Integrity Monitoring is enabled, you have a **Change Tracking** resource of type **Solution**. For data collection frequency details, see [Change Tracking data collection details](#) for Azure Change Tracking.

NOTE

If you remove the **Change Tracking** resource, you will also disable the File Integrity Monitoring feature in Security Center.

Which files should I monitor?

You should think about the files that are critical for your system and applications when choosing which files to monitor. Consider choosing files that you don't expect to change without planning. Choosing files that are frequently changed by applications or operating system (such as log files and text files) create a lot of noise which make it difficult to identify an attack.

Security Center recommends which files you should monitor as a default according to known attack patterns that include file and registry changes.

Using File Integrity Monitoring

1. Open the **Security Center** dashboard.

2. In the left pane under **Advanced Cloud Defense**, select **File Integrity Monitoring**.

The screenshot shows the Azure Security Center - Overview dashboard. On the left, there's a navigation menu with sections like Overview, Getting started, Events, Search, Policy & Compliance, Resource security hygiene, Threat protection, Automation & Orchestration, Advanced Cloud Defense, and File Integrity Monitoring (which is highlighted with a red box). The main area displays various metrics and charts. In the 'File Integrity Monitoring' section, it shows 166 covered resources, a secure score of 800 out of 1.2K, and 37 active recommendations. It also includes a chart of security alerts by severity (High: 36, Medium: 23, Low: 7) and a timeline of security alerts over time.

File Integrity Monitoring opens.

The screenshot shows a list of workspaces under the File Integrity Monitoring workspace. Each row contains information about the workspace, including its name, total changes, total computers, location, subscription, and status buttons (Upgrade Plan or Enable).

| WORKSPACE NAME | TOTAL CHANGES | TOTAL COMPUTERS | LOCATION | SUBSCRIPTION | |
|--|---------------|-----------------|----------|-------------------|---------------------------|
| testingworkspacecmdlet | 0 | 0 | East US | Contoso IT - demo | UPGRADE PLAN |
| a-mgmtworkspace | 0 | 2 | East US | Contoso IT - demo | ENABLE |
| contosoretail-it | 351 | 56 | East US | Contoso IT - demo | |
| defaultworkspace-e4272367-5645-4c4e-9c67-3b... | 0 | 1 | East US | Contoso IT - demo | |
| oms-experience-center-2016 | 0 | 21 | East US | Contoso IT - demo | ENABLE |

The following information is provided for each workspace:

- Total number of changes that occurred in the last week (you may see a dash “-” if FIM is not enabled on the workspace)
- Total number of computers and VMs reporting to the workspace
- Geographic location of the workspace
- Azure subscription that the workspace is under

The following buttons may also be shown for a workspace:

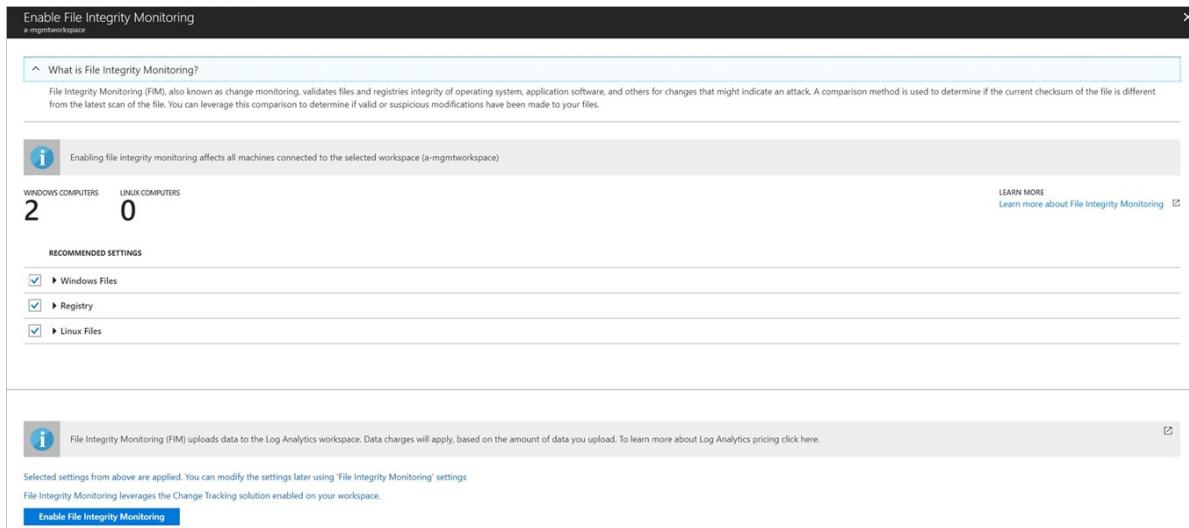
- ENABLE Indicates that FIM is not enabled for the workspace. Selecting the workspace lets you enable FIM on all machines under the workspace.
- UPGRADE PLAN Indicates that the workspace or subscription is not running under Security Center’s Standard tier. To use the FIM feature, your subscription must be running Standard. Selecting the workspace enables you to upgrade to Standard. To learn more about the Standard tier and how to upgrade, see [Upgrade to Security Center’s Standard tier for enhanced security](#).
- A blank (there is no button) means that FIM is already enabled on the workspace.

Under **File Integrity Monitoring**, you can select a workspace to enable FIM for that workspace, view the File Integrity Monitoring dashboard for that workspace, or [upgrade](#) the workspace to Standard.

Enable FIM

To enable FIM on a workspace:

1. Under **File Integrity Monitoring**, select a workspace with the **Enable** button.
2. **Enable file integrity monitoring** opens displaying the number of Windows and Linux machines under the workspace.



The recommended settings for Windows and Linux are also listed. Expand **Windows files**, **Registry**, and **Linux files** to see the full list of recommended items.

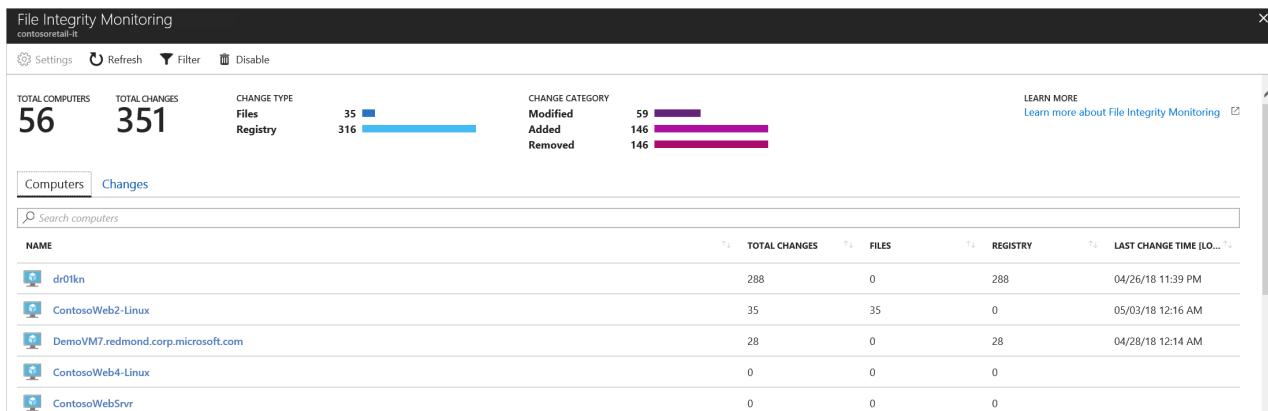
3. Uncheck any recommended entities you do not want to apply FIM to.
4. Select **Apply file integrity monitoring** to enable FIM.

NOTE

You can change the settings at any time. See Edit monitored entities below to learn more.

View the FIM dashboard

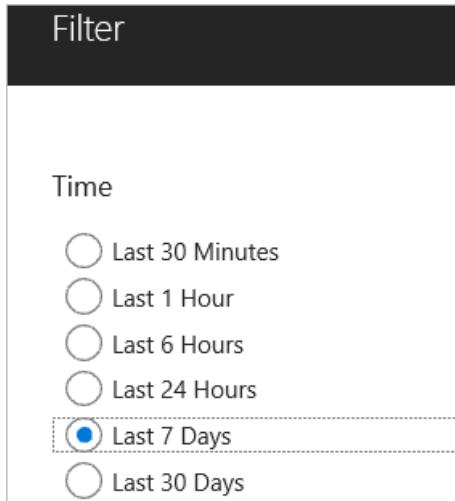
The **File integrity monitoring** dashboard displays for workspaces where FIM is enabled. The FIM dashboard opens after you enable FIM on a workspace or when you select a workspace in the **File Integrity Monitoring** window that already has FIM enabled.



The FIM dashboard for a workspace displays the following details:

- Total number of machines connected to the workspace
- Total number of changes that occurred during the selected time period
- A breakdown of change type (files, registry)
- A breakdown of change category (modified, added, removed)

Selecting Filter at the top of the dashboard lets you apply the period of time that you want to see changes for.



The **Computers** tab (shown above) lists all machines reporting to this workspace. For each machine, the dashboard lists:

- Total changes that occurred during the selected period of time
- A breakdown of total changes as file changes or registry changes

Log Search opens when you enter a machine name in the search field or select a machine listed under the Computers tab. Log Search displays all the changes made during the selected time period for the machine. You can expand a change for more information.

The screenshot shows the Log Search interface with a query for ConfigurationChange on ContosoWeb1. The results table shows four entries for 'web.config' files modified on 2/27/2018. The columns are: TimeGenerated, Computer, ConfigChangeType, ChangeCategory, Name, FileSystemPath, Size, and DateCreated.

| TimeGenerated | Computer | ConfigChangeType | ChangeCategory | Name | FileSystemPath | Size | DateCreated |
|--------------------------|-------------------------------|------------------|----------------|------------|---|--------|-------------|
| 2/27/2018 7:44:24.763 PM | ContosoWeb1.ContosoRetail.com | Files | Modified | web.config | C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\web.config | 43,133 | 7/16/2016 |
| 2/27/2018 6:44:25.227 PM | ContosoWeb1.ContosoRetail.com | Files | Modified | web.config | C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\web.config | 43,133 | 7/16/2016 |
| 2/27/2018 5:44:35.450 PM | ContosoWeb1.ContosoRetail.com | Files | Modified | web.config | C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\web.config | 43,133 | 7/16/2016 |
| 2/27/2018 4:44:25.603 PM | ContosoWeb1.ContosoRetail.com | Files | Modified | web.config | C:\Windows\Microsoft.NET\Framework\v4.0.30319\Config\web.config | 43,133 | 7/16/2016 |

The **Changes** tab (shown below) lists all changes for the workspace during the selected time period. For each entity that was changed, the dashboard lists the:

- Computer that the change occurred on
- Type of change (registry or file)
- Category of change (modified, added, removed)
- Date and time of change

TOTAL COMPUTERS **TOTAL CHANGES**

CHANGE TYPE

| Files | Registry | 35 | 316 |
|-------|----------|----|-----|
|-------|----------|----|-----|

CHANGE CATEGORY

| Modified | Added | Removed |
|----------|-------|---------|
| 59 | 146 | 146 |

LEARN MORE [Learn more about File Integrity Monitoring](#)

Computers **Changes**

i Presenting the latest 100 changes. Click here to view all changes in Log Analytics.

Search changes

| ENTITY | COMPUTER | TYPE | CATEGORY | CHANGE TIME [LOC...] |
|---------------------|-------------------|-------|----------|----------------------|
| /etc/webserver.conf | ContosoWeb2-Linux | Files | Modified | 05/03/18 12:16 AM |
| /etc/webserver.conf | ContosoWeb2-Linux | Files | Modified | 05/02/18 11:16 PM |
| /etc/webserver.conf | ContosoWeb2-Linux | Files | Modified | 05/02/18 09:44 PM |
| /etc/webserver.conf | ContosoWeb2-Linux | Files | Modified | 05/02/18 08:06 PM |

Change details opens when you enter a change in the search field or select an entity listed under the **Changes** tab.

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDl\RemoveS... **X**

Change details

| PROPERTY | VALUE BEFORE | VALUE AFTER |
|---------------------------|---|---|
| Acls | [{ "Name": "owner" "Value": "NT AUTHORITY\\SYSTEM" } { ...] | [{ "Name": "owner" "Value": "NT AUTHORITY\\SYSTEM" } { ...] |
| ValueData | C:\Windows\System32\WINTRUST.DLL | C:\Windows\SysWOW64\WINTRUST.DLL |
| ▼ Unchanged properties... | | |
| SourceComputer | cda27197-3886-4fbb-8720-1f2304d1ae1d | No Change |
| RegistryKey | HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\OID\EncodingType 0\CryptSIPDl\RemoveS... | No Change |
| Hive | HKEY_LOCAL_MACHINE | No Change |
| ValueName | Dll | No Change |
| ValueType | REG_SZ | No Change |
| Size | 32 | No Change |
| SourceSystem | OpsManager | No Change |
| MG | 00000000-0000-0000-0000-000000000001 | No Change |
| ManagementGroup | AOI-5bc7c24b-ad6c-4f7f-905c-3ac3f3259938 | No Change |
| TenantId | 5bc7c24b-ad6c-4f7f-905c-3ac3f3259938 | No Change |
| VMUUID | c14ded1b-054b-4483-9fd1-1829eb76c406 | No Change |

Edit monitored entities

1. Return to the **File Integrity Monitoring** dashboard and select **Settings**.

TOTAL MACHINES **TOTAL CHANGES**

CHANGE TYPE

| Files | Registry | 4 | 0 |
|-------|----------|---|---|
|-------|----------|---|---|

CHANGE CATEGORY

| Modified | Added | Removed |
|----------|-------|---------|
| 4 | 0 | 0 |

LEARN MORE [Learn more about file integrity monitor](#) [Which files should I monitor](#)

Computers **Changes**

i Presenting the latest 100 changes. Click here to view all changes in Log Analytics.

Search computers

| NAME | TOTAL CHANGES | FILES | REGISTRY | LAST CHANGE TIME |
|-------------------------------|---------------|-------|----------|-------------------|
| ContosoWeb1.ContosoRetail.com | 4 | 4 | 0 | 02/27/18 07:44 PM |
| ContosoAzADD52 | 0 | 0 | 0 | |
| On-Premise-16S | 0 | 0 | 0 | |
| CDMNEBALTVM0397.smx.net | 0 | 0 | 0 | |
| ContosoAzASRVM2 | 0 | 0 | 0 | |

Workspace Configuration opens displaying three tabs: **Windows Registry**, **Windows Files**, and **Linux**

Files. Each tab lists the entities that you can edit in that category. For each entity listed, Security Center identifies if FIM is enabled (true) or not enabled (false). Editing the entity lets you enable or disable FIM.

| GROUP | ENABLED | REGISTRY KEY | RECURSIVE |
|-------------|---------|---|-----------|
| | true | HKEY_LOCAL_MACHINE\Software\contoso | false |
| | true | HKEY_LOCAL_MACHINE\Software\Background\ShellEx\ContextMenuHandlers | false |
| Recommended | true | HKEY_LOCAL_MACHINE\Software\Classes\Directory\ShellEx\ContextMenuHandlers | true |
| Recommended | true | HKEY_LOCAL_MACHINE\Software\Classes\Directory\ShellEx\ContextMenuHandlers | true |
| Recommended | true | HKEY_LOCAL_MACHINE\Software\Classes\Directory\ShellEx\CopyHookHandlers | true |

- Select an identity protection. In this example, we selected an item under Windows Registry. **Edit for Change Tracking** opens.

Enabled
True False

* Item Name
FIM_Registry_118

Group
Security

* Windows Registry Key
HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Cryptography\OID

Under **Edit for Change Tracking** you can:

- Enable (True) or disable (False) file integrity monitoring
- Provide or change the entity name
- Provide or change the value or path
- Delete the entity, discard the change, or save the change

Add a new entity to monitor

- Return to the **File integrity monitoring dashboard** and select **Settings** at the top. **Workspace Configuration** opens.
- Under **Workspace Configuration**, select the tab for the type of entity that you want to add: Windows Registry, Windows Files, or Linux Files. In this example, we selected **Linux Files**.

| GROUP | ENABLED | PATH | TYPE | UNKS | RECURSIVE | SUDO |
|-------------|---------|---------------------------------|------|--------|-----------|------|
| ChangeDemo | true | /etc/webserver.conf | File | Follow | false | true |
| OMSAgent | false | /etc/rsyslog.d/95-omsagent.conf | File | Follow | false | true |
| Recommended | false | /etc/*.*conf | File | Follow | true | true |

- Select **Add**. **Add for Change Tracking** opens.

Add Linux File for Change Tracking X

Save Delete Discard

Enabled
 True False

* Item Name

Group

* Enter Path

Path Type

Recursion
 On Off

Use Sudo
 On Off

Links

- On the **Add** page, type the requested information and select **Save**.

Disable monitored entities

- Return to the **File Integrity Monitoring** dashboard.
- Select a workspace where FIM is currently enabled. A workspace is enabled for FIM if it is missing the **Enable** button or **Upgrade Plan** button.

Security Center - File Integrity Monitoring
Showing all subscriptions

| WORKSPACE NAME | TOTAL CHANGES | TOTAL COMPUTERS | LOCATION | SUBSCRIPTION |
|--|---------------|-----------------|-------------|--------------|
| defaultworkspace-212f9889-769e-45ae-ab43-6d... | 0 | 10 | East US | ASC DEMO |
| jogazit-test | 0 | 1 | East US | ASC DEMO |
| defaultworkspace-212f9889-769e-45ae-ab43-6d... | 0 | 1 | West Europe | ASC DEMO |

UPGRADE PLAN **ENABLE**

- Under File Integrity Monitoring, select **Settings**.

The screenshot shows the FIM dashboard with the following data:

- TOTAL COMPUTERS:** 10
- TOTAL CHANGES:** 0
- CHANGE TYPE:**
 - File: 0
 - Registry: 0
- CHANGE CATEGORY:**
 - Modified: 0
 - Added: 0
 - Removed: 0
- LEARN MORE:** Learn more about File Integrity Monitoring | Which files should be monitored?

| NAME | TOTAL CHANGES | FILES | REGISTRY | LAST CHANGE TIME [LOCAL] |
|----------------------------------|---------------|-------|----------|--------------------------|
| On-Premise-16S | 0 | 0 | 0 | |
| ContosoWebBE2.CONTOSO.europa.com | 0 | 0 | 0 | |

4. Under **Workspace Configuration**, select a group where **Enabled** is set to true.

| GROUP | ENABLED | PATH | TYPE | RECURSIVE |
|----------|---------|-----------------|------|-----------|
| Security | true | C:\autoexec.bat | File | false |
| Security | true | C:\boot.ini | File | false |

5. Under **Edit for Change Tracking** window set **Enabled** to False.

The dialog has the following fields:

- Enabled:** False (highlighted with a red border)
- Item Name:** FIM_WindowsFiles_1
- Group:** Security
- Enter Path:** C:\autoexec.bat

6. Select **Save**.

Folder and path monitoring using wildcards

Use wildcards to simplify tracking across directories. The following rules apply when you configure folder monitoring using wildcards:

- Wildcards are required for tracking multiple files.
- Wildcards can only be used in the last segment of a path, such as C:\folder\file or /etc/*.conf
- If an environment variable includes a path that is not valid, validation will succeed but the path will fail when inventory runs.
- When setting the path, avoid general paths such as c:/*.* which will result in too many folders being traversed.

Disable FIM

You can disable FIM. FIM uses the Azure Change Tracking solution to track and identify changes in your environment. By disabling FIM, you remove the Change Tracking solution from selected workspace.

1. To disable FIM, return to the **File Integrity Monitoring** dashboard.
2. Select a workspace.
3. Under **File Integrity Monitoring**, select **Disable**.

Disable File Integrity Monitoring

File Integrity Monitoring uses the Azure Change Tracking solution to track and identify changes in your environment. By disabling File Integrity Monitoring you remove the Change Tracking solution from workspace: 'contosoretail-it'. [To learn more click here](#)

| Workspace | Size | Changes | Last Change |
|-------------------|-------|---------|--------------------|
| dr01kn | 10.3K | 0 | 04/27/18, 9:39 AM |
| ContosoIT2 | 222 | 2 | 04/24/18, 10:52 PM |
| ContosoJumpBox | 48 | 0 | 04/25/18, 8:01 PM |
| ContosoWeb2-Linux | 35 | 35 | 04/29/18, 7:44 AM |

Remove **Cancel**

4. Select **Remove** to disable.

Next steps

In this article, you learned to use File Integrity Monitoring (FIM) in Security Center. To learn more about Security Center, see the following pages:

- [Setting security policies](#) -- Learn how to configure security policies for your Azure subscriptions and resource groups.
- [Managing security recommendations](#) -- Learn how recommendations help you protect your Azure resources.
- [Security health monitoring](#)--Learn how to monitor the health of your Azure resources.
- [Managing and responding to security alerts](#)--Learn how to manage and respond to security alerts.
- [Monitoring partner solutions](#) -- Learn how to monitor the health status of your partner solutions.
- [Azure Security blog](#)--Get the latest Azure security news and information.

Adaptive Network Hardening in Azure Security Center

11/27/2019 • 4 minutes to read • [Edit Online](#)

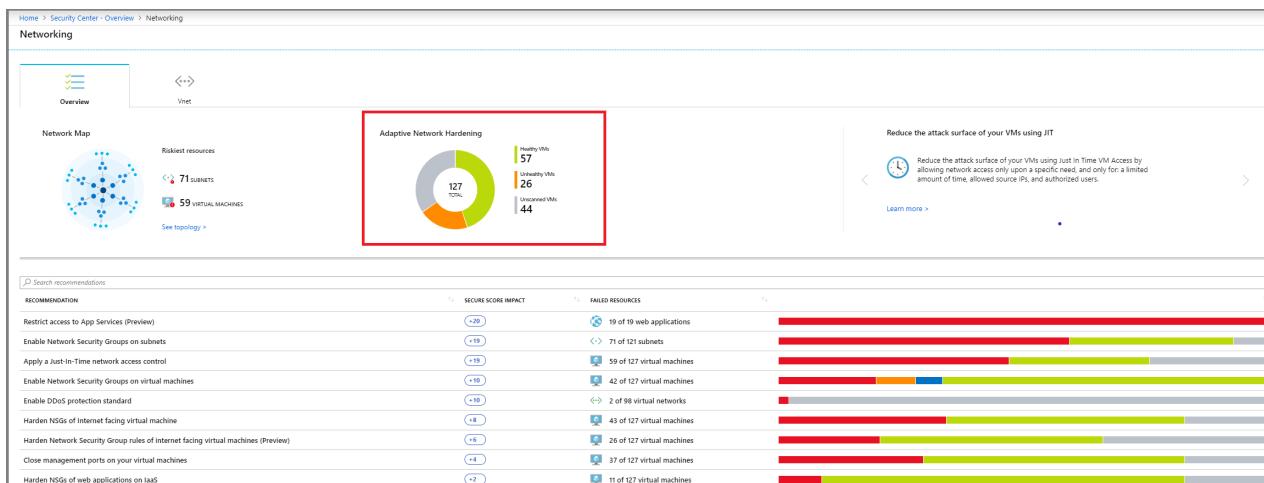
Learn how to configure Adaptive Network Hardening in Azure Security Center.

What is Adaptive Network Hardening?

Applying [network security groups \(NSG\)](#) to filter traffic to and from resources, improves your network security posture. However, there can still be some cases in which the actual traffic flowing through the NSG is a subset of the NSG rules defined. In these cases, further improving the security posture can be achieved by hardening the NSG rules, based on the actual traffic patterns.

Adaptive Network Hardening provides recommendations to further harden the NSG rules. It uses a machine learning algorithm that factors in actual traffic, known trusted configuration, threat intelligence, and other indicators of compromise, and then provides recommendations to allow traffic only from specific IP/port tuples.

For example, let's say the existing NSG rule is to allow traffic from 140.20.30.10/24 on port 22. The Adaptive Network Hardening's recommendation, based on the analysis, would be to narrow the range and allow traffic from 140.23.30.10/29 – which is a narrower IP range, and deny all other traffic to that port.



NOTE

Adaptive Network Hardening recommendations are supported on the following ports: 22, 3389, 21, 23, 445, 4333, 3306, 1433, 1434, 53, 20, 5985, 5986, 5432, 139, 66, 1128

View Adaptive Network Hardening alerts and rules

- In Security Center, select **Networking** -> **Adaptive Network Hardening**. The network VMs are listed under three separate tabs:
 - Unhealthy resources:** VMs that currently have recommendations and alerts that were triggered by running the Adaptive Network Hardening algorithm.
 - Healthy resources:** VMs without alerts and recommendations.
 - Unscanned resources:** VMs that the Adaptive Network Hardening algorithm cannot be run on

because of one of the following reasons:

- **VMs are Classic VMs:** Only Azure Resource Manager VMs are supported.
- **Not enough data is available:** In order to generate accurate traffic hardening recommendations, Security Center requires at least 30 days of traffic data.
- **VM is not protected by ASC standard:** Only VMs that are set to Security Center's Standard pricing tier are eligible for this feature.

| NAME | SUBSCRIPTION |
|-------|-------------------|
| App03 | Contoso IT - demo |
| App04 | Contoso IT - demo |
| App05 | Contoso IT - demo |
| App06 | Contoso IT - demo |
| App07 | Contoso IT - demo |
| App08 | Contoso IT - demo |

- From the **Unhealthy resources** tab, select a VM to view its alerts and the recommended hardening rules to apply.

| TYPE | NAME | DESTINATION PORT | ALLOWED SOURCE IP RANGES | PROTOCOL | ALERTS |
|---|------|------------------|--------------------------|----------|--------|
| System Generated | 22 | None | TCP | 0 | |
| System Generated | 1128 | None | TCP | 2 | |
| SecurityCenter-ANCRule_3389_TCP_Inbound_ALLOW_1551874842891 | 3389 | 167.220.198.345 | TCP | 0 | |
| Allow_DC_Manager | 5506 | 180.212.35.10/30 | TCP/UDP | 0 | |

Review and apply Adaptive Network Hardening recommended rules

- From the **Unhealthy resources** tab, select a VM. The alerts and recommended hardening rules are listed.

| DESCRIPTION | COUNT | DATE | DESTINATION PROTOCOL | DESTINATION PORT | STATE | SEVERITY |
|--|-------|-----------|----------------------|------------------|--------|----------|
| Traffic from forbidden IP addresses was detected | 22 | 3/4/2019 | TCP | 3389 | Active | Low |
| Traffic from forbidden IP addresses was detected | 16 | 2/27/2019 | TCP | 3389 | Active | Low |

NOTE

The **Rules** tab lists the rules that Adaptive Network Hardening recommends you add. The **Alerts** tab lists the alerts that were generated due to traffic flowing to the resource, which is not within the IP range allowed in the recommended rules.

2. If you want to change some of the parameters of a rule, you can modify it, as explained in [Modify a rule](#).

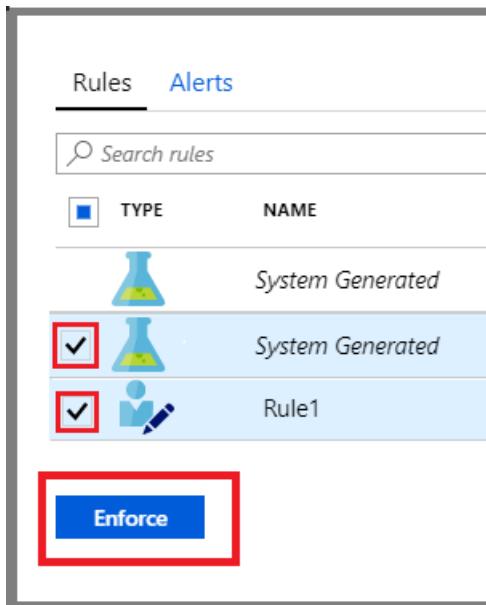
NOTE

You can also [delete](#) or [add](#) a rule.

3. Select the rules that you want to apply on the NSG, and click **Enforce**.

NOTE

The enforced rules are added to the NSG(s) protecting the VM. (A VM could be protected by an NSG that is associated to its NIC, or the subnet in which the VM resides, or both)



Modify a rule

You may want to modify the parameters of a rule that has been recommended. For example, you may want to change the recommended IP ranges.

Some important guidelines for modifying an Adaptive Network Hardening rule:

- You can modify the parameters of "allow" rules only.
- You cannot change "allow" rules to become "deny" rules.

NOTE

Creating and modifying "deny" rules is done directly on the NSG. For more information, see [Create, change, or delete a network security group](#).

- A **Deny all traffic** rule is the only type of "deny" rule that would be listed here, and it cannot be modified. You can, however, delete it (see [Delete a rule](#)).

NOTE

A **Deny all traffic** rule is recommended when, as a result of running the algorithm, Security Center does not identify traffic that should be allowed, based on the existing NSG configuration. Therefore, the recommended rule is to deny all traffic to the specified port. The name of this type of rule is displayed as "*System Generated*". After enforcing this rule, its actual name in the NSG will be a string comprised of the protocol, traffic direction, "DENY", and a random number.

To modify an Adaptive Network Hardening rule:

1. To modify some of the parameters of a rule, in the **Rules** tab, click on the three dots (...) at the end of the rule's row, and click **Edit**.

| Type | Name | Destination Port | Allowed Source IP Ranges | Protocol | Alerts |
|---|------|------------------|--------------------------|----------|--------|
| System Generated | 22 | None | TCP | 0 | ... |
| System Generated | 1128 | None | TCP | 2 | ... |
| SecurityCenter-ANCRule_3389_TCP_Inbound_ALLOW_1551874842891 | 3389 | 167.220.196.245 | TCP | 0 | ... |
| Allow_DC_Manager | 5506 | 180.212.35.10/30 | TCP/UDP | 0 | ... |

2. In the **Edit rule** window, update the details that you want to change, and click **Save**.

NOTE

After clicking **Save**, you have successfully changed the rule. However, you have not applied it to the NSG. To apply it, you must select the rule in the list, and click **Enforce** (as explained in the next step).

| DESTINATION PORT | ALLOWED SOURCE IP RANGES | PROTOCOL | ALERTS |
|-------------------------------------|--------------------------|----------|--------|
| 22 | None | TCP | 0 |
| 21 | None | TCP | 0 |
| 1433 | None | TCP | 0 |
| 1434 | None | TCP | 0 |
| 20 | None | TCP | 0 |
| 1128 | None | TCP | 0 |
| 389_TCP_Inbound_ALLOW_1552212663373 | 167.220.196.245 | TCP | 0 |

3. To apply the updated rule, from the list, select the updated rule and click **Enforce**.

Rules Alerts

Search rules

| TYPE | NAME |
|-------------------------------------|------------------|
| System Generated | System Generated |
| System Generated | System Generated |
| <input checked="" type="checkbox"/> | Rule1 |

Enforce

Add a new rule

You can add an "allow" rule that was not recommended by Security Center.

NOTE

Only "allow" rules can be added here. If you want to add "deny" rules, you can do so directly on the NSG. For more information, see [Create, change, or delete a network security group](#).

To add an Adaptive Network Hardening rule:

1. Click **Add rule** (located in the top-left corner).

Manage Adaptive Network Hardening recommendations

+ Add rule

Recommended rules Total alerts New alerts

4 2 --

| TYPE | NAME | DESTINATION PORT | ALLOWED SOURCE IP RANGES | PROTOCOL | ALERTS |
|---|------|------------------|--------------------------|----------|--------|
| System Generated | 22 | None | TCP | 0 | ... |
| System Generated | 1128 | None | TCP | 2 | ... |
| SecurityCenter-ANCRule_3389_TCP_Inbound_ALLOW_1551874842891 | 3389 | 167.220.196.245 | TCP | 0 | ... |
| Allow_DC_Manager | 5506 | 180.212.35.10/30 | TCP/UDP | 0 | ... |

Enforce

2. In the **New rule** window, enter the details and click **Add**.

NOTE

After clicking **Add**, you have successfully added the rule, and it is listed with the other recommended rules. However, you have not applied it on the NSG. To activate it, you must select the rule in the list, and click **Enforce** (as explained in the next step).

3. To apply the new rule, from the list, select the new rule and click **Enforce**.

| Type | Name | Destination Port | Allowed Source IP Ranges | Protocol | Alerts |
|------------------|---|------------------|--------------------------|----------|--------|
| System Generated | | 22 | None | TCP | 0 |
| System Generated | | 1128 | None | TCP | 2 |
| System Generated | SecurityCenter-ANCRule_3389_TCP_Inbound_ALLOW_1551874842891 | 3389 | 167.220.196.245 | TCP | 0 |
| User-defined | Rule1 | 5506 | 180.212.35.10/30 | TCP/UDP | 0 |

Enforce

Delete a rule

When necessary, you can delete a recommended rule for the current session. For example, you may determine that applying a suggested rule could block legitimate traffic.

To delete an Adaptive Network Hardening rule for your current session:

1. In the **Rules** tab, click on the three dots (...) at the end of the rule's row, and click **Delete**.

| Recommended rules | Total alerts | New alerts |
|-------------------|--------------|------------|
| 4 | 2 | -- |

| Type | Name | Destination Port | Allowed Source IP Ranges | Protocol | Alerts | Actions |
|------------------|---|------------------|--------------------------|----------|--------|---|
| System Generated | System Generated | 22 | None | TCP | 0 | Edit ... |
| System Generated | System Generated | 1128 | None | TCP | 2 | Edit ... |
| System Generated | SecurityCenter-ANCRule_3389_TCP_Inbound_ALLOW_1551874842891 | 3389 | 167.220.196.245 | TCP | 0 | Edit ... |
| User-defined | Allow_DC_Manager | 5506 | 180.212.35.10/30 | TCP/UDP | 0 | Edit Delete ... |

Enforce

Apply disk encryption in Azure Security Center

2/25/2020 • 2 minutes to read • [Edit Online](#)

Azure Security Center recommends that you apply disk encryption if you have Windows or Linux VM disks that are not encrypted using Azure Disk Encryption. Disk Encryption lets you encrypt your Windows and Linux IaaS VM disks. Encryption is recommended for both the OS and data volumes on your VM.

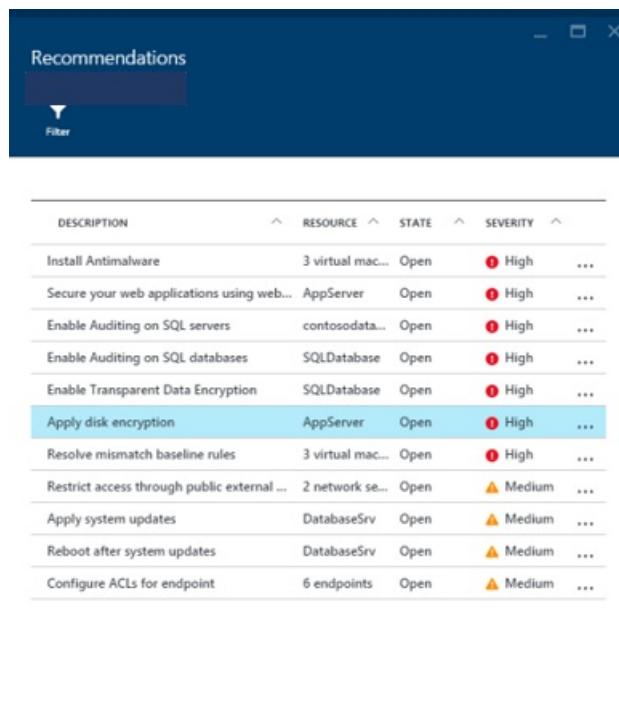
Disk Encryption uses the industry standard [BitLocker](#) feature of Windows and the [DM-Crypt](#) feature of Linux. These features provide OS and data encryption to help protect and safeguard your data and meet your organizational security and compliance commitments. Disk Encryption is integrated with [Azure Key Vault](#) to help you control and manage the disk encryption keys and secrets in your Key Vault subscription, while ensuring that all data in the VM disks are encrypted at rest in your [Azure Storage](#).

NOTE

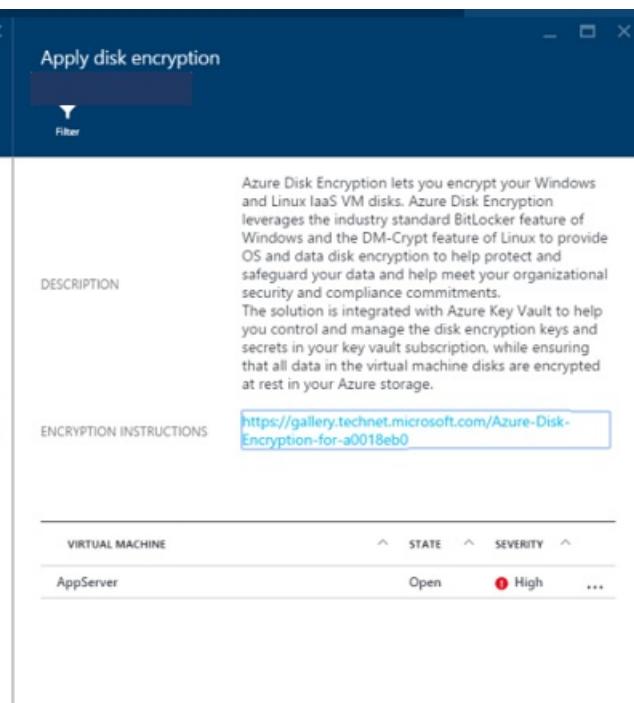
Azure Disk Encryption is supported on the following Windows server operating systems - Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2. Disk encryption is supported on the following Linux server operating systems - Ubuntu, CentOS, SUSE, and SUSE Linux Enterprise Server (SLES).

Implement the recommendation

1. In the **Recommendations** blade, select **Apply disk encryption**.
2. In the **Apply disk encryption** blade, you see a list of VMs for which Disk Encryption is recommended.
3. Follow the instructions to apply encryption to these VMs.



| DESCRIPTION | RESOURCE | STATE | SEVERITY | ... |
|---|------------------|-------------|-------------|------------|
| Install Antimalware | 3 virtual mac... | Open | High | ... |
| Secure your web applications using web... | AppServer | Open | High | ... |
| Enable Auditing on SQL servers | contosodata... | Open | High | ... |
| Enable Auditing on SQL databases | SQLDatabase | Open | High | ... |
| Enable Transparent Data Encryption | SQLDatabase | Open | High | ... |
| Apply disk encryption | AppServer | Open | High | ... |
| Resolve mismatch baseline rules | 3 virtual mac... | Open | High | ... |
| Restrict access through public external ... | 2 network se... | Open | Medium | ... |
| Apply system updates | DatabaseSrv | Open | Medium | ... |
| Reboot after system updates | DatabaseSrv | Open | Medium | ... |
| Configure ACLs for endpoint | 6 endpoints | Open | Medium | ... |



Azure Disk Encryption lets you encrypt your Windows and Linux IaaS VM disks. Azure Disk Encryption leverages the industry standard BitLocker feature of Windows and the DM-Crypt feature of Linux to provide OS and data disk encryption to help protect and safeguard your data and help meet your organizational security and compliance commitments. The solution is integrated with Azure Key Vault to help you control and manage the disk encryption keys and secrets in your key vault subscription, while ensuring that all data in the virtual machine disks are encrypted at rest in your Azure storage.

<https://gallery.technet.microsoft.com/Azure-Disk-Encryption-for-a0018eb0>

| VIRTUAL MACHINE | STATE | SEVERITY | ... |
|-----------------|-------|----------|-----|
| AppServer | Open | High | ... |

To encrypt Azure Virtual Machines that have been identified by Security Center as needing encryption, we recommend the following steps:

- Install and configure Azure PowerShell. This enables you to run the PowerShell commands required to set up the prerequisites required to encrypt Azure Virtual Machines.
- Obtain and run the Azure Disk Encryption Prerequisites Azure PowerShell script.

- Encrypt your virtual machines.

[Encrypt a Windows IaaS VM with Azure PowerShell](#) walks you through these steps. This topic assumes you are using a Windows client machine from which you configure disk encryption.

There are many approaches that can be used for Azure Virtual Machines. If you are already well-versed in Azure PowerShell or Azure CLI, then you may prefer to use alternate approaches. To learn about these other approaches, see [Azure disk encryption](#).

See also

This document showed you how to implement the Security Center recommendation "Apply disk encryption." To learn more about disk encryption, see the following:

- [Encryption and key management with Azure Key Vault](#) (video, 36 min 39 sec) -- Learn how to use disk encryption management for IaaS VMs and Azure Key Vault to help protect and safeguard your data.
- [Azure disk encryption](#) (document) -- Learn how to enable disk encryption for Windows and Linux VMs.

To learn more about Security Center, see the following:

- [Setting security policies in Azure Security Center](#) -- Learn how to configure security policies.
- [Security health monitoring in Azure Security Center](#) -- Learn how to monitor the health of your Azure resources.
- [Managing and responding to security alerts in Azure Security Center](#) -- Learn how to manage and respond to security alerts.
- [Managing security recommendations in Azure Security Center](#) -- Learn how recommendations help you protect your Azure resources.
- [Azure Security blog](#) -- Find blog posts about Azure security and compliance.

Apply system updates in Azure Security Center

2/25/2020 • 2 minutes to read • [Edit Online](#)

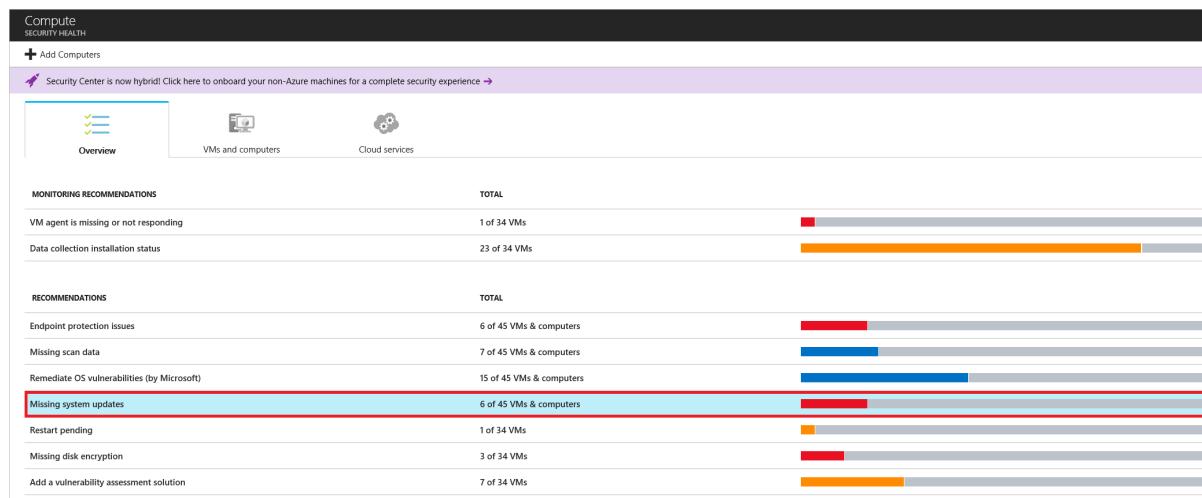
Azure Security Center monitors daily Windows and Linux virtual machines (VMs) and computers for missing operating system updates. Security Center retrieves a list of available security and critical updates from Windows Update or Windows Server Update Services (WSUS), depending on which service is configured on a Windows computer. Security Center also checks for the latest updates in Linux systems. If your VM or computer is missing a system update, Security Center will recommend that you apply system updates.

Implement the recommendation

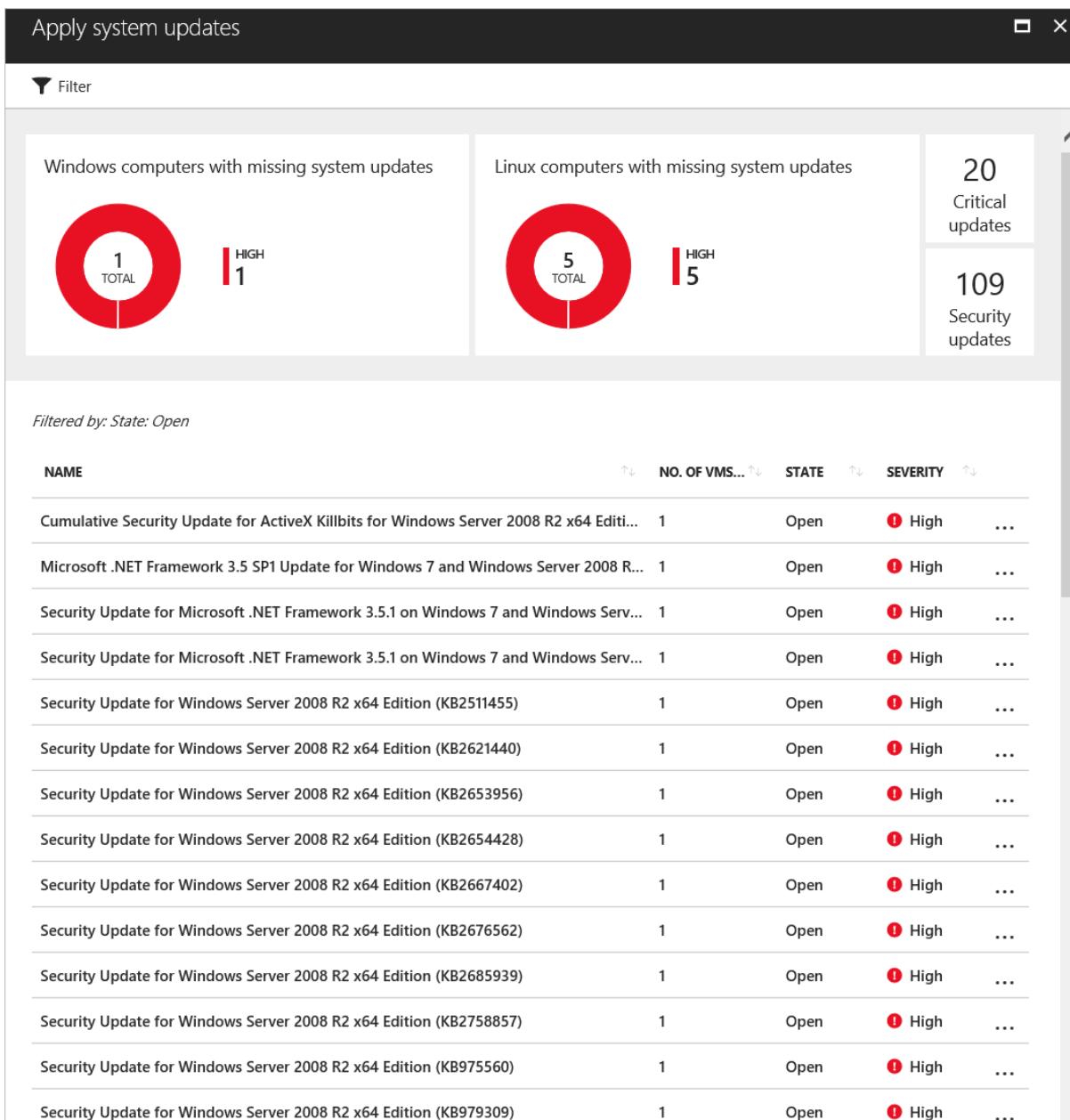
Apply system updates is presented as a recommendation in Security Center. If your VM or computer is missing a system update, this recommendation will be displayed under **Recommendations** and under **Compute**. Selecting the recommendation opens the **Apply system updates** dashboard.

In this example, we will use **Compute**.

1. Select **Compute** under the Security Center main menu.



2. Under **Compute**, select **Missing system updates**. The **Apply system updates** dashboard opens.



The top of the dashboard provides:

- The total number of Windows and Linux VMs and computers missing system updates.
- The total number of critical updates missing across your VMs and computers.
- The total number of security updates missing across your VMs and computers.

The bottom of the dashboard lists all missing updates across your VMs and computers, and the severity of the missing update. The list includes:

- NAME: Name of the missing update.
- NO. OF VMs & COMPUTERS: Total number of VMs and computers that are missing this update.
- STATE: The current state of the recommendation:
 - Open: The recommendation has not been addressed yet.
 - In Progress: The recommendation is currently being applied to those resources, and no action is required by you.
 - Resolved: The recommendation was already finished. (When the issue has been resolved, the entry is dimmed).
- SEVERITY: Describes the severity of that particular recommendation:

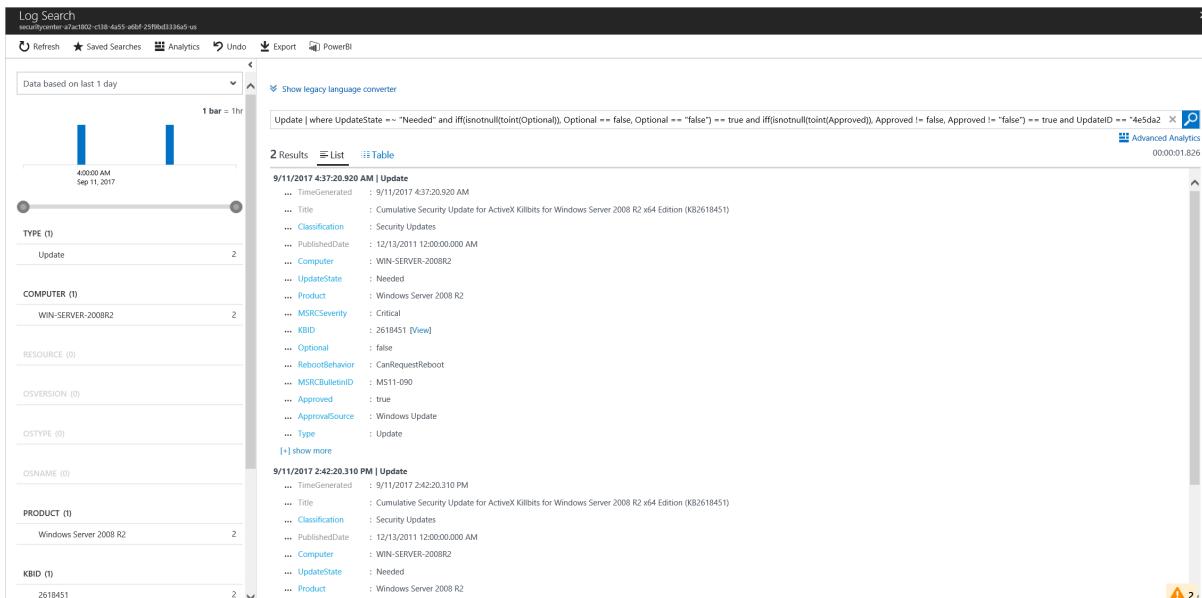
- High: A vulnerability exists with a meaningful resource (application, virtual machine, or network security group) and requires attention.
 - Medium: Non-critical or additional steps are required to complete a process or eliminate a vulnerability.
 - Low: A vulnerability should be addressed but does not require immediate attention. (By default, low recommendations are not presented, but you can filter on low recommendations if you want to view them.)
3. Select a missing update in the list to view details.

| | |
|--------------------|--|
| KBID | 2618451 |
| SYSTEM UPDATE NAME | Cumulative Security Update for ActiveX Killbits for Windows Server 2008 R2 x64 Edition (KB2618451) |
| CLASSIFICATION | Security Updates |
| SEVERITY | Critical |
| SUPPORT | https://support.microsoft.com/kb/2618451 |
| RELEASE DATE | 2011-12-13T08:00:00Z |

4. Select the **Search** icon in the top ribbon. An Azure Monitor logs search query opens filtered to the computers missing the update.

| SOURCECOMPUTER | COMPUTER | AGGREGATEDVALUE |
|-------------------------------------|-------------------|-----------------|
| 87723414-df8b-4607-b737-be4b82ebf5a | WIN-SERVER-2008R2 | 1 |

5. Select a computer from the list for more information. Another search result opens with information filtered only for that computer.



Next steps

To learn more about Security Center, see the following:

- [Setting security policies in Azure Security Center](#) -- Learn how to configure security policies for your Azure subscriptions and resource groups.
- [Managing security recommendations in Azure Security Center](#) -- Learn how recommendations help you protect your Azure resources.
- [Security health monitoring in Azure Security Center](#) -- Learn how to monitor the health of your Azure resources.
- [Managing and responding to security alerts in Azure Security Center](#) -- Learn how to manage and respond to security alerts.
- [Monitoring partner solutions with Azure Security Center](#) -- Learn how to monitor the health status of your partner solutions.
- [Azure Security blog](#) -- Find blog posts about Azure security and compliance.

Manage endpoint protection issues with Azure Security Center

2/25/2020 • 4 minutes to read • [Edit Online](#)

Azure Security Center monitors the status of antimalware protection and reports this under the Endpoint protection issues page. Security Center highlights issues, such as detected threats and insufficient protection, which can make your virtual machines (VMs) and computers vulnerable to antimalware threats. By using the information under **Endpoint protection issues**, you can identify a plan to address any issues identified.

Security Center reports the following endpoint protection issues:

- Endpoint protection not installed on Azure VMs – A supported antimalware solution is not installed on these Azure VMs.
- Endpoint protection not installed on non-Azure computers – A supported antimalware is not installed on these non-Azure computers.
- Endpoint protection health:
 - Signature out of date – An antimalware solution is installed on these VMs and computers, but the solution does not have the latest antimalware signatures.
 - No real time protection – An antimalware solution is installed on these VMs and computers, but it is not configured for real-time protection. The service may be disabled or Security Center may be unable to obtain the status because the solution is not supported. See [partner integration](#) for a list of supported solutions.
 - Not reporting – An antimalware solution is installed but not reporting data.
 - Unknown – An antimalware solution is installed but its status is unknown or reporting an unknown error.

NOTE

See [Integrate security solutions](#) for a list of endpoint protection security solutions integrated with Security Center.

Implement the recommendation

Endpoint protection issues is presented as a recommendation in Security Center. If your environment is vulnerable to antimalware threats, this recommendation will be displayed under **Recommendations** and under **Compute**. To see the **Endpoint protection issues dashboard**, you need to follow the Compute workflow.

In this example, we will use **Compute**. We will look at how to install antimalware on Azure VMs and on non-Azure computers.

Install antimalware on Azure VMs

1. Select **Compute & apps** under the Security Center main menu or **Overview**.

The screenshot shows the Compute Security Health dashboard. At the top, there are three navigation links: Overview, VMs and computers, and Cloud services. Below these are sections for Monitoring Recommendations and Recommendations.

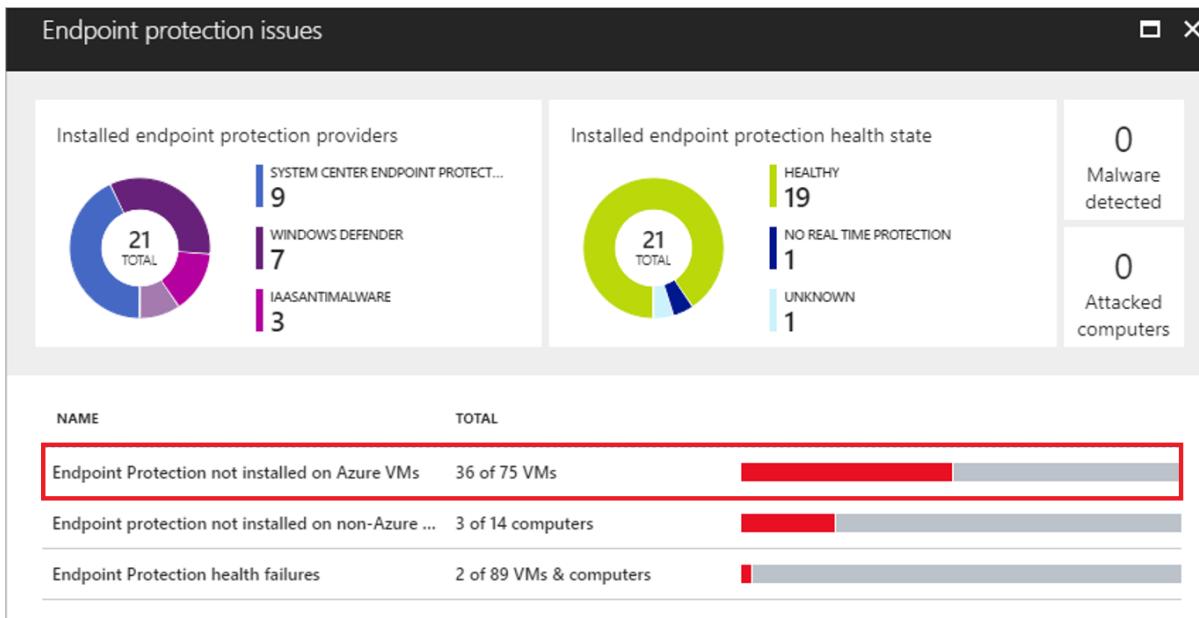
MONITORING RECOMMENDATIONS

| | TOTAL |
|---------------------------------------|--------------|
| VM agent is missing or not responding | 1 of 34 VMs |
| Data collection installation status | 23 of 34 VMs |

RECOMMENDATIONS

| | TOTAL |
|---|--------------------------|
| Endpoint protection issues | 6 of 45 VMs & computers |
| Missing scan data | 7 of 45 VMs & computers |
| Remediate OS vulnerabilities (by Microsoft) | 15 of 45 VMs & computers |
| Missing system updates | 6 of 45 VMs & computers |
| Restart pending | 1 of 34 VMs |
| Missing disk encryption | 3 of 34 VMs |
| Add a vulnerability assessment solution | 7 of 34 VMs |

2. Under **Compute**, select **Endpoint protection issues**. The **Endpoint protection issues** dashboard opens.



The top of the dashboard provides:

- Installed endpoint protection providers - Lists the different providers identified by Security Center.
- Installed endpoint protection health state - Shows the health state of VMs and computers that have an endpoint protection solution installed. The chart shows the number of VMs and computers that are healthy and the number with insufficient protection.
- Malware detected – Shows the number of VMs and computers where Security Center is reporting detected malware.
- Attacked computers – Shows the number of VMs and computers where Security Center is reporting attacks by malware.

At the bottom of the dashboard there is a list of endpoint protection issues which includes the following information:

- **TOTAL** - The number of VMs and computers impacted by the issue.
- A bar aggregating the number of VMs and computers impacted by the issue. The colors in the bar identify priority:
 - Red - High priority and should be addressed immediately
 - Orange - Medium priority and should be addressed as soon as possible

3. Select **Endpoint protection not installed on Azure VMs**.

4. Under **Endpoint protection not installed on Azure VMs** is a list of Azure VMs that do not have antimalware installed. You can choose to install antimalware on all VMs in the list or select individual VMs to install antimalware on by clicking on the specific VM.
5. Under **Select Endpoint protection**, select the endpoint protection solution you want to use. In this example, select **Microsoft Antimalware**.
6. Additional information about the endpoint protection solution is displayed. Select **Create**.

Install antimalware on non-Azure computers

1. Go back to **Endpoint protection issues** and select **Endpoint protection not installed on non-Azure computers**.

2. Under **Endpoint protection not installed on non-Azure computers**, select a workspace. An Azure Monitor logs search query filtered to the workspace opens and lists computers missing antimalware. Select a computer from the list for more information.

Another search result opens with information filtered only for that computer.

The screenshot shows the Azure Security Center Log Search interface. A search query is displayed at the top: "ProtectionStatus | where (ComputerEnvironment != "Azure" or isEmpty(ResourceId)) and (TypeofProtection == "Malicious Software Removal Tool" or TypeofProtection == "No Anti-Malware Tool was detected") | where Computer == "WIN-SERVER-2016"". The results section shows 2 items found. The first item is a log entry from 9/11/2017 at 9:28:12.613 PM, detailing a protection status check for a specific computer. The second item is another log entry from 9/11/2017 at 10:28:12.610 PM, also for the same computer, indicating no anti-malware tool was detected.

NOTE

We recommend that endpoint protection be provisioned for all VMs and computers to help identify and remove viruses, spyware, and other malicious software.

Next steps

This article showed you how to implement the Security Center recommendation "Install Endpoint Protection." To learn more about enabling Microsoft Antimalware in Azure, see the following document:

- [Microsoft Antimalware for Cloud Services and Virtual Machines](#) -- Learn how to deploy Microsoft Antimalware.

To learn more about Security Center, see the following documents:

- [Setting security policies in Azure Security Center](#) -- Learn how to configure security policies.
- [Managing security recommendations in Azure Security Center](#) -- Learn how recommendations help you protect your Azure resources.
- [Security health monitoring in Azure Security Center](#) -- Learn how to monitor the health of your Azure resources.
- [Managing and responding to security alerts in Azure Security Center](#) -- Learn how to manage and respond to security alerts.
- [Monitoring partner solutions with Azure Security Center](#) -- Learn how to monitor the health status of your partner solutions.

Azure Security Center Threat Intelligence Report

2/27/2020 • 2 minutes to read • [Edit Online](#)

This document explains how Azure Security Center Threat Intelligent Reports can help you learn more about a threat that generated a security alert.

What is a threat intelligence report?

Security Center threat protection works by monitoring security information from your Azure resources, the network, and connected partner solutions. It analyzes this information, often correlating information from multiple sources, to identify threats. For more information, see [How Azure Security Center detects and responds to threats](#).

When Security Center identifies a threat, it will trigger a [security alert](#), which contains detailed information regarding a particular event, including suggestions for remediation. To assist incident response teams, investigate and remediate threats, Security Center includes a threat intelligence report that contains information about the threat that was detected, including information such as the:

- Attacker's identity or associations (if this information is available)
- Attackers' objectives
- Current and historical attack campaigns (if this information is available)
- Attackers' tactics, tools, and procedures
- Associated indicators of compromise (IoC) such as URLs and file hashes
- Victimology, which is the industry and geographic prevalence to assist you in determining if your Azure resources are at risk
- Mitigation and remediation information

NOTE

The amount of information in any particular report will vary; the level of detail is based on the malware's activity and prevalence.

Security Center has three types of threat reports, which can vary according to the attack. The reports available are:

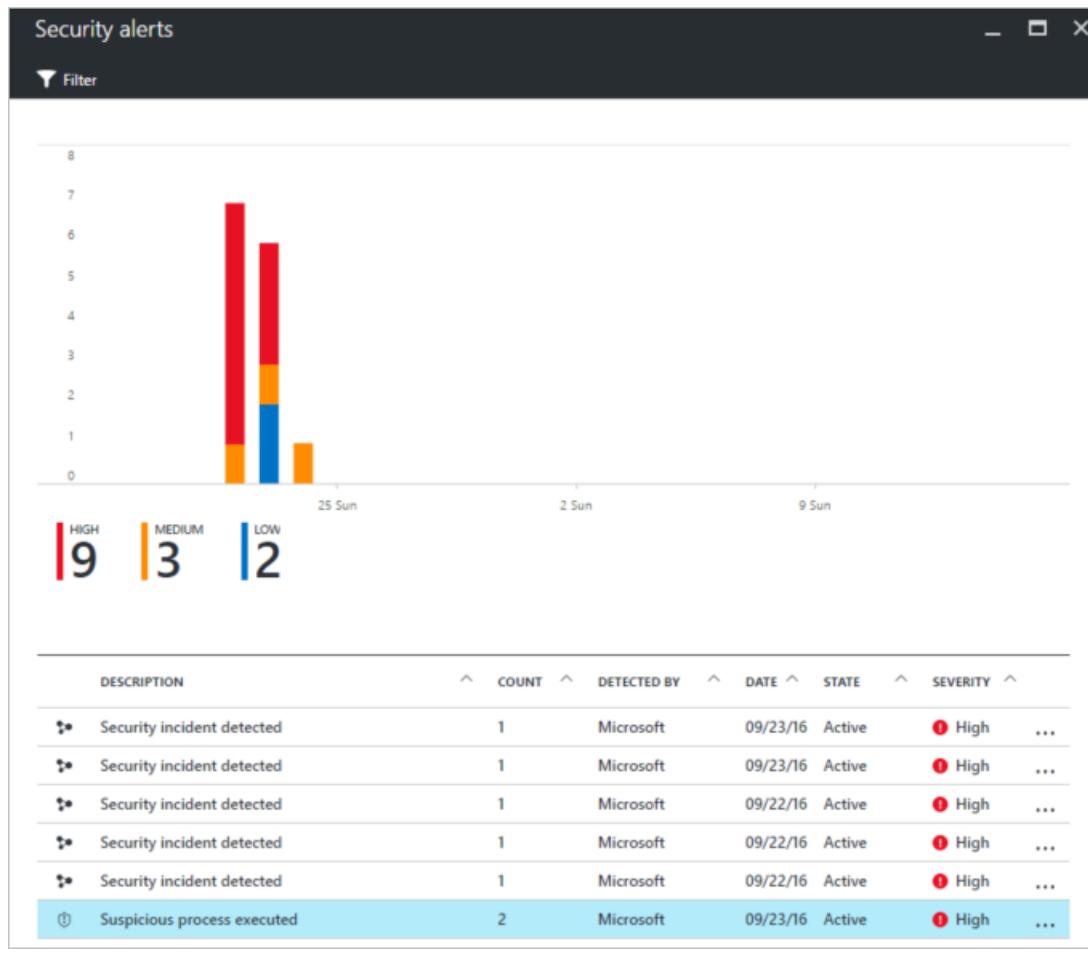
- **Activity Group Report:** provides deep dives into attackers, their objectives and tactics.
- **Campaign Report:** focuses on details of specific attack campaigns.
- **Threat Summary Report:** covers all of the items in the previous two reports.

This type of information is useful during the incident response process, where there is an ongoing investigation to understand the source of the attack, the attacker's motivations, and what to do to mitigate this issue moving forward.

How to access the threat intelligence report?

You can review your current alerts by looking at the **Security alerts** tile. Open the Azure portal and follow the steps below to see more details about each alert:

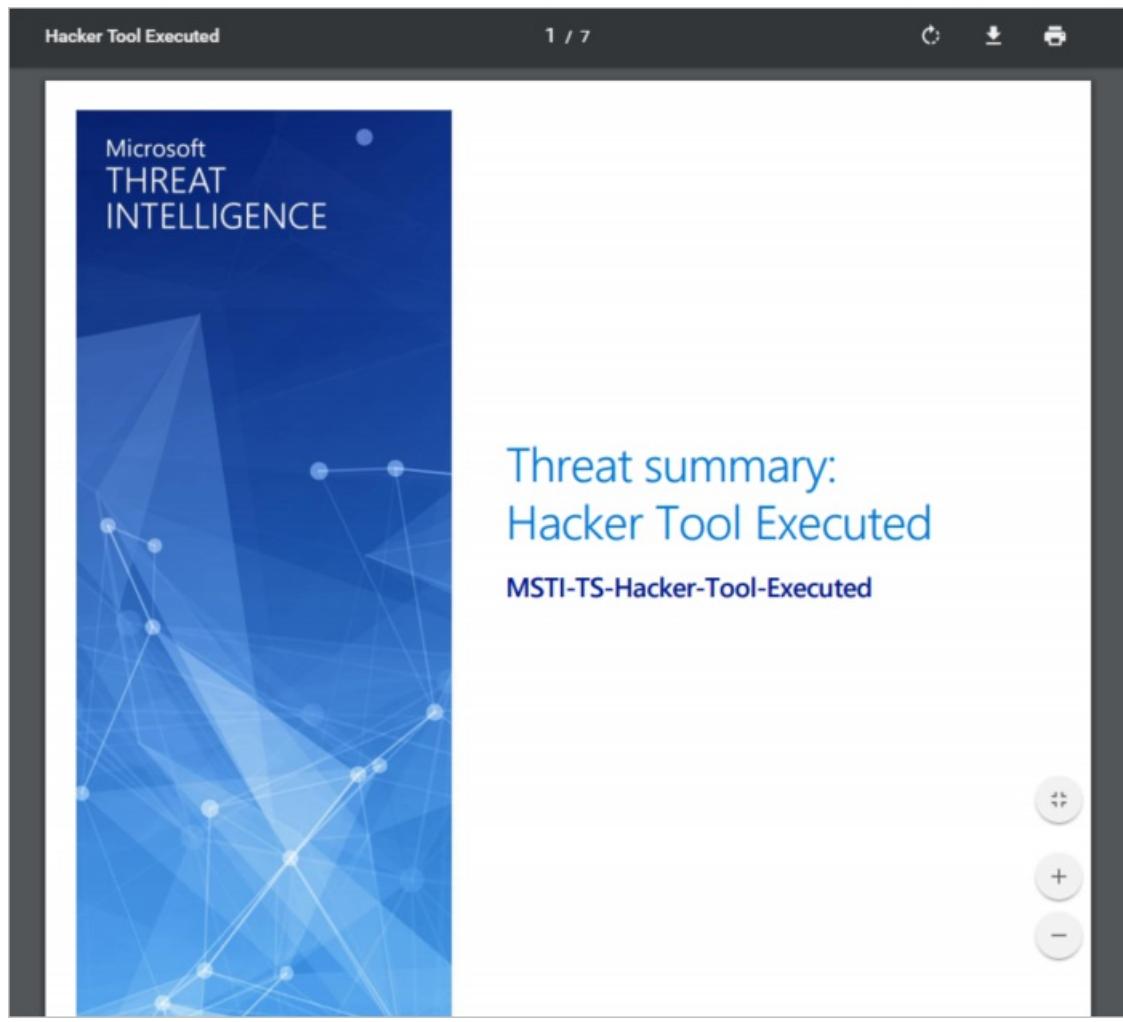
1. On the Security Center dashboard, you will see the **Security alerts** tile.
2. Click the tile to open the **Security alerts** blade that contains more details about the alerts and click in the security alert that you want to obtain more information about.



3. In this case, the **Suspicious process executed** blade shows the details about the alert as shown in the figure below:

| Suspicious process executed | |
|-----------------------------|--|
| IgniteOMS | |
| DESCRIPTION | Machine logs indicate that the suspicious Process: 'C:\Temp\mimikatz.exe' was running with the command line: '"C:\Temp\mimikatz.exe"' |
| DETECTION TIME | Friday, September 23, 2016, 2:56:22 PM |
| SEVERITY | ! High |
| STATE | Active |
| ATTACKED RESOURCE | IgniteOMS |
| SUBSCRIPTION | [REDACTED] |
| DETECTED BY |  Microsoft |
| ACTION TAKEN | Detected |
| DOMAIN NAME | IGNITEOMS |
| USER NAME | yuri |
| PARENT PROCESS | - |
| PROCESS ID | 0xc1c |
| USER SID | S-1-5-21-1997640134-403717899-730413893-500 |
| REPORTS | Report: Hacker tool executed |
| REMEDIATION STEPS | <p>1. Run Process Explorer and try to identify unknown running processes (see https://technet.microsoft.com/en-us/sysinternals/bb896653.aspx)</p> <p>2. Escalate the alert to the information security team</p> <p>3. Make sure the machine is completely updated and has an updated anti-malware application installed</p> <p>4. Run a full anti-malware scan and verify that the threat was removed</p> <p>5. Install and run Microsoft's Malicious Software Removal Tool (see https://www.microsoft.com/en-us/download/malicious-software-removal-tool-details.aspx)</p> <p>6. Run Microsoft's Autoruns utility and try to identify unknown applications that are configured to run at login (see https://technet.microsoft.com/en-us/sysinternals/bb897441.aspx)</p> |

4. The amount of information available for each security alert will vary according to the type of alert. In the **REPORTS** field, you have a link to the threat intelligence report. Click on it and another browser window will appear with PDF file.



From here you can download the PDF for this report and read more about the security issue that was detected and take actions based on the information provided.

See also

In this document, you learned how Azure Security Center Threat Intelligent Reports can help during an investigation about security alerts. To learn more about Azure Security Center, see the following:

- [Azure Security Center planning and operations guide](#). Learn how to plan and understand the design considerations to adopt Azure Security Center.
- [Managing and responding to security alerts in Azure Security Center](#). Learn how to manage and respond to security alerts.
- [Handling Security Incident in Azure Security Center](#)

Alert confidence score (Preview)

2/25/2020 • 2 minutes to read • [Edit Online](#)

Azure Security Center provides you with visibility across the resources you run in Azure, and alerts you when it detects potential issues. The volume of alerts can be challenging for a security operations team to individually address, and it becomes necessary to prioritize which alerts to investigate. Investigating alerts can be complex and time consuming, and as a result, some alerts are ignored.

The confidence score (currently in preview) in Security Center can help your team triage and prioritize alerts. Security Center automatically applies industry best practices, intelligent algorithms, and processes used by analysts to determine whether a threat is legitimate and provides you with meaningful insights in the form of a confidence score.

How the confidence score is triggered

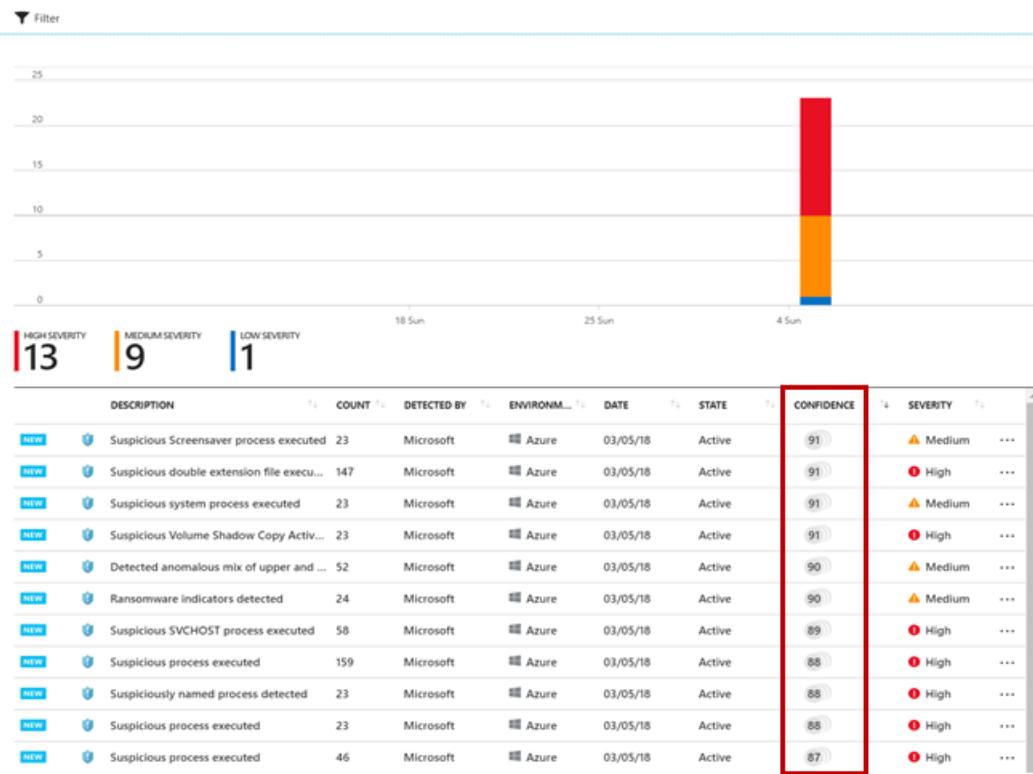
Alerts are generated when suspicious processes are detected running on your virtual machines. Security Center reviews and analyzes these alerts on Windows virtual machines running in Azure. It performs automated checks and correlations using advanced algorithms across multiple entities and data sources across the organization, and all your Azure resources, and presents with a confidence score which is a measure of how confident Security Center is that the alert is genuine and needs to be investigated.

Understanding the confidence score

The confidence score ranges between 1 and 100 and represents the confidence Security Center has that the alert needs to be investigated. The higher the score is, the more confident Security Center is that the alert indicates genuine malicious activity. The confidence score includes a list of the top reasons why the alert received its confidence score. The confidence score makes it easier for security analysts to prioritize their response to alerts and address the most pressing attacks first, ultimately reducing the amount of time it takes to respond to attacks and breaches.

To view the confidence score:

- In the Security Center portal, open the Security alerts blade.
- The alerts and incidents are organized from highest to lowest, meaning the more confident Security Center is that an alert represents a threat, the closer it is to the top of the page.



To view the data that contributed to Security Center's confidence in an alert:

- In the Security alert blade, under **Confidence**, view the observations that contributed to the confidence score and gain insights related to the alert. This provides you with more insight into the nature of the activities that caused the alert.

Suspicious Screensaver process executed admin-AGENT-2

 Learn more

| | |
|-------------------|---|
| RESOURCE TYPE |  Virtual Machine |
| ACCOUNT LOGON ID | 1234567a |
| COMMAND LINE | c:\user\temp\scrsave.scr |
| DOMAIN NAME | contoso |
| PARENT PROCESS | unknown |
| PARENT PROCESS ID | 8636 |
| PROCESS ID | 4824 |
| USER NAME | admin-AGENT-2 |
| USER SID | 1-2-3-4-5-6-7-8-9 |
| REPORTS | Report: Suspicious Screen Saver Execution |

Confidence

91

This alert confidence score is based on the following observations:

-  Suspicious process execution path for this subscription
-  admin-AGENT-2 generated multiple security alerts
-  admin-AGENT-2 appeared in multiple alerts

Use Security Center's confidence score to prioritize alert triage in your environment. The confidence score saves you time and effort by automatically investigating alerts, applying industry best practices and intelligent algorithms, and acting as a virtual analyst to determine which threats are real and where you need to focus your attention.

Investigate Incidents and Alerts in Azure Security Center (Retired)

2/25/2020 • 5 minutes to read • [Edit Online](#)

This document helps you use the investigation feature (Preview) in Azure Security Center to investigate security incidents and alerts.

NOTE

The alerts and incidents investigation (Preview) experience has been retired on July 31st, 2019. For more information and alternative services, see [Retirement of Security Center features \(July 2019\)](#).

What is investigation in Security Center?

The Investigation feature in Security Center allows you to triage, understand the scope, and track down the root cause of a potential [security incident](#).

The intent is to facilitate the investigation process by linking all entities ([security alerts](#), users, computers and incidents) that are involved with the incident you are investigating. Security Center can do this by correlating relevant data with any involved entities and exposing this correlation in using a live graph that helps you navigate through the objects and visualize relevant information.

NOTE

- [Custom alerts](#) are not supported in Security Center's investigation feature.
- Investigation is only supported for alerts based on data collected from Windows servers.

How Investigation works?

The Investigation is composed by a graph that occupies the central area of the investigation dashboard. The graph is always focused on a specific entity, and presents the entities that are related to it. An entity could be a security alert, user, computer or incident.



The user can navigate from one entity to another by clicking on it in the graph. The graph automatically centralizes on the selected entity and its related entities. Entities that are not relevant anymore may be removed from the graph.

Investigation path

While the user is navigating to different entities the investigation path helps to keep track of the investigation context and allows quick navigation. The incident that contains the investigation results is always in the left-most incident in the investigation path.



General information

When an entity is presented in the graph, the tabs show additional information on this entity. The **Info** tab presents general information on the entity from various available information sources.

Successful RDP brute force attack

Related TO INCIDENT **PRIORITY High** **InternalTestProvider DETECTED BY**

Alert details

DESCRIPTION
Several Remote Desktop login attempts were detected from FreeRDP (96.81.218.10), some of which were able to successfully login to the machine. Event logs analysis shows that in the last 30 minutes there were 60 failed attempts. 20 of the failed login attempts aimed at non-existent users. 1 of the failed login attempts aimed at existing users.

ALERT ID
2518965585638226038_2ea73417-247a-4080-b640-8a792a27fea8

TIME GENERATED
9/18/2017 8:58:56.000 AM

SOURCE
FreeRDP (96.81.218.10)

SUCCESSFUL LOGINS
1

ATTACK DURATION
30 minutes

FAILED ATTEMPTS
60

NON-EXISTENT USERS
20

EXISTING USERS
1

REPORTS
[Report: RDP Brute Forcing](#)

SEVERITY
High

REPORTINGSYSTEM
Azure

- Info**
- Entities**
- Search**
- Exploration**
- Playbooks**
- Comments**
- Audit**

The info tab shows information relevant to the incident selected in the map. Incident is a container that includes the results of an investigation. Every investigation happens in the context of an incident.

An incident is only created when a user clicks on the **Start investigation** button for a specific alert. The basic capability available for the investigator is to mark entities such as user, computer or alert. When an entity is marked as related, a reason is provided. From this point onward, this entity appears directly under the incident in the graph and in the incident entities list.

Entities

The **Entities** tab shows all the related entities grouped by type. It is useful in two cases: when there are too many entities to present in the graph and when the entities names are too long, and it is easier to examine them in a tabular way.



Successful RDP brute force attack

Incidents 1

TITLE

Security incident detected

Computers 1

NAME

ContosoWebFE1

Users 1

NAME

Author

>

- i Info
- cube Entities
- magnifying glass Search
- binoculars Exploration
- user group Playbooks

Search

The **Search** tab presents all the log types that are available for the entity. For each log type, you can see how many records are available. Clicking on each log type takes you to the search screen. In the search screen, you can refine your search and use the various search features such as setting alerts. In the current release, the search tab is available only for users and computers entities.



ContosoWebFE1

You have the following logs on computer 'ContosoWebFE1':

| NAME | COUNT |
|-------------------------|-------|
| SecurityEvent | 3.4K |
| Heartbeat | 1.8K |
| Update | 745 |
| SecurityBaseline | 262 |
| Usage | 104 |
| ProtectionStatus | 31 |
| SecurityDetection | 7 |
| UpdateSummary | 5 |
| SecurityBaselineSummary | 2 |

>

- i Info
- cube Entities
- magnifying glass Search
- binoculars Exploration
- user group Playbooks

Exploration

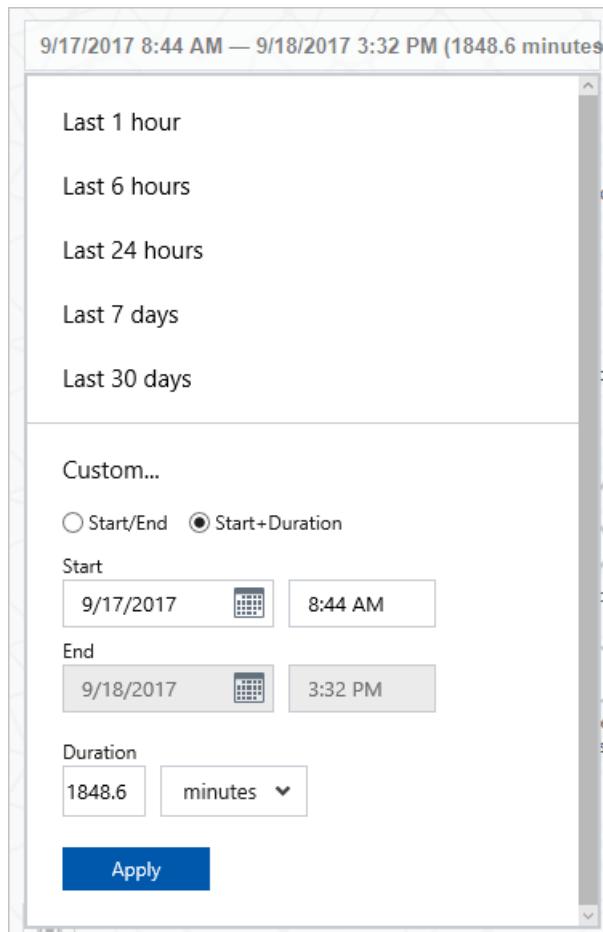
The **Exploration** tab allows the investigator to examine data related to various issues related to the entity. For example, when a machine is investigated, the list of processes executed on it is presented in the exploration tab. In some cases, the exploration tab presents data that might indicate a suspicious issue. The investigator can examine the data within the tab or open it in the search screen to examine large sets of data and to use advanced search options such as filtering and export to Excel.

The screenshot shows the Microsoft Security Graph interface. At the top left is a computer monitor icon and the text "ContosoWebFE1". To the right is a navigation bar with four items: "Info" (highlighted), "Entities", "Search", and "Exploration". The main area displays a list of issues for the computer "ContosoWebFE1".

| Issue Description | Count | Action |
|--|-------|--|
| > ⚠ Accounts that added members to security-enabled gro... | 2 | 🔍 |
| > ℹ Distinct processes executed on the machine | 70 | 🔍 |
| > ℹ Number of accounts logged on to the machine | 9 | 🔍 |

Timeline

Most of the data that is presented in the graph and the various tabs is relevant for a specific time period. This time scope is set using the time scope selector on the top left side of the graph. The investigator has various methods to select the time scope.



The following items are sensitive to the time scope:

- User-computer relationship in the graph, only users that logged in to the computer within this time scope are presented.
- Which alerts are presented when you examine computers and users: only alerts that occur within the time scope are presented.
- The entities tab follow the same logic as the graph.

The following items are going to be presented regardless of the selected time scope:

- When an alert is presented, all the entities that are contained in it, such as users and computers, are always presented.
- If an incident contains an entity, it is going to be presented.

NOTE

The **Search** and **Exploration** tab only show records within this time scope.

How to perform an investigation?

You can start your investigation from a security incident, or from an alert, the option that you choose will vary according to your needs. The steps that follows are used to start an investigation from an alert:

1. Open **Security Center** dashboard.
2. Click on **Security Alerts**, and select the incident that you want to investigate.
3. In the incident's page, click on the **Start Investigation** button, and the **Investigation** dashboard appears.

This screenshot shows the 'Suspicious SVCHOST process executed' investigation dashboard. At the top, there are two buttons: 'Start investigation' and 'Run playbooks'. Below this, the 'DESCRIPTION' section states: 'The system process SVCHOST was observed running in an abnormal context. Malware often use SVCHOST to masquerade its malicious activity.' The 'DETECTION TIME' is listed as 'Tuesday, September 12, 2017 6:15:18 AM'. The 'SEVERITY' is marked as 'High'. The 'STATE' is 'Dismissed'. The 'ATTACKED RESOURCE' is highlighted with a blue border and labeled 'CONTOSOWEBF1'.

4. From this dashboard you can select the entity in the map, and the relevant information about this entity appears on the right side of the screen.

This screenshot shows the 'Investigation Dashboard (Preview)' with the URL 'defaultworkspace=d4272367-5645-4cde-9c67-3b74b59a6982-eus'. On the left, the 'Investigation path' shows a network of entities: 'Investigation' -> 'Suspicious SVCHOST process ...'. On the right, the 'Suspicious SVCHOST process executed' details are shown. It includes a 'Related TO INCIDENT' dropdown, a 'PRIORITY' indicator (High), and an 'ASC DETECTED BY' icon. The 'Alert details' section provides a detailed description of the incident, including the detection time ('9/11/2017 6:17 AM — 9/14/2017 4:29 PM (4931.3 minutes)'), alert ID ('2518970858816206281_984058c2-b9b2-4254-9842-8377ca8df5ff'), and time generated ('9/12/2017 6:15:36.000 AM'). It also lists additional related entities, domain name ('CONTOSO'), process name ('c:\users\contoso\administrator\svchost.exe'), command line ('c:\users\contoso\administrator\svchost.exe'), parent process ('unknown'), process ID ('4484'), and account logon ID ('0x31436a').

From this point you can explore the entities that were involved in this incident, and explore more details about each one of them.

See also

In this document, you learned how to use the investigation feature in Security Center. To learn more about Security Center, see the following:

- [Managing and responding to security alerts in Azure Security Center](#). Learn how to manage alerts, and respond to security incidents in Security Center.
- [Security health monitoring in Azure Security Center](#). Learn how to monitor the health of your Azure resources.
- [Understanding security alerts in Azure Security Center](#). Learn about the different types of security alerts.

Manage user data found in an Azure Security Center investigation

1/14/2020 • 2 minutes to read • [Edit Online](#)

This article provides information on how to manage the user data found in Azure Security Center's investigation feature. Investigation data is stored in [Azure Monitor logs](#) and exposed in Security Center. Managing user data includes the ability to delete or export data.

NOTE

This article provides steps for how to delete personal data from the device or service and can be used to support your obligations under the GDPR. If you're looking for general info about GDPR, see the [GDPR section of the Service Trust portal](#).

Searching for and identifying personal data

In the Azure portal, you can use Security Center's [investigation feature](#) to search for personal data. The investigation feature is available under **Security Alerts**.

The investigation feature shows all entities, user information, and data under the **Entities** tab.

Securing and controlling access to personal information

A Security Center user assigned the role of Reader, Owner, Contributor, or Account Administrator can access customer data within the tool.

See [Built-in roles for Azure role-based access control](#) to learn more about the Reader, Owner, and Contributor roles. See [Azure subscription administrators](#) to learn more about the Account Administrator role.

Deleting personal data

A Security Center user assigned the role of Owner, Contributor, or Account Administrator can delete the investigation information.

To delete an investigation, you can submit a `DELETE` request to the Azure Resource Manager REST API:

```
DELETE  
https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.OperationalInsights/workspaces/{workspaceName}/features/security/incidents/{incidentName}
```

The `incidentName` input can be found by listing all incidents using a `GET` request:

```
GET  
https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.OperationalInsights/workspaces/{workspaceName}/features/security/incidents
```

Exporting personal data

A Security Center user assigned the role of Owner, Contributor, or Account Administrator can export the investigation information. To export investigation information, go to the **Entities** tab to copy and paste the relevant

information.

Next steps

For more information about managing user data, see [Manage user data in Azure Security Center](#). To learn more about deleting private data in Azure Monitor logs, see [How to export and delete private data](#).

Azure Security Center planning and operations guide

2/27/2020 • 13 minutes to read • [Edit Online](#)

This guide is for information technology (IT) professionals, IT architects, information security analysts, and cloud administrators planning to use Azure Security Center.

Planning guide

This guide covers tasks that you can follow to optimize your use of Security Center based on your organization's security requirements and cloud management model. To take full advantage of Security Center, it is important to understand how different individuals or teams in your organization use the service to meet secure development and operations, monitoring, governance, and incident response needs. The key areas to consider when planning to use Security Center are:

- Security Roles and Access Controls
- Security Policies and Recommendations
- Data Collection and Storage
- Ongoing non-Azure resources
- Ongoing Security Monitoring
- Incident Response

In the next section, you will learn how to plan for each one of those areas and apply those recommendations based on your requirements.

NOTE

Read [Azure Security Center frequently asked questions \(FAQ\)](#) for a list of common questions that can also be useful during the designing and planning phase.

Security roles and access controls

Depending on the size and structure of your organization, multiple individuals and teams may use Security Center to perform different security-related tasks. In the following diagram, you have an example of fictitious personas and their respective roles and security responsibilities:

| | |
|--|---|
|  <p>Jeff Cloud Workload Owner</p> <p>Manages a cloud workload and its related resources (often in a DevOps role)</p> <p>Responsible for implementing and maintaining protections in accordance with the company security policy</p> <p>In small orgs, also defines policy and monitor alerts</p> |  <p>Ellen CISO/CIO</p> <p>Responsible for all aspects of security for the company</p> <p>Wants to understand the company's security posture across cloud workloads</p> <p>Needs to be informed of major attacks and risks</p> |
|  <p>David IT Security</p> <p>Sets company security policies to ensure the appropriate protections are in place</p> <p>Monitors compliance with policies</p> <p>Generates reports for leadership or auditors</p> |  <p>Judy Security Ops</p> <p>Monitors and responds to security alerts 24/7</p> <p>Escalates to Cloud Workload Owner or IT Security Analyst</p> <p>Sometimes performed by a Managed Security Provider</p> |
|  <p>Sam Security Analyst</p> <p>Investigates attacks</p> <p>Work with Cloud Workload Owner to apply remediation</p> | |

Security Center enables these individuals to meet these various responsibilities. For example:

Jeff (Workload Owner)

- Manage a cloud workload and its related resources
- Responsible for implementing and maintaining protections in accordance with company security policy

Ellen (CISO/CIO)

- Responsible for all aspects of security for the company
- Wants to understand the company's security posture across cloud workloads
- Needs to be informed of major attacks and risks

David (IT Security)

- Sets company security policies to ensure the appropriate protections are in place
- Monitors compliance with policies
- Generates reports for leadership or auditors

Judy (Security Operations)

- Monitors and responds to security alerts 24/7
- Escalates to Cloud Workload Owner or IT Security Analyst

Sam (Security Analyst)

- Investigate attacks
- Work with Cloud Workload Owner to apply remediation

Security Center uses [Role-Based Access Control \(RBAC\)](#), which provides [built-in roles](#) that can be assigned to users, groups, and services in Azure. When a user opens Security Center, they only see information related to resources they have access to. Which means the user is assigned the role of Owner, Contributor, or Reader to the subscription or resource group that a resource belongs to. In addition to these roles, there are two specific Security Center roles:

- **Security reader:** a user that belongs to this role is able to view only Security Center configurations, which include recommendations, alerts, policy, and health, but it won't be able to make changes.
- **Security admin:** same as security reader but it can also update the security policy, dismiss recommendations and alerts.

The Security Center roles described above do not have access to other service areas of Azure such as Storage, Web & Mobile, or Internet of Things.

Using the personas explained in the previous diagram, the following RBAC would be needed:

Jeff (Workload Owner)

- Resource Group Owner/Contributor

Ellen (CISO/CIO)

- Subscription Owner/Contributor or Security Admin

David (IT Security)

- Subscription Owner/Contributor or Security Admin

Judy (Security Operations)

- Subscription Reader or Security Reader to view Alerts
- Subscription Owner/Contributor or Security Admin required to dismiss Alerts

Sam (Security Analyst)

- Subscription Reader to view Alerts
- Subscription Owner/Contributor required to dismiss Alerts
- Access to the workspace may be required

Some other important information to consider:

- Only subscription Owners/Contributors and Security Admins can edit a security policy.
- Only subscription and resource group Owners and Contributors can apply security recommendations for a resource.

When planning access control using RBAC for Security Center, be sure to understand who in your organization will be using Security Center. Also, what types of tasks they will be performing and then configure RBAC accordingly.

NOTE

We recommend that you assign the least permissive role needed for users to complete their tasks. For example, users who only need to view information about the security state of resources but not take action, such as applying recommendations or editing policies, should be assigned the Reader role.

Security policies and recommendations

A security policy defines the desired configuration of your workloads and helps ensure compliance with company or regulatory security requirements. In Security Center, you can define policies for your Azure subscriptions, which can be tailored to the type of workload or the sensitivity of data.

Security Center policies contain the following components:

- **Data collection:** agent provisioning and data collection settings.
- **Security policy:** an [Azure Policy](#) that determines which controls are monitored and recommended by Security Center, or use Azure Policy to create new definitions, define additional policies, and assign policies across management groups.
- **Email notifications:** security contacts and notification settings.

- **Pricing tier:** free or standard pricing selection, which determine which Security Center features are available for resources in scope (can be specified for subscriptions, resource groups and workspaces).

NOTE

Specifying a security contact will ensure that Azure can reach the right person in your organization if a security incident occurs. Read [Provide security contact details in Azure Security Center](#) for more information on how to enable this recommendation.

Security policies definitions and recommendations

Security Center automatically creates a default security policy for each of your Azure subscriptions. You can edit the policy in Security Center or use Azure Policy to create new definitions, define additional policies, and assign policies across Management Groups (which can represent the entire organization, a business unit in it etc.), and monitor compliance to these policies across these scopes.

Before configuring security policies, review each of the [security recommendations](#), and determine whether these policies are appropriate for your various subscriptions and resource groups. It is also important to understand what action should be taken to address Security Recommendations and who in your organization will be responsible for monitoring for new recommendations and taking the needed steps.

Data collection and storage

Azure Security Center uses the Microsoft Monitoring Agent – this is the same agent used by the Azure Monitor service – to collect security data from your virtual machines. [Data collected](#) from this agent will be stored in your Log Analytics workspace(s).

Agent

When automatic provisioning is enabled in the security policy, the Microsoft Monitoring Agent (for [Windows](#) or [Linux](#)) is installed on all supported Azure VMs, and any new ones that are created. If the VM or computer already has the Microsoft Monitoring Agent installed, Azure Security Center will leverage the current installed agent. The agent's process is designed to be non-invasive and have very minimal impact on VM performance.

The Microsoft Monitoring Agent for Windows requires use TCP port 443. See the [Troubleshooting article](#) for additional details.

If at some point you want to disable Data Collection, you can turn it off in the security policy. However, because the Microsoft Monitoring Agent may be used by other Azure management and monitoring services, the agent will not be uninstalled automatically when you turn off data collection in Security Center. You can manually uninstall the agent if needed.

NOTE

To find a list of supported VMs, read the [Azure Security Center frequently asked questions \(FAQ\)](#).

Workspace

A workspace is an Azure resource that serves as a container for data. You or other members of your organization might use multiple workspaces to manage different sets of data that is collected from all or portions of your IT infrastructure.

Data collected from the Microsoft Monitoring Agent (on behalf of Azure Security Center) will be stored in either an existing Log Analytics workspace(s) associated with your Azure subscription or a new workspace(s), taking into account the Geo of the VM.

In the Azure portal, you can browse to see a list of your Log Analytics workspaces, including any created by

Azure Security Center. A related resource group will be created for new workspaces. Both will follow this naming convention:

- Workspace: *DefaultWorkspace-[subscription-ID]-[geo]*
- Resource Group: *DefaultResourceGroup-[geo]*

For workspaces created by Azure Security Center, data is retained for 30 days. For existing workspaces, retention is based on the workspace pricing tier. If you want, you can also use an existing workspace.

NOTE

Microsoft makes strong commitment to protect the privacy and security of this data. Microsoft adheres to strict compliance and security guidelines—from coding to operating a service. For more information about data handling and privacy, read [Azure Security Center Data Security](#).

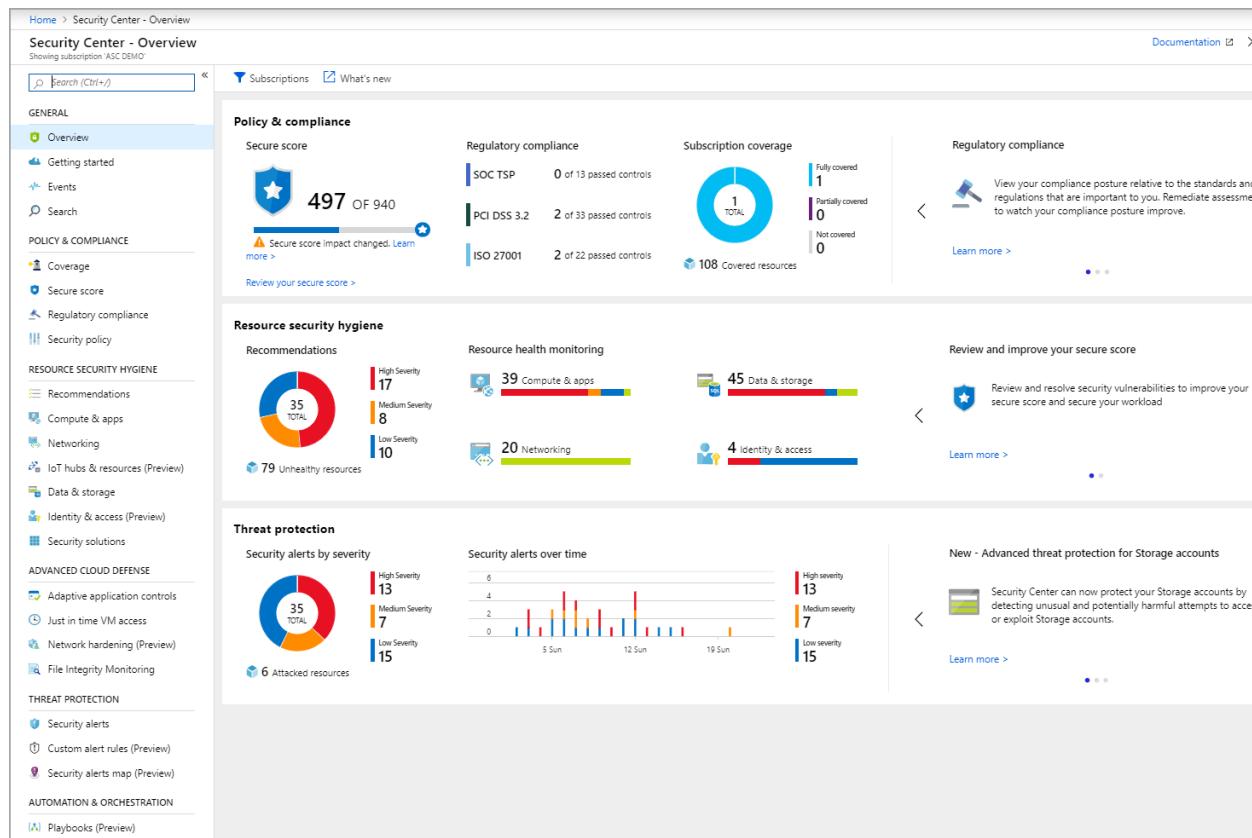
Onboarding non-Azure resources

Security Center can monitor the security posture of your non-Azure computers but you need to first onboard these resources. Read [Onboarding to Azure Security Center Standard for enhanced security](#) for more information on how to onboard non-Azure resources.

Ongoing security monitoring

After initial configuration and application of Security Center recommendations, the next step is considering Security Center operational processes.

The Security Center Overview provides a unified view of security across all your Azure resources and any non-Azure resources you have connected. The example below shows an environment with many issues to be addressed:



NOTE

Security Center will not interfere with your normal operational procedures, it will passively monitor your deployments and provide recommendations based on the security policies you enabled.

When you first opt in to use Security Center for your current Azure environment, make sure that you review all recommendations, which can be done in the **Recommendations** tile or per resource (**Compute**, **Networking**, **Storage & data**, **Application**).

Once you address all recommendations, the **Prevention** section should be green for all resources that were addressed. Ongoing monitoring at this point becomes easier since you will only take actions based on changes in the resource security health and recommendations tiles.

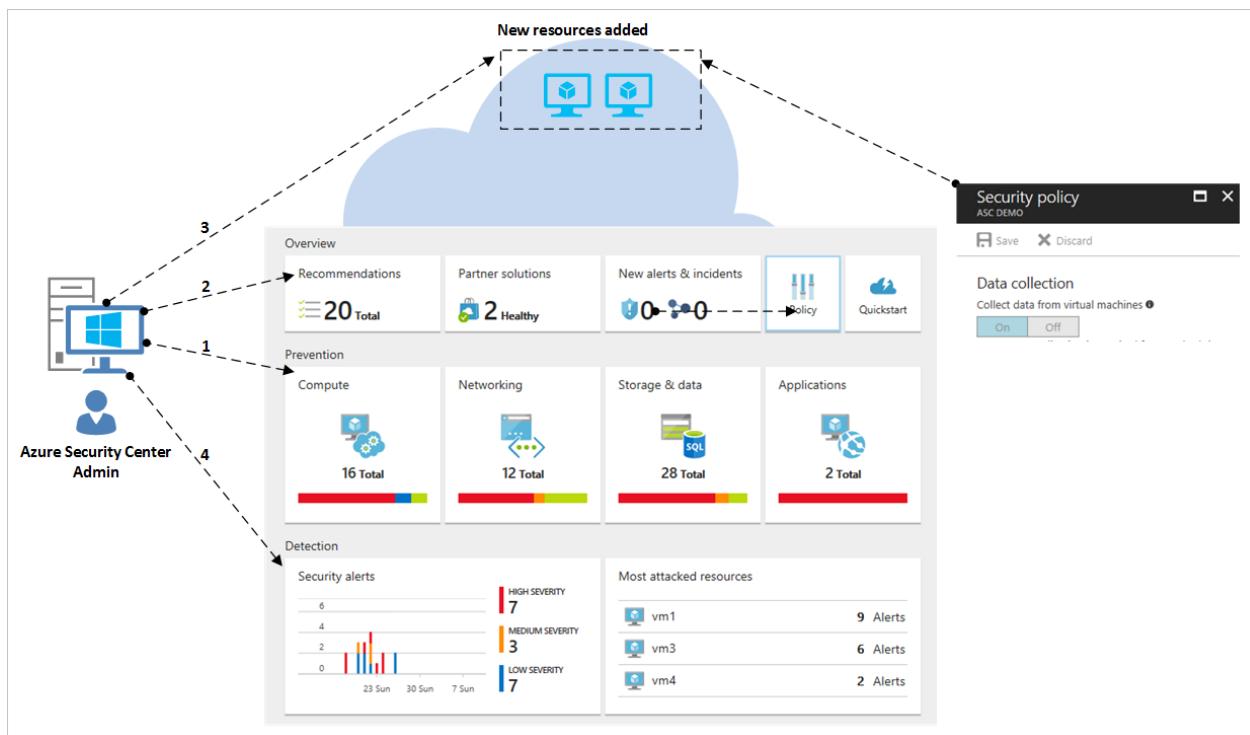
The **Detection** section is more reactive, these are alerts regarding issues that are either taking place now, or occurred in the past and were detected by Security Center controls and 3rd party systems. The Security Alerts tile will show bar graphs that represent the number of alerts that were found in each day, and their distribution among the different severity categories (low, medium, high). For more information about Security Alerts, read [Managing and responding to security alerts in Azure Security Center](#).

Plan to visit the [threat intelligence](#) option as part of your daily security operations. There you can identify security threats against the environment, such as identify if a particular computer is part of a botnet.

Monitoring for new or changed resources

Most Azure environments are dynamic, with resources regularly being created, spun up or down, reconfigured, and changed. Security Center helps ensure that you have visibility into the security state of these new resources.

When you add new resources (VMs, SQL DBs) to your Azure Environment, Security Center will automatically discover these resources and begin to monitor their security. This also includes PaaS web roles and worker roles. If Data Collection is enabled in the [Security Policy](#), additional monitoring capabilities will be enabled automatically for your virtual machines.

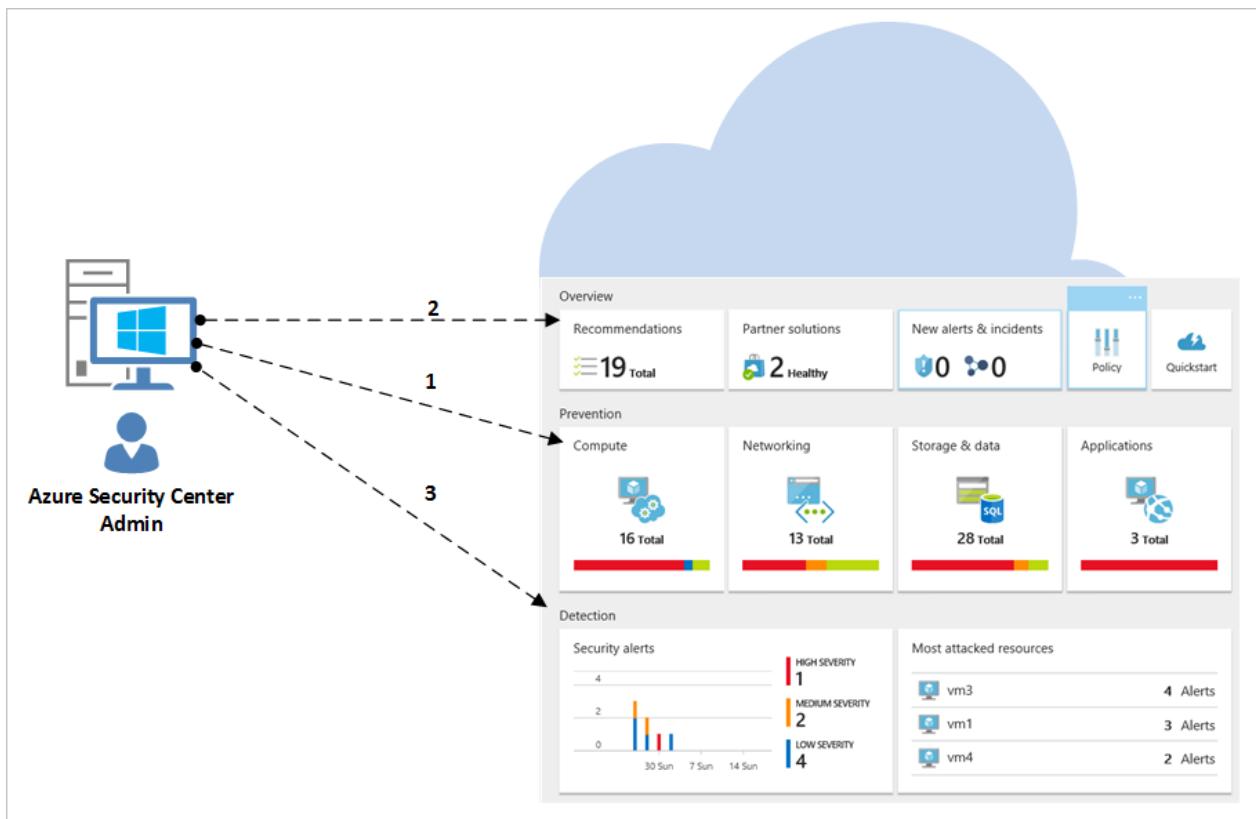


1. For virtual machines, click **Compute & apps**, under the **Resource Security Hygiene** section. Any issues with enabling data or related recommendations will be surfaced in the **Overview** tab, and **Monitoring Recommendations** section.
2. View the **Recommendations** to see what, if any, security risks were identified for the new resource.

3. It is very common that when new VMs are added to your environment, only the operating system is initially installed. The resource owner might need some time to deploy other apps that will be used by these VMs. Ideally, you should know the final intent of this workload. Is it going to be an Application Server? Based on what this new workload is going to be, you can enable the appropriate **Security Policy**, which is the third step in this workflow.

4. As new resources are added to your Azure environment, new alerts may appear in the **Security Alerts** tile. Look for new alerts in this tile and follow the recommendations.

You should also regularly monitor existing resources for configuration changes that could have created security risks, drift from recommended baselines, and security alerts. Start at the Security Center dashboard. From there, you have three major areas to review on a consistent basis.



1. The **Prevention** section panel provides you quick access to your key resources. Use this option to monitor Compute, Networking, Storage & data and Applications.
2. The **Recommendations** panel enables you to review Security Center recommendations. During your ongoing monitoring, you may find that you don't have recommendations on a daily basis, which is normal since you addressed all recommendations on the initial Security Center setup. For this reason, you may not have new information in this section every day and will just need to access it as needed.
3. The **Detection** section might change on either a very frequent or very infrequent basis. Always review your security alerts and take actions based on Security Center recommendations.

Hardening access and applications

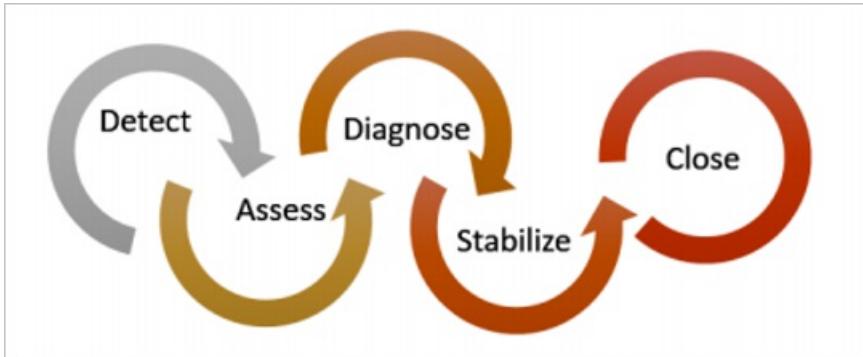
As part of your security operations, you should also adopt preventative measures to restrict access to VMs, and control the applications that are running on VMs. By locking down inbound traffic to your Azure VMs, you are reducing the exposure to attacks, and at the same time providing easy access to connect to VMs when needed. Use [just-in-time VM](#) access feature to hardening access to your VMs.

You can use [Adaptive Application Controls](#) to limit which applications can run on your VMs located in Azure. Among other benefits, this helps harden your VMs against malware. Using machine learning, Security Center analyzes processes running in the VM to help you create whitelisting rules.

Incident response

Security Center detects and alerts you to threats as they occur. Organizations should monitor for new security alerts and take action as needed to investigate further or remediate the attack. For more information on how Security Center threat protection works, read [How Azure Security Center detects and responds to threats](#).

While this article doesn't have the intent to assist you creating your own Incident Response plan, we are going to use Microsoft Azure Security Response in the Cloud lifecycle as the foundation for incident response stages. The stages are shown in the following diagram:



NOTE

You can use the National Institute of Standards and Technology (NIST) [Computer Security Incident Handling Guide](#) as a reference to assist you building your own.

You can use Security Center Alerts during the following stages:

- **Detect:** identify a suspicious activity in one or more resources.
- **Assess:** perform the initial assessment to obtain more information about the suspicious activity.
- **Diagnose:** use the remediation steps to conduct the technical procedure to address the issue.

Each Security Alert provides information that can be used to better understand the nature of the attack and suggest possible mitigations. Some alerts also provide links to either more information or to other sources of information within Azure. You can use the information provided for further research and to begin mitigation, and you can also search security-related data that is stored in your workspace.

The following example shows a suspicious RDP activity taking place:

Suspicious RDP VM activity

WebServer

| | |
|-------------------|---|
| ALERT | Several Remote Desktop login attempts were detected from FreeRDP. All the attempts in the last 24 hours were on invalid accounts. |
| DETECTION TIME | Tuesday, April 12, 2016, 7:10:17 PM |
| SEVERITY | Medium |
| STATE | Active |
| ATTACKED RESOURCE | WebServer |
| DETECTED BY | Microsoft |
| ACTION TAKEN | Detected |
| ACCOUNTS SEEN | 3 |
| FAILED ATTEMPTS | 16 |
| SOURCE | FreeRDP |
| DURATION | 13 hours |
| REMEDIAL STEPS | <ol style="list-style-type: none">1. If available, add the source IP to NSG block list for 24 hours (see https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-nsg/)2. Enforce the use of strong passwords and do not reuse them across multiple VMs and services (see http://windows.microsoft.com/en-us/Windows7/Tips-for-creating-strong-passwords-and-passphrases)3. Create an allow list for RDP access in NSG (see https://azure.microsoft.com/en-us/documentation/articles/virtual-networks-nsg/) |

This page shows the details regarding the time that the attack took place, the source hostname, the target VM and also gives recommendation steps. In some circumstances, the source information of the attack may be empty. Read [Missing Source Information in Azure Security Center Alerts](#) for more information about this type of behavior.

From this page, you can also start an [investigation](#) to better understand the timeline of the attack, how the attack took place, which systems were potentially compromised, which credentials were used, and see a graphical representation of the entire attack chain.

Once you identify the compromised system, you can run a [Workflow Automation](#) that was previously created. These are a collection of procedures that can be executed from Security Center once triggered by an alert.

In the [How to Leverage the Azure Security Center & Microsoft Operations Management Suite for an Incident Response](#) video, you can see some demonstrations that can help you to understand how Security Center can be used in each one of those stages.

NOTE

Read [Managing and responding to security alerts in Azure Security Center](#) for more information on how to use Security Center capabilities to assist you during your Incident Response process.

Next steps

In this document, you learned how to plan for Security Center adoption. To learn more about Security Center, see the following:

- [Managing and responding to security alerts in Azure Security Center](#)
- [Security health monitoring in Azure Security Center](#) — Learn how to monitor the health of your Azure

resources.

- [Monitoring partner solutions with Azure Security Center](#) — Learn how to monitor the health status of your partner solutions.
- [Azure Security Center FAQ](#) — Find frequently asked questions about using the service.
- [Azure Security blog](#) — Find blog posts about Azure security and compliance.

FAQ - General questions about Azure Security Center

2/27/2020 • 3 minutes to read • [Edit Online](#)

What is Azure Security Center?

Azure Security Center helps you prevent, detect, and respond to threats with increased visibility into and control over the security of your resources. It provides integrated security monitoring and policy management across your subscriptions, helps detect threats that might otherwise go unnoticed, and works with a broad ecosystem of security solutions.

Security Center uses the Microsoft Monitoring Agent to collect and store data. For in-depth details, see [Data collection in Azure Security Center](#).

How do I get Azure Security Center?

Azure Security Center is enabled with your Microsoft Azure subscription and accessed from the [Azure portal](#). To access it, [sign in to the portal](#), select **Browse**, and scroll to **Security Center**.

Which Azure resources are monitored by Azure Security Center?

Azure Security Center monitors the following Azure resources:

- Virtual machines (VMs) (including [Cloud Services](#))
- Virtual machine scale sets
- Azure Virtual Networks
- Containers
- Azure SQL service
- Azure Storage account
- Azure Web Apps (in [App Service Environment](#))
- Partner solutions integrated with your Azure subscription such as a web application firewall on VMs and on App Service Environment

In addition, non-Azure (including on-premises) machines can also be monitored by Azure Security Center. Both [Windows machines](#) and [Linux machines](#) are supported.

How can I see the current security state of my Azure resources?

The **Security Center Overview** page shows the overall security posture of your environment broken down by Compute, Networking, Storage & data, and Applications. Each resource type has an indicator showing identified security vulnerabilities. Clicking each tile displays a list of security issues identified by Security Center, along with an inventory of the resources in your subscription.

What is a security policy?

A security policy defines the set of controls that are recommended for resources within the specified subscription. In Azure Security Center, you define policies for your Azure subscriptions according to your company's security requirements and the type of applications or sensitivity of the data in each subscription.

The security policies enabled in Azure Security Center drive security recommendations and monitoring. To learn more about security policies, see [Security health monitoring in Azure Security Center](#).

Who can modify a security policy?

To modify a security policy, you must be a Security Administrator or an Owner or Contributor of that subscription.

To learn how to configure a security policy, see [Setting security policies in Azure Security Center](#).

What is a security recommendation?

Azure Security Center analyzes the security state of your Azure resources. When potential security vulnerabilities are identified, recommendations are created. The recommendations guide you through the process of configuring the needed control. Examples are:

- Provisioning of anti-malware to help identify and remove malicious software
- [Network security groups](#) and rules to control traffic to virtual machines
- Provisioning of a web application firewall to help defend against attacks targeting your web applications
- Deploying missing system updates
- Addressing OS configurations that do not match the recommended baselines

Only recommendations that are enabled in Security Policies are shown here.

What triggers a security alert?

Azure Security Center automatically collects, analyzes, and fuses log data from your Azure resources, the network, and partner solutions like antimalware and firewalls. When threats are detected, a security alert is created. Examples include detection of:

- Compromised virtual machines communicating with known malicious IP addresses
- Advanced malware detected using Windows error reporting
- Brute force attacks against virtual machines
- Security alerts from integrated partner security solutions such as Anti-Malware or Web Application Firewalls

Why did Secure Score values change?

As of February 2019, Security Center adjusted the score of a few recommendations, in order to better fit their severity. As a result of this adjustment, there may be changes in overall Secure Score values. For more information about Secure Score, see [Secure Score calculation](#).

What's the difference between threats detected and alerted on by Microsoft Security Response Center versus Azure Security Center?

The Microsoft Security Response Center (MSRC) performs select security monitoring of the Azure network and infrastructure and receives threat intelligence and abuse complaints from third parties. When MSRC becomes aware that customer data has been accessed by an unlawful or unauthorized party or that the customer's use of Azure does not comply with the terms for Acceptable Use, a security incident manager notifies the customer. Notification typically occurs by sending an email to the security contacts specified in Azure Security Center or the Azure subscription owner if a security contact is not specified.

Security Center is an Azure service that continuously monitors the customer's Azure environment and applies analytics to automatically detect a wide range of potentially malicious activity. These detections are surfaced as security alerts in the Security Center dashboard.

Billing questions

2/27/2020 • 2 minutes to read • [Edit Online](#)

How does billing work for Azure Security Center?

Security Center is offered in two tiers:

- The **free tier** provides visibility into the security state of your Azure resources, basic security policy, security recommendations, and integration with security products and services from partners.
- The **standard tier** adds threat protection capabilities that includes security alerts, threat intelligence, behavioral analysis, anomaly detection, and threat attribution reports. You can start a standard tier free trial. To upgrade, select [Pricing Tier](#) in the security policy. To learn more, see the [pricing page](#).

How can I track who in my organization performed pricing tier changes in Azure Security Center

Azure Subscriptions may have multiple administrators with permissions to change the pricing tier. To find out which user performed a pricing tier change, use the Azure Activity Log. For more information, see [here](#).

Permissions

2/25/2020 • 2 minutes to read • [Edit Online](#)

How do permissions work in Azure Security Center?

Azure Security Center uses [Role-Based Access Control \(RBAC\)](#), which provides [built-in roles](#) that can be assigned to users, groups, and services in Azure.

Security Center assesses the configuration of your resources to identify security issues and vulnerabilities. In Security Center, you only see information related to a resource when you are assigned the role of Owner, Contributor, or Reader for the subscription or resource group that a resource belongs to.

See [Permissions in Azure Security Center](#) to learn more about roles and allowed actions in Security Center.

Who can modify a security policy?

To modify a security policy, you must be a Security Administrator or an Owner or Contributor of that subscription.

To learn how to configure a security policy, see [Setting security policies in Azure Security Center](#).

FAQ - Questions about data collection, agents, and workspaces

2/25/2020 • 11 minutes to read • [Edit Online](#)

Security Center collects data from your Azure virtual machines (VMs), Virtual machine scale sets, IaaS containers, and non-Azure computers (including on-premises machines) to monitor for security vulnerabilities and threats. Data is collected using the Microsoft Monitoring Agent, which reads various security-related configurations and event logs from the machine and copies the data to your workspace for analysis.

Am I billed for Azure Monitor logs on the workspaces created by Security Center?

No. Workspaces created by Security Center, while configured for Azure Monitor logs per node billing, don't incur Azure Monitor logs charges. Security Center billing is always based on your Security Center security policy and the solutions installed on a workspace:

- **Free tier** – Security Center enables the 'SecurityCenterFree' solution on the default workspace. You won't be billed for the Free tier.
- **Standard tier** – Security Center enables the 'Security' solution on the default workspace.

For more information on pricing, see [Security Center pricing](#).

NOTE

The log analytics pricing tier of workspaces created by Security Center does not affect Security Center billing.

NOTE

This article was recently updated to use the term Azure Monitor logs instead of Log Analytics. Log data is still stored in a Log Analytics workspace and is still collected and analyzed by the same Log Analytics service. We are updating the terminology to better reflect the role of [logs in Azure Monitor](#). See [Azure Monitor terminology changes](#) for details.

What qualifies a VM for automatic provisioning of the Microsoft Monitoring Agent installation?

Windows or Linux IaaS VMs qualify if:

- The Microsoft Monitoring Agent extension is not currently installed on the VM.
- The VM is in running state.
- The Windows or Linux [Azure Virtual Machine Agent](#) is installed.
- The VM is not used as an appliance such as web application firewall or next generation firewall.

Can I delete the default workspaces created by Security Center?

Deleting the default workspace is not recommended. Security Center uses the default workspaces to store security data from your VMs. If you delete a workspace, Security Center is unable to collect this data and some security recommendations and alerts are unavailable.

To recover, remove the Microsoft Monitoring Agent on the VMs connected to the deleted workspace. Security Center reinstalls the agent and creates new default workspaces.

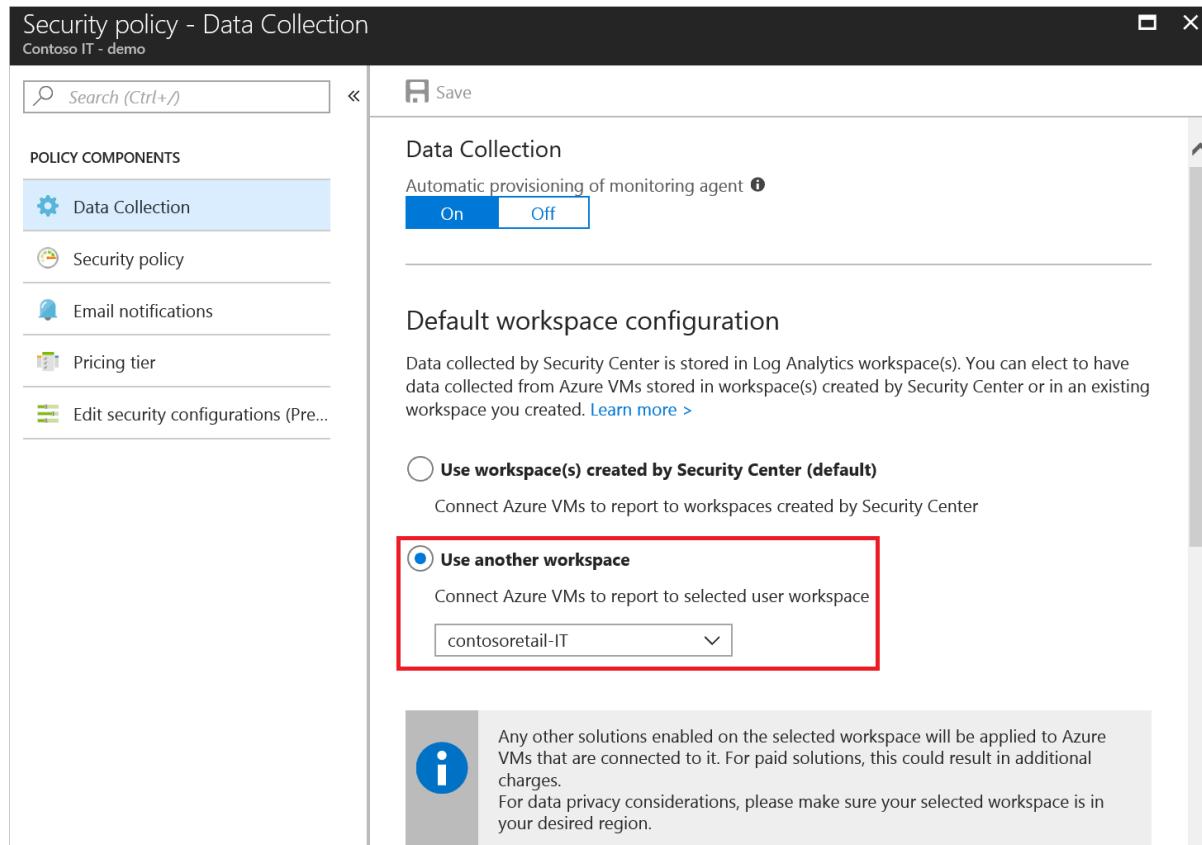
How can I use my existing Log Analytics workspace?

You can select an existing Log Analytics workspace to store data collected by Security Center. To use your existing Log Analytics workspace:

- The workspace must be associated with your selected Azure subscription.
- At a minimum, you must have read permissions to access the workspace.

To select an existing Log Analytics workspace:

1. Under **Security policy – Data Collection**, select **Use another workspace**.



2. From the pull-down menu, select a workspace to store collected data.

NOTE

In the pull down menu, only workspaces that you have access to and are in your Azure subscription are shown.

3. Select **Save**. You will be asked if you would like to reconfigure monitored VMs.

- Select **No** if you want the new workspace settings to **apply on new VMs only**. The new workspace settings only apply to new agent installations; newly discovered VMs that do not have the Microsoft Monitoring Agent installed.
- Select **Yes** if you want the new workspace settings to **apply on all VMs**. In addition, every VM connected to a Security Center created workspace is reconnected to the new target workspace.

NOTE

If you select **Yes**, don't delete any workspaces created by Security Center until all VMs have been reconnected to the new target workspace. This operation fails if a workspace is deleted too early.

- To cancel the operation, select **Cancel**.

What if the Microsoft Monitoring Agent was already installed as an extension on the VM?

When the Monitoring Agent is installed as an extension, the extension configuration allows reporting to only a single workspace. Security Center does not override existing connections to user workspaces. Security Center will store security data from a VM in a workspace that is already connected, provided that the "Security" or "SecurityCenterFree" solution has been installed on it. Security Center may upgrade the extension version to the latest version in this process.

For more information, see [Automatic provisioning in cases of a pre-existing agent installation](#).

What if a Microsoft Monitoring Agent is directly installed on the machine but not as an extension (Direct Agent)?

If the Microsoft Monitoring Agent is installed directly on the VM (not as an Azure extension), Security Center will install the Microsoft Monitoring Agent extension, and may upgrade the Microsoft Monitoring agent to the latest version.

The agent installed will continue to report to its already configured workspace(s), and in addition will report to the workspace configured in Security Center (Multi-homing is supported on Windows machines).

If the configured workspace is a user workspace (not Security Center's default workspace), you will need to install the "Security"/"SecurityCenterFree" solution on it for Security Center to start processing events from VMs and computers reporting to that workspace.

For Linux machines, Agent multi-homing is not yet supported - hence, if an existing agent installation is detected, automatic provisioning will not occur and the machine's configuration will not be altered.

For existing machines on subscriptions onboarded to Security Center before March 17 2019, when an existing agent will be detected, the Microsoft Monitoring Agent extension will not be installed and the machine will not be affected. For these machines, see the "Resolve monitoring agent health issues on your machines" recommendation to resolve the agent installation issues on these machines

For more information, see the next section [What happens if a System Center Operations Manager or OMS direct agent is already installed on my VM?](#)

What if a System Center Operations Manager agent is already installed on my VM?

Security center will install the Microsoft Monitoring Agent extension side by side to the existing System Center Operations Manager agent. The existing agent will continue to report to the System Center Operations Manager server normally. Note that the Operations Manager agent and Microsoft Monitoring Agent share common run-time libraries, which will be updated to the latest version during this process. Note - If version 2012 of the Operations Manager agent is installed, do not turn on automatic provisioning (manageability capabilities can be lost when the Operations Manager server is also version 2012).

What is the impact of removing these extensions?

If you remove the Microsoft Monitoring Extension, Security Center is not able to collect security data from the VM and some security recommendations and alerts are unavailable. Within 24 hours, Security Center determines that the VM is missing the extension and reinstalls the extension.

How do I stop the automatic agent installation and workspace creation?

You can turn off automatic provisioning for your subscriptions in the security policy but this is not recommended.

Turning off automatic provisioning limits Security Center recommendations and alerts. To disable automatic provisioning:

1. If your subscription is configured for the Standard tier, open the security policy for that subscription and select the **Free** tier.

| Pricing tier | Features | Cost |
|--------------|--|----------------------|
| Free | <ul style="list-style-type: none">✓ Security assessment✓ Security recommendations✓ Basic security policy✓ Connected partner solutions✗ Just in time VM Access✗ Network threat detection✗ VM threat detection | 0.00 USD/NODE/MONTH |
| Standard | <ul style="list-style-type: none">✓ Security assessment✓ Security recommendations✓ Basic security policy✓ Connected partner solutions✓ Just in time VM Access✓ Network threat detection✓ VM threat detection | 15.00 USD/NODE/MONTH |

2. Next, turn off automatic provisioning by selecting **Off** on the **Security policy – Data collection** page.

Security policy - Data Collection
ASC DEMO

Search (Ctrl+ /)

POLICY COMPONENTS

- Data Collection**
- Security policy
- Email notifications
- Pricing tier

Save

Onboarding

Automatic provisioning of monitoring agent ?

On **Off**

Default workspace configuration

Data collected by Security Center is stored in Log Analytics workspace(s). You can elect to have data collected from Azure VMs stored in workspace(s) created by Security Center or in an existing workspace you created.

Use workspace(s) created by Security Center (default)
Connect Azure VMs to report to workspaces created by Security Center

Use another workspace
Connect Azure VMs to report to selected user workspace

Choose a workspace ▾

i Any other solutions enabled on the selected workspace will be applied to Azure VMs that are connected to it. For paid solutions, this could result in additional charges.

Should I opt out of the automatic agent installation and workspace creation?

NOTE

Be sure to review sections [What are the implications of opting out?](#) and [recommended steps when opting out](#) if you choose to opt out of automatic provisioning.

You may want to opt out of automatic provisioning if the following applies to you:

- Automatic agent installation by Security Center applies to the entire subscription. You cannot apply automatic installation to a subset of VMs. If there are critical VMs that cannot be installed with the Microsoft Monitoring Agent, then you should opt out of automatic provisioning.
- Installation of the Microsoft Monitoring Agent (MMA) extension updates the agent's version. This applies to a direct agent and a System Center Operations Manager agent (in the latter, the Operations Manager and MMA share common runtime libraries - which will be updated in the process). If the installed Operations Manager agent is version 2012 and is upgraded, manageability capabilities can be lost when the Operations Manager server is also version 2012. Consider opting out of automatic provisioning if the installed Operations Manager agent is version 2012.
- If you have a custom workspace external to the subscription (a centralized workspace), then you should opt out of automatic provisioning. You can manually install the Microsoft Monitoring Agent extension and connect it to your workspace without Security Center overriding the connection.
- If you want to avoid creation of multiple workspaces per subscription and you have your own custom workspace within the subscription, then you have two options:
 - You can opt out of automatic provisioning. After migration, set the default workspace settings as described in [How can I use my existing Log Analytics workspace?](#)
 - Or, you can allow the migration to complete, the Microsoft Monitoring Agent to be installed on the

VMs, and the VMs connected to the created workspace. Then, select your own custom workspace by setting the default workspace setting with opting in to reconfiguring the already installed agents. For more information, see [How can I use my existing Log Analytics workspace?](#)

What are the implications of opting out of automatic provisioning?

When migration is complete, Security Center can't collect security data from the VM and some security recommendations and alerts are unavailable. If you opt out, install the Microsoft Monitoring Agent manually. See [recommended steps when opting out](#).

What are the recommended steps when opting out of automatic provisioning?

Manually install the Microsoft Monitoring Agent extension so Security Center can collect security data from your VMs and provide recommendations and alerts. See [agent installation for Windows VM](#) or [agent installation for Linux VM](#) for guidance on installation.

You can connect the agent to any existing custom workspace or Security Center created workspace. If a custom workspace does not have the 'Security' or 'SecurityCenterFree' solutions enabled, then you will need to apply a solution. To apply, select the custom workspace or subscription and apply a pricing tier via the **Security policy – Pricing tier** page.

| Pricing Tier | Included Features | Excluded Features | Price |
|--------------|---|---|----------------------|
| Free | ✓ Security assessment ✓ Security recommendations ✓ Basic security policy ✓ Connected partner solutions | ✗ Just in time VM Access ✗ Network threat detection ✗ VM threat detection | 0.00 USD/NODE/MONTH |
| Standard | All features listed for Free + ✓ Just in time VM Access ✓ Network threat detection ✓ VM threat detection | | 15.00 USD/NODE/MONTH |

Security Center will enable the correct solution on the workspace based on the selected pricing tier.

How do I remove OMS extensions installed by Security Center?

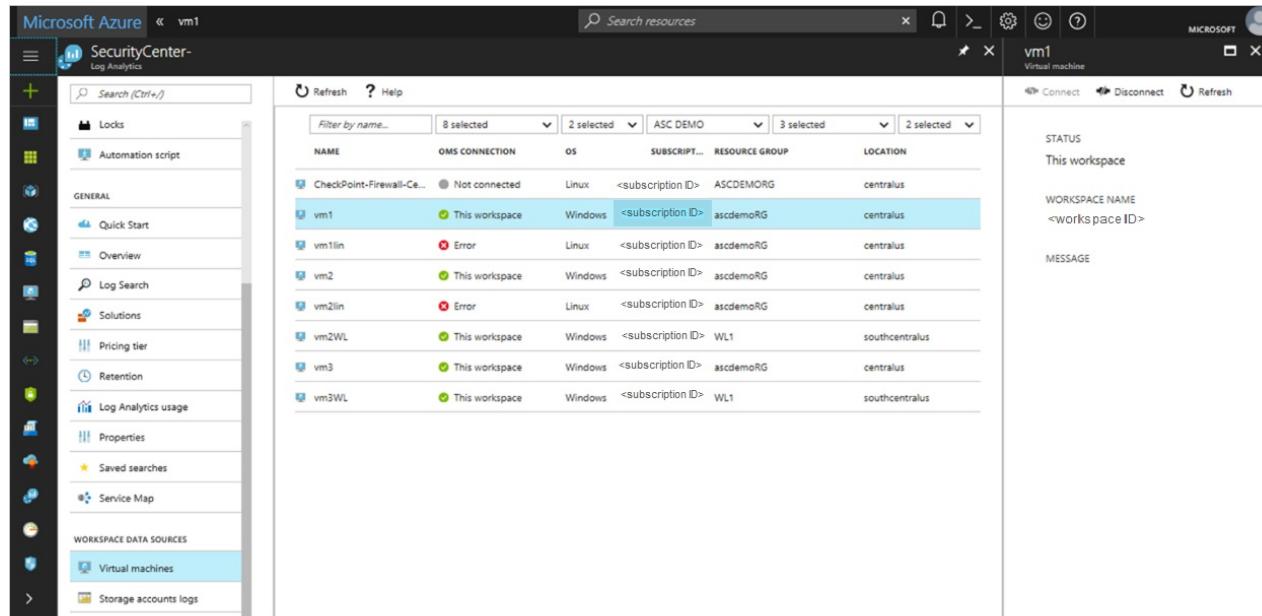
You can manually remove the Microsoft Monitoring Agent. This is not recommended as it limits Security Center recommendations and alerts.

NOTE

If data collection is enabled, Security Center will reinstall the agent after you remove it. You need to disable data collection before manually removing the agent. See [How do I stop the automatic agent installation and workspace creation?](#) for instructions on disabling data collection.

To manually remove the agent:

1. In the portal, open **Log Analytics**.
2. On the Log Analytics page, select a workspace:
3. Select the VMs that you don't want to monitor and select **Disconnect**.



| NAME | OMS CONNECTION | OS | SUBSCRIPT... | RESOURCE GROUP | LOCATION |
|---------------------------|----------------|---------|-------------------|----------------|----------------|
| CheckPoint-Firewall-Ce... | Not connected | Linux | <subscription ID> | ASCDEMORG | centralus |
| vm1 | This workspace | Windows | <subscription ID> | ascdemoRG | centralus |
| vm1lin | Error | Linux | <subscription ID> | ascdemoRG | centralus |
| vm2 | This workspace | Windows | <subscription ID> | ascdemoRG | centralus |
| vm2lin | Error | Linux | <subscription ID> | ascdemoRG | centralus |
| vm2WL | This workspace | Windows | <subscription ID> | WL1 | southcentralus |
| vm3 | This workspace | Windows | <subscription ID> | ascdemoRG | centralus |
| vm3WL | This workspace | Windows | <subscription ID> | WL1 | southcentralus |

NOTE

If a Linux VM already has a non-extension OMS agent, removing the extension removes the agent as well and you'll have to reinstall it.

How do I disable data collection?

Automatic provisioning is off by default. You can disable automatic provisioning from resources at any time by turning off this setting in the security policy. Automatic provisioning is highly recommended in order to get security alerts and recommendations about system updates, OS vulnerabilities, and endpoint protection.

To disable data collection, [Sign in to the Azure portal](#), select **Browse**, select **Security Center**, and select **Select policy**. Select the subscription that you wish to disable automatic provisioning. When you select a subscription **Security policy - Data collection** opens. Under **Auto provisioning**, select **Off**.

How do I enable data collection?

You can enable data collection for your Azure subscription in the Security policy. To enable data collection. [Sign in to the Azure portal](#), select **Browse**, select **Security Center**, and select **Security policy**. Select the subscription that you wish to enable automatic provisioning. When you select a subscription **Security policy - Data collection** opens. Under **Auto provisioning**, select **On**.

What happens when data collection is enabled?

When automatic provisioning is enabled, Security Center provisions the Microsoft Monitoring Agent on all supported Azure VMs and any new ones that are created. Automatic provisioning is recommended but manual agent installation is also available. [Learn how to install the Microsoft Monitoring Agent extension](#).

The agent enables the process creation event 4688 and the *CommandLine* field inside event 4688. New processes created on the VM are recorded by EventLog and monitored by Security Center's detection services. For more information on the details recorded for each new process, see [description fields in 4688](#). The agent also collects the 4688 events created on the VM and stores them in search.

The agent also enables data collection for [Adaptive Application Controls](#), Security Center configures a local AppLocker policy in Audit mode to allow all applications. This policy will cause AppLocker to generate events, which are then collected and leveraged by Security Center. It is important to note that this policy will not be configured on any machines on which there is already a configured AppLocker policy.

When Security Center detects suspicious activity on the VM, the customer is notified by email if [security contact information](#) has been provided. An alert is also visible in Security Center's security alerts dashboard.

Will Security Center work using an OMS gateway?

Yes. Azure Security Center leverages Azure Monitor to collect data from Azure VMs and servers, using the Microsoft Monitoring Agent. To collect the data, each VM and server must connect to the Internet using HTTPS. The connection can be direct, using a proxy, or through the [OMS Gateway](#).

Does the Monitoring Agent impact the performance of my servers?

The agent consumes a nominal amount of system resources and should have little impact on the performance. For more information on performance impact and the agent and extension, see the [planning and operations guide](#).

Where is my data stored?

Data collected from this agent is stored in either an existing Log Analytics workspace associated with your subscription or a new workspace. For more information, see [Data Security](#).

FAQ - Questions about virtual machines

2/25/2020 • 2 minutes to read • [Edit Online](#)

What types of virtual machines are supported?

Monitoring and recommendations are available for virtual machines (VMs) created using both the [classic](#) and [Resource Manager](#) deployment models.

See [Supported platforms in Azure Security Center](#) for a list of supported platforms.

Why doesn't Azure Security Center recognize the antimalware solution running on my Azure VM?

Azure Security Center has visibility into antimalware installed through Azure extensions. For example, Security Center is not able to detect antimalware that was pre-installed on an image you provided or if you installed antimalware on your virtual machines using your own processes (such as configuration management systems).

Why do I get the message "Missing Scan Data" for my VM?

This message appears when there is no scan data for a VM. It can take some time (less than an hour) for scan data to populate after Data Collection is enabled in Azure Security Center. After the initial population of scan data, you may receive this message because there is no scan data at all or there is no recent scan data. Scans do not populate for a VM in a stopped state. This message could also appear if scan data has not populated recently (in accordance with the retention policy for the Windows agent, which has a default value of 30 days).

How often does Security Center scan for operating system vulnerabilities, system updates, and endpoint protection issues?

Below are the latency times for Security Center scans of vulnerabilities, updates, and issues:

- Operating system security configurations – data is updated within 48 hours
- System updates – data is updated within 24 hours
- Endpoint Protection issues – data is updated within 8 hours

Security Center typically scans for new data every hour, and refreshes the recommendations accordingly.

NOTE

Security Center uses the Microsoft Monitoring Agent to collect and store data. To learn more, see [Azure Security Center Platform Migration](#).

Why do I get the message "VM Agent is Missing?"

The VM Agent must be installed on VMs to enable Data Collection. The VM Agent is installed by default for VMs that are deployed from the Azure Marketplace. For information on how to install the VM Agent on other VMs, see the blog post [VM Agent and Extensions](#).

FAQ for customers already using Azure Monitor logs

2/27/2020 • 2 minutes to read • [Edit Online](#)

Does Security Center override any existing connections between VMs and workspaces?

If a VM already has the Microsoft Monitoring Agent installed as an Azure extension, Security Center does not override the existing workspace connection. Instead, Security Center uses the existing workspace. The VM will be protected provided that the "Security" or "SecurityCenterFree" solution has been installed on the workspace to which it is reporting.

A Security Center solution is installed on the workspace selected in the Data Collection screen if not present already, and the solution is applied only to the relevant VMs. When you add a solution, it's automatically deployed by default to all Windows and Linux agents connected to your Log Analytics workspace. [Solution Targeting](#) allows you to apply a scope to your solutions.

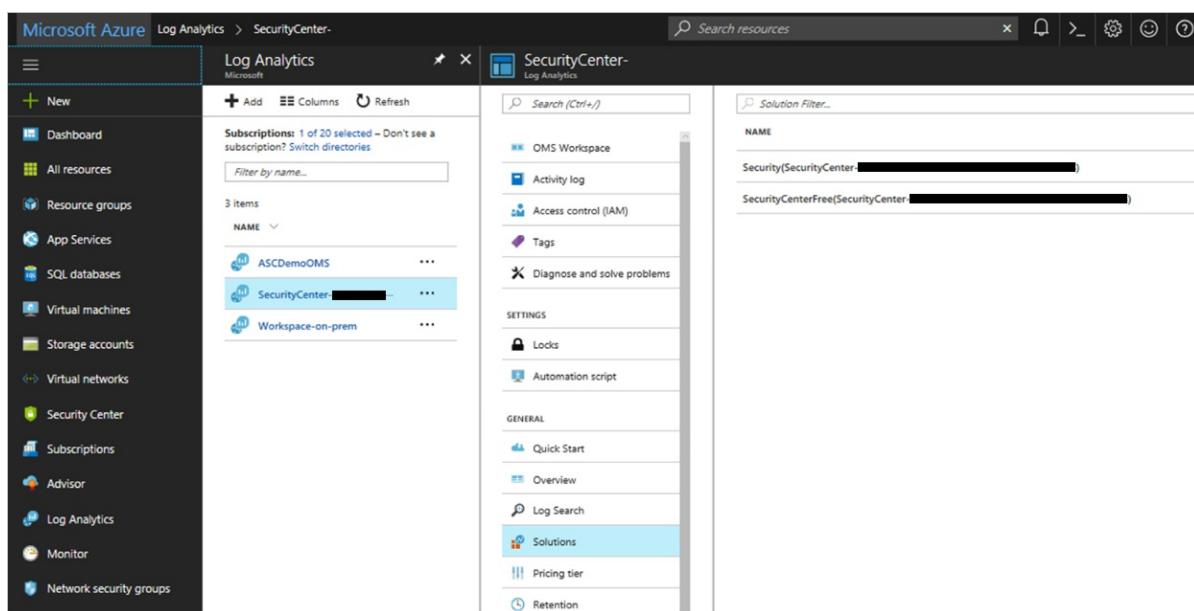
TIP

If the Microsoft Monitoring Agent is installed directly on the VM (not as an Azure extension), Security Center does not install the Microsoft Monitoring Agent, and security monitoring is limited.

Does Security Center install solutions on my existing Log Analytics workspaces? What are the billing implications?

When Security Center identifies that a VM is already connected to a workspace you created, Security Center enables solutions on this workspace according to your pricing tier. The solutions are applied only to the relevant Azure VMs, via [solution targeting](#), so the billing remains the same.

- **Free tier** – Security Center installs the 'SecurityCenterFree' solution on the workspace. You won't be billed for the Free tier.
- **Standard tier** – Security Center installs the 'Security' solution on the workspace.



I already have workspaces in my environment, can I use them to collect security data?

If a VM already has the Microsoft Monitoring Agent installed as an Azure extension, Security Center uses the existing connected workspace. A Security Center solution is installed on the workspace if not present already, and the solution is applied only to the relevant VMs via [solution targeting](#).

When Security Center installs the Microsoft Monitoring Agent on VMs, it uses the default workspace(s) created by Security Center.

I already have security solution on my workspaces. What are the billing implications?

The Security & Audit solution is used to enable Security Center standard tier features for Azure VMs. If the Security & Audit solution is already installed on a workspace, Security Center uses the existing solution. There is no change in billing.

Retirement of Security Center features (July 2019)

2/25/2020 • 7 minutes to read • [Edit Online](#)

NOTE

This document details the list of features that were retired from Azure Security Center on July 31st, 2019.

We made several [improvements](#) to Azure Security Center over the six months leading up to July 2019. With these improved capabilities, we removed some redundant features and related APIs from Security Center on July 31, 2019.

Most of these retired features can be replaced with other functionality in Azure Security Center or Azure Log Analytics. Other features can be implemented using [Azure Sentinel \(preview\)](#).

Retired Security Center features include:

- [Events dashboard](#)
- [Search menu entry](#)
- [View classic Identity & Access link on Identity and access \(preview\)](#)
- [Security events map button on Security alerts map \(preview\)](#)
- [Custom alert rules \(preview\)](#)
- [Investigate button in threat protection security alerts](#)
- [A subset of Security solutions](#)
- [Edit security configurations for Security policies](#)
- [Security and audit dashboard \(originally used in OMS portal\) for Log Analytics workspaces](#)

This article provides detailed information for each retired feature and the steps you can take to implement replacement features.

Events dashboard

Security Center uses Microsoft Monitoring Agent to collect various security-related configurations and events from your machines. It stores these events in your workspaces. The [events dashboard](#) lets you view this data and gives you an entry point to Log Analytics.

We retired the events dashboard that appeared when you selected a workspace:

Events dashboard
defaultworkspace-212f9889-769e-45ae-ab43-6da33674bd26-eus

Filter **Add Notable Event** **Edit Notable Events**

Events over time - Last 7 Days

No events found.

All events by type [Notable events](#)

| NAME | # OF EVENTS |
|------------------|-------------|
| No events found. | |

Events dashboard - the new experience

We encourage you to use the native capabilities of Azure Log Analytics to view notable events on your workspaces.

If you've created custom notable events in Security Center, they'll be accessible. In Log Analytics, go to **Select workspace > Saved Searches**. Your data won't be lost or modified. Native notable events are also available from the same screen in Log Analytics.

A-MgmtWorkspace - Saved searches
Log Analytics workspace

[Add](#)

| NAME | CATEGORY | FUNCTION ALIAS |
|--|---------------------|----------------|
| test Alert rule | Alertibiza | ... |
| All Computers with their most recent data | General Exploration | ... |
| Distribution of data Types | General Exploration | ... |
| Stale Computers (data older than 24 hours) | General Exploration | ... |
| Which Management Group is generating ... | General Exploration | ... |
| All Events | Log Management | ... |
| All Events with level "Warning" | Log Management | ... |
| All IIS Log Entries | Log Management | ... |
| All Syslog Records grouped by Facility | Log Management | ... |
| All Syslog Records grouped by ProcessNa... | Log Management | ... |
| All Syslog Records with Errors | Log Management | ... |
| All Syslogs | Log Management | ... |

Search menu entry

Azure Security Center currently uses Azure Monitor logs search to retrieve and analyze your security data. This screen serves as a window to Log Analytics search page, and enables users to run search queries on their selected

workspace. For more information, see [Azure Security Center search](#). We retired this search window:

The screenshot shows the Azure Security Center - Search interface. On the left, there's a sidebar with a search bar at the top, followed by sections for GENERAL (Overview, Getting started, Events, Search), POLICY & COMPLIANCE (Coverage, Secure score, Security policy, Regulatory compliance), and RESOURCE SECURITY HYGIENE. The 'Search' menu entry under GENERAL is highlighted with a blue background. The main area is titled 'Search' and prompts 'Choose a workspace to view its search dashboard'. It lists three workspaces: 'defaultworkspace-212f9889-76...' (East US, ASC DEMO), 'exportsecuritycenterdatatolog...' (East US, ASC DEMO), and 'defaultworkspace-212f9889-76...' (West Europe, ASC DEMO). The first workspace is selected and highlighted with a dashed border.

Search menu entry - the new experience

We encourage you to use the Azure Log Analytics native capabilities to perform Search queries on your workspaces. Go to Azure Log Analytics and select **Logs**.

The screenshot shows the Azure Log Analytics Logs blade for the 'A-MgmtWorkspace' workspace. The left sidebar includes options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings (Locks, Export template), General (Quick Start, Workspace summary), Logs (selected), and Solutions. The main area has a search bar at the top, followed by a 'New Query 1' button, workspace selection ('A-MgmtWorkspace'), run button ('Run'), time range ('Last 24 hours'), and save/help buttons. Below is a schema viewer with a 'Schema' tab, a filter preview, and a search bar ('Type your query here...'). A 'Get started with sample queries' section provides links to Computer availability, Computer performance, and Data usage. The 'Logs' menu entry in the sidebar is highlighted with a blue background.

Classic Identity & Access (Preview)

The Classic Identity & Access experience in Security Center currently shows a dashboard of identity and access information in Log Analytics. To view this dashboard:

1. Select **View classic Identity & Access**.

Home > Security Center - Identity & access (Preview) > Identity & Access dashboard

Showing subscription 'ASC DEMO'

GENERAL

- Overview
- Getting started
- Events
- Search

POLICY & COMPLIANCE

- Coverage
- Secure score
- Security policy
- Regulatory compliance

RESOURCE SECURITY HYGIENE

- Recommendations
- Compute & apps
- IoT hubs & resources
- Networking
- Data & storage
- Identity & access (Preview)
- Security solutions

ADVANCED CLOUD DEFENSE

View classic Identity & Access

Overview **Subscriptions** **Key vaults**

Search recommendations

| RECOMMENDATION | SECURE SCORING | FAILED RESOURCES |
|--|----------------|----------------------|
| Enable MFA for accounts with owner permissions on your s... | +50 | 1 of 1 subscriptions |
| Remove external accounts with write permissions from you... | +30 | 1 of 1 subscriptions |
| Enable MFA for accounts with write permissions on your su... | +30 | 1 of 1 subscriptions |
| Designate up to 3 owners on your subscription (Preview) | +5 | 1 of 1 subscriptions |
| Enable MFA for accounts with read permissions on your su... | +30 | 1 of 1 subscriptions |
| Remove external accounts with read permissions from your... | +15 | 1 of 1 subscriptions |
| Remove deprecated accounts from your subscription (Previe... | +10 | 1 of 1 subscriptions |
| Enable diagnostic logs in Key Vault | +5 | 3 of 3 key vaults |

2. View the Identity & Access dashboard.

Identity & Access dashboard

Refresh

Identity & Access dashboard

Choose a workspace to view its identity & access dashboard

| WORKSPACE NAME | FAILED LOGONS | SUCCESSFUL LOGONS | LOCATION | SUBSCRIPTION |
|---|---------------|-------------------|-------------|--------------|
| defaultworkspace-212f9889-769e-45ae-ab43-6da33674bd26-eus | - | - | East US | ASC DEMO |
| exportsecuritycenterdatatologaworkspacetest | - | - | East US | ASC DEMO |
| defaultworkspace-212f9889-769e-45ae-ab43-6da33674bd26-weu | - | - | West Europe | ASC DEMO |

3. Select a workspace to open the Identity & Access dashboard in Log Analytics to view identity and access information on your workspace.

Identity & Access (Preview)

defaultworkspace-212f9889-769e-45ae-ab43-6da33674bd26-eus

Refresh **Logs**

Last 24 hours

IDENTITY POSTURE

| | |
|--------|-----------|
| Logons | 0% FAILED |
| 0 | 0 |

FAILED LOGONS

| | |
|--|---------|
| Failed logon reasons | 0 TOTAL |
| No failed logons were found for the time period. | |

LOGONS OVER TIME

0 SUCCESSFUL | 0 FAILED

1
0.5
0
3:00 PM 7:00 PM 11:00 PM 3:00 AM 7:00 AM 11:00 AM 3:00 PM 7:00 PM

ACCOUNTS LOGGED ON

| | |
|--------------------|---|
| Accounts logged on | 0 |
| 0 | 0 |

ACCOUNTS FAILED TO LOG ON

| | |
|---------------------------|---|
| Accounts failed to log on | 0 |
| 0 | 0 |

LOCKED ACCOUNTS

| | |
|-----------------|---|
| Locked accounts | 0 |
| 0 | 0 |

ACCOUNTS WITH CHANGED OR RESET PASSWORD

| | |
|---|---|
| Accounts with changed or reset password | 0 |
| 0 | 0 |

ACTIVE CRITICAL NOTABLE ISSUES

| | |
|--------------------------------|---|
| Active critical notable issues | 0 |
| 0 | 0 |

ACTIVE WARNING NOTABLE ISSUES

| | |
|-------------------------------|---|
| Active warning notable issues | 0 |
| 0 | 0 |

COMPUTER ACCESSED

No logon attempts were found for the time period.

LOGON ATTEMPTS

No logon attempts were found for the time period.

We retired all three screens shown in the preceding steps. Your data remains available in the Log Analytics security

solution and wasn't modified or removed.

Classic Identity & Access (Preview) - the new experience

The Log Analytics dashboard has shown insights on a single workspace. However, native Security Center capabilities provide visibility into all subscriptions and all workspaces associated with them. You can access an easy-to use view that lets you focus on what's important with recommendations ranked according to their Secure Score.

All the features of the **Identity & Access** dashboard in Log Analytics can be reached by selecting **Identity & access (Preview)** within Security Center.

| RECOMMENDATION | SECURE SCORE | FAILED RESOURCES |
|--|--------------|----------------------|
| Enable MFA for accounts with owner permissions on your s... | +50 | 1 of 1 subscriptions |
| Remove external accounts with write permissions from you... | +30 | 1 of 1 subscriptions |
| Enable MFA for accounts with write permissions on your su... | +30 | 1 of 1 subscriptions |
| Designate up to 3 owners on your subscription (Preview) | +5 | 1 of 1 subscriptions |
| Enable MFA for accounts with read permissions on your su... | +30 | 1 of 1 subscriptions |
| Remove external accounts with read permissions from your... | +15 | 1 of 1 subscriptions |
| Remove deprecated accounts from your subscription (Previe... | +10 | 1 of 1 subscriptions |
| Enable diagnostic logs in Key Vault | +5 | 3 of 3 key vaults |

Security events map

Security Center provides you with a [security alerts map](#) to help identify security threats. The **Go to security events map** button in that map opens a dashboard that allows you to view raw security events on the selected workspace.

We removed the **Go to security events map** button and the per-workspace dashboard.

Security Center - Security alerts map (Preview)

Showing subscription 'ASC DEMO'

Search (Ctrl+/
)

GENERAL

- Overview
- Getting started
- Events
- Search

POLICY & COMPLIANCE

- Coverage
- Secure score
- Security policy
- Regulatory compliance

RESOURCE SECURITY HYGIENE

- Recommendations
- Compute & apps
- IoT hubs & resources
- Networking
- Data & storage
- Identity & access (Preview)
- Security solutions

ADVANCED CLOUD DEFENSE

- Adaptive application controls
- Just in time VM access
- File Integrity Monitoring

THREAT PROTECTION

- Security alerts
- Custom alert rules (Preview)
- Security alerts map (Preview)

AUTOMATION & ORCHESTRATION

- Playbooks (Preview)

Security alerts map

This map presents security alerts that contain IP addresses targeting your resources. Markings on the map represent sources of the attack on your resources.

Go to security events map

When you select the **Go to security events map** button, it opened the (now retired) threat intelligence dashboard.

Home > Security Center - Security alerts map (Preview) > Threat intelligence dashboard

Threat intelligence dashboard

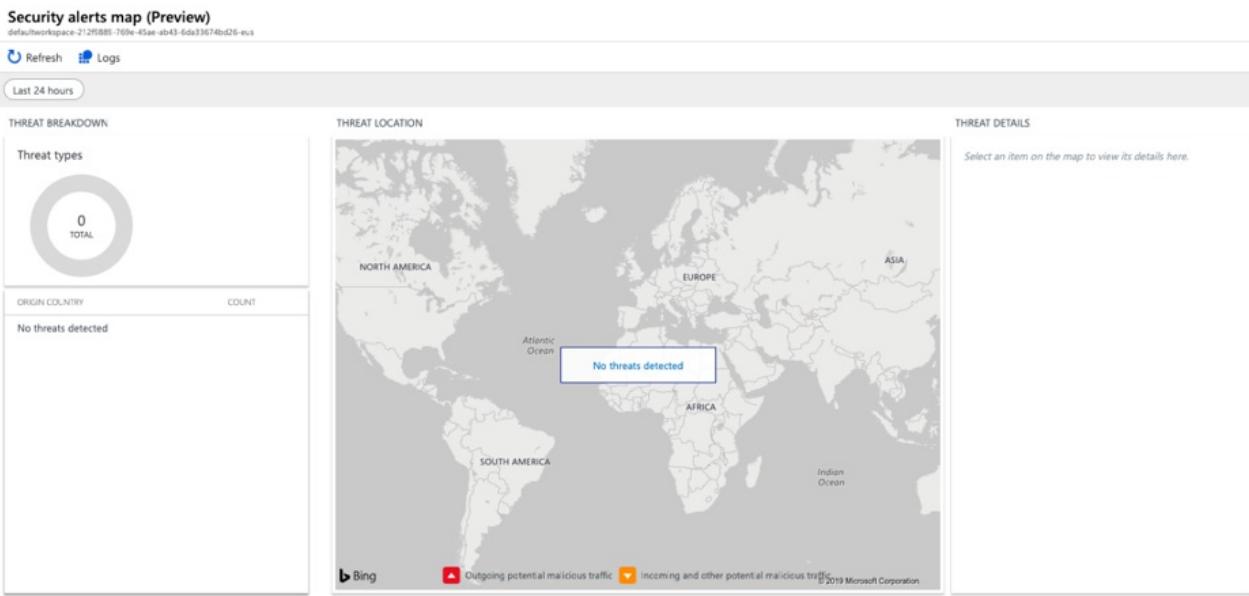
Refresh

Threat intelligence dashboard

Choose a workspace to view its threat intelligence dashboard

| WORKSPACE NAME | MALICIOUS IP | LOCATION | SUBSCRIPTION |
|---|--------------|-------------|--------------|
| defaultworkspace-212f9889-769e-45ae-ab43-6da33674bd26.... | - | East US | ASC DEMO |
| exportsecuritycenterdatatalogoworkspacetest | - | East US | ASC DEMO |
| defaultworkspace-212f9889-769e-45ae-ab43-6da33674bd26.... | - | West Europe | ASC DEMO |

When you choose a workspace to view its threat intelligence dashboard, you opened the (now retired) security alerts map (preview) screen in Log Analytics.



Your existing data remains available in the Log Analytics security solution and wasn't modified or removed.

Security events map - the new experience

We encourage you to use the alerts map functionality built into Security Center: **Security alerts map (Preview)**. This functionality provides an optimized experience and works across all subscriptions and associated workspaces. It gives you a high-level view across your environment and isn't focused on a single workspace.

Custom alert rules (Preview)

We [retired the custom alerts experience](#) on June 30, 2019 because its underlying infrastructure was retired. After the retirement date, custom security alerts are no longer generated. We recommend that you enable [Azure Sentinel](#) and re-create your custom alerts there. Alternatively, you can create your alerts with Azure Monitor log alerts.

To create custom alerts with Azure Sentinel:

1. [Open Azure Sentinel](#) and select the workspace where your custom alerts are stored
2. Select **Analytics** from the menu
3. Follow instructions in the following [tutorial](#) on how to create custom alerts in Azure Sentinel

If you're not interested in using Azure Sentinel, you can create your alerts with Azure Monitor log alerts. For instructions, see [Create, view, and manage log alerts by using Azure Monitor](#) and [Log alerts in Azure Monitor](#).

Security Center - Custom alert rules (Preview)

Showing subscription 'ASC DEMO'



| | | |
|--|---------------------------------------|-------------------------|
| <input type="text" value="Search (Ctrl+I)"/> | New custom alert rule | Refresh |
| Custom alerts is powered by Azure Monitor classic alerts, that will soon be retired. Users are advised to use other Azure services instead. Click here to learn more → | | |
| GENERAL | | |
| Overview | | |
| Getting started | | |
| Events | | |
| Search | | |
| POLICY & COMPLIANCE | | |
| Coverage | | |
| Secure score | | |
| Security policy | | |
| Regulatory compliance | | |
| RESOURCE SECURITY HYGIENE | | |
| Recommendations | | |
| Compute & apps | | |
| IoT hubs & resources | | |
| Networking | | |
| Data & storage | | |
| Identity & access (Preview) | | |
| Security solutions | | |
| ADVANCED CLOUD DEFENSE | | |
| Adaptive application controls | | |
| Just in time VM access | | |
| File Integrity Monitoring | | |
| THREAT PROTECTION | | |
| Security alerts | | |
| Custom alert rules (Preview) | | |

▼ What are custom alert rules?

▼ How do custom alert rules work?

Custom Alert Rules

3 Total

Filter items...

| ALERT NAME | DESCRIPTION | WORKSPACE | SEVERITY | ... |
|---|---|---------------------------------|----------|-----|
| SecurityBaseline | SecurityBaseline | defaultworkspace-212f9889-76... | Medium | ... |
| Login Brute Force | | defaultworkspace-212f9889-76... | Medium | ... |
| Logins from wrong subnets | Login from subnets that are not expected to send logins | defaultworkspace-212f9889-76... | Medium | ... |

For more information on custom alerts retirement, see [Custom Alert Rules in Azure Security Center \(Preview\)](#).

Security alerts investigation

The [Investigation feature](#) in Security Center helps you triage a potential security incident. The feature allows you to understand the scope of an incident and track down its root cause. We removed this feature from Security Center because it's been replaced with an improved experience in [Azure Sentinel](#).

Security incident with shared process detected

| | |
|---------------------|---|
| Description | The incident which started on 2019-04-22 16:15:55 UTC and recently detected on 2019-04-23 03:43:45 UTC indicates that an attacker has abused resource in your resource ContosoASCAAlert |
| Activity start time | Monday, April 22, 2019, 7:15:55 PM |
| Activity end time | Monday, April 22, 2019, 11:42:02 PM |
| Severity | ! High |
| State | Active |
| Attacked Resource | ContosoASCAAlert |
| Subscription | Contoso IT - demo |
| Detected by | Microsoft |
| Environment | Azure |
| Remediation Steps | <ol style="list-style-type: none"> Escalate the alert to the information security team. Review the remediation steps of each one of the alerts |

Alerts included in this incident

| DESCRIPTION | COUNT | ACTIVITY TIME | ATTACKED RESOURCE | SEVERITY |
|---|-------|--------------------|-------------------|---|
| Suspicious process executed | 4 | 04/22/19, 11:34 PM | ContosoASCAAlert | ! High |
| Suspicious command execution | 4 | 04/22/19, 11:34 PM | ContosoASCAAlert | ! High |
| Suspicious double extension file executed | 4 | 04/22/19, 11:34 PM | ContosoASCAAlert | ! High |
| Suspicious Volume Shadow Copy Activity | 4 | 04/22/19, 11:34 PM | ContosoASCAAlert | ! High |
| Antimalware Action Taken | 4 | 04/22/19, 11:42 PM | ContosoASCAAlert | ! Low |

Notable events included in this incident

| DESCRIPTION | COUNT | ACTIVITY TIME | ATTACKED RESOURCE |
|--------------------------|-------|-------------------|-------------------|
| An event log was cleared | 4 | 04/22/19, 7:15 PM | ContosoASCAAlert |

Investigate

When you select the **Investigate** button from a **Security incident** screen, you open the Investigation Dashboard (Preview) in Log Analytics. We retired the Investigation Dashboard.

Your existing data remains available in the Log Analytics security solution and wasn't modified or removed.

Investigation Dashboard (Preview)

The screenshot shows the Azure Security Center Investigation Dashboard. At the top, there's a header bar with 'Refresh' and 'Logs' buttons. Below the header, the main area has a title 'Security incident detected' with a blue circular icon. To the right of the title are three status indicators: 'Unrelated TO INCIDENT' (blue), 'High PRIORITY' (red), and 'ASC DETECTED BY' (blue). On the far right, a vertical sidebar lists navigation options: 'Entities' (selected), 'Search', 'Exploration', 'Playbooks', 'Comments', and 'Audit'. The main content area includes a timeline selector for '4/2/2019 4:30 PM — 4/3/2019 4:30 PM (1 day)'. On the left, there's a large circular diagram with '130 alerts' and a central 'Security incident detected' icon. The right side contains two sections: 'General Information' (with fields like DESCRIPTION, ALERT ID, TIME GENERATED, etc.) and 'Remediation Steps' (with steps 1 and 2).

Investigation - the new experience

We encourage you to transition to [Azure Sentinel](#) for a rich investigation experience. Azure Sentinel provides powerful search and query tools to hunt for security threats across your organization's data sources.

Subset of security solutions

Security Center can enable [integrated security solutions in Azure](#). We retired the following partner solutions from Security Center. These solutions are enabled in [Azure Sentinel](#) along with a number of additional data sources.

- [Next generation firewall and web application firewall solutions](#)
- [Integration of security solutions that support the Common Event Format \(CEF\)](#)
- [Microsoft Advanced Threat Analytics](#)
- [Azure AD Identity Protection](#)

After retirement, you cannot add or modify any of the solution types mentioned in the preceding list, either from the UI or the API. Azure Security Center will no longer discover any new instances of these partner solutions.

If you have existing connected solutions, we encourage you to move to Azure Sentinel.

Security Center - Security solutions

Showing subscription 'Rome (LDC - Detection E2E Tests Prod)'

Filter

GENERAL

- Overview
- Getting started
- Events
- Search

POLICY & COMPLIANCE

- Coverage
- Secure score
- Security policy
- Regulatory compliance

RESOURCE SECURITY HYGIENE

- Recommendations
- Compute & apps
- IoT hubs & resources
- Networking
- Data & storage
- Identity & access (Preview)
- Security solutions

ADVANCED CLOUD DEFENSE

- Adaptive application controls
- Just in time VM access
- File Integrity Monitoring

THREAT PROTECTION

- Security alerts
- Custom alert rules (Preview)
- Security alerts map (Preview)

AUTOMATION & ORCHESTRATION

- Playbooks (Preview)

Connected solutions

Partner security solutions were not connected yet

View all security solutions currently connected to Azure Security Center, monitor the health of solutions, and access the solutions' management tools for advanced configuration.

To learn more [go to documentation](#)



Add data sources (7)

Connect your security solution to Azure Security Center.

Non-Azure servers

MICROSOFT

Onboard your non-Azure computers to Azure Security Center and gain security assessment, recommendations and more powerful features

ADD

SIEM

SELECTED SIEMS

Integrate Azure Security Center alerts into SIEM for a central monitoring. See the list of supported SIEMS

ADD

Web Application Firewall

SELECTED SOLUTIONS

Deploy a supported WAF solution to protect your web applications. It will also enable you to get alerts generated by the solution shown and enriched in the Azure Security Center alerts queue

ADD

Next Generation Firewall

SELECTED SOLUTIONS

Deploy a supported NGFW solution to protect your virtual machines. It will also enable you to get alerts generated by the solution shown and enriched in the Azure Security Center alerts queue

ADD

Advanced Threat Analytics

MICROSOFT

Integrate Microsoft Advanced Threat Analytics suspicious activities along with other detections in your environment, and gain correlations and otherwise undetectable

ADD

Azure AD Identity Protec...

MICROSOFT

Integrate Microsoft Azure AD Identity Protection alerts along with other detections in your environment, gain fusion detection and otherwise undetectable attacks

ADD

Common Event Format

ANY PUBLISHER

Integrate any security solution that support Common Event Format (CEF), take advantage of Search & Custom Alert Rules, and Threat Intelligence enrichment for each log

Edit security configurations for security policies

Azure Security Center monitors security configurations by applying a set of [over 150 recommended rules](#) for hardening the OS. These rules pertain to firewalls, auditing, password policies, and more. If a machine is found to have a vulnerable configuration, Security Center generates a security recommendation. The [Edit security configuration screen](#) allows customers to customize the default OS security configuration in Security Center.

We retired this preview feature. To reset your security configurations back to their default values after the retirement date, do so via the API or Powershell using the [following instructions](#).

Settings - Edit security configurations

ASC DEMO

Save Discard Reset

View and modify the OS configurations that are **assessed** by Security Center to identify potential security vulnerabilities.



- This policy will not modify the machines' configuration.
- This policy will be stored under all workspaces under the selected subscription.
- This policy will apply to all machines connected to these workspaces.

[Go to documentation for additional information](#)

Step 1: Download OS Security Configuration file

[Download file](#)

Step 2: Edit OS Security Configuration file according to documentation

Step 3: Select the modified configuration file to upload

Select a file

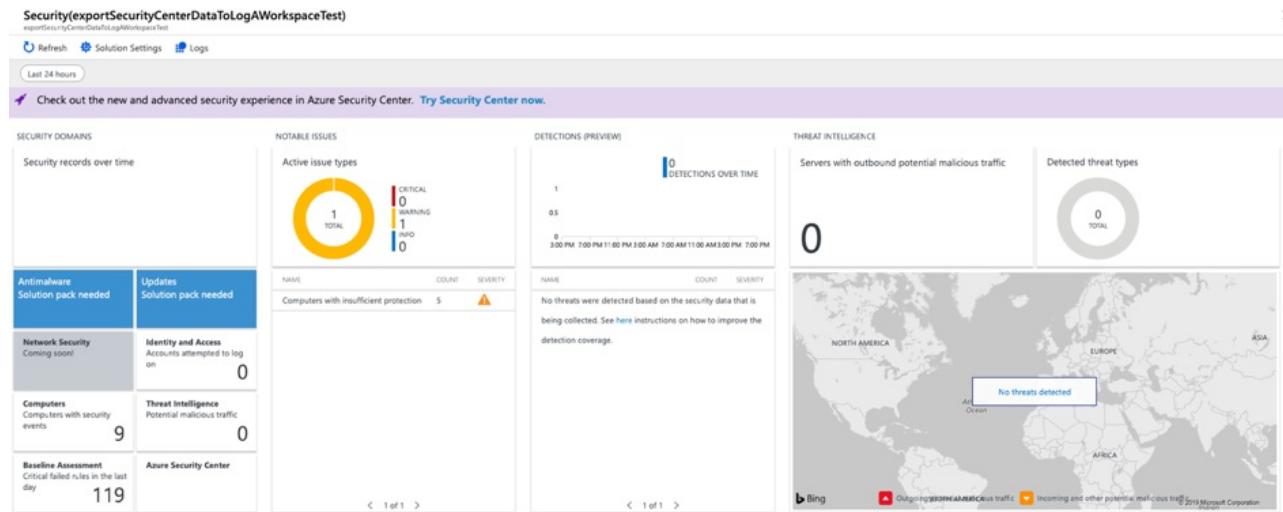
Step 4: Click Save to apply changes or Reset to restore default configuration

Edit security configurations - the new experience

We intend to enable Security Center to support the [Guest configuration agent](#). Such an update will allow a much richer feature set, including support for more operating systems and integration of Azure in-guest policies for guest configurations. After these changes are enabled, you'll also have the ability to control configurations at scale and apply them to new resources automatically.

Security and audit dashboard for Log Analytics workspaces

The security and audit dashboard was originally used in the OMS portal. In Log Analytics, the dashboard provides a per-workspace overview of notable security events and threats, a threat intelligence map, and an identity-and-access assessment of security events saved in the workspace. We removed the dashboard. As we already recommended in the dashboard UI, we advise you to transition to Azure Security Center.



Security and audit dashboard - the new experience

We advise you to switch to Azure Security Center. It provides the same security overview across multiple subscriptions and the workspaces associated with them, plus a richer feature set.

You can get the original Log Analytics queries that populate the security and audit dashboard in the [GitHub repository](#) for Security Center.

Next steps

- Learn more about [Azure Security Center](#).
- Learn more about [Azure Sentinel](#).

Endpoint protection assessment and recommendations in Azure Security Center

12/30/2019 • 3 minutes to read • [Edit Online](#)

Azure Security Center provides health assessments of [supported](#) versions of Endpoint protection solutions. This article explains the scenarios that lead Security Center to generate the following two recommendations:

- **Install endpoint protection solutions on your virtual machine**
- **Resolve endpoint protection health issues on your machines**

Windows Defender

- Security Center recommends you "**Install endpoint protection solutions on virtual machine**" when `Get-MpComputerStatus` runs and the result is **AMServiceEnabled: False**
- Security Center recommends you "**Resolve endpoint protection health issues on your machines**" when `Get-MpComputerStatus` runs and any of the following occurs:
 - Any of the following properties are false:
AMServiceEnabled
AntispywareEnabled
RealTimeProtectionEnabled
BehaviorMonitorEnabled
IoavProtectionEnabled
OnAccessProtectionEnabled
 - If one or both of the following properties are 7 or more.
AntispywareSignatureAge
AntivirusSignatureAge

Microsoft System Center endpoint protection

- Security Center recommends you "**Install endpoint protection solutions on virtual machine**" when importing **SCEPMpModule ("\$env:ProgramFiles\Microsoft Security Client\MpProvider\MpProvider.psd1")** and running `Get-MProtComputerStatus` results with **AMServiceEnabled = false**
- Security Center recommends you "**Resolve endpoint protection health issues on your machines**" when `Get-MprotComputerStatus` runs and any of the following occurs:
 - At least one of the following properties is false:

```
**AMServiceEnabled**  
  
**AntispywareEnabled**  
  
**RealTimeProtectionEnabled**  
  
**BehaviorMonitorEnabled**  
  
**IoavProtectionEnabled**  
  
**OnAccessProtectionEnabled**
```

- If one or both of the following Signature Updates is greater or equal to 7.

```
**AntispywareSignatureAge**  
  
**AntivirusSignatureAge**
```

Trend Micro

- Security Center recommends you "**Install endpoint protection solutions on virtual machine**" when any of the following checks aren't met:
 - **HKLM:\SOFTWARE\TrendMicro\Deep Security Agent** exists
 - **HKLM:\SOFTWARE\TrendMicro\Deep Security Agent\InstallationFolder** exists
 - The **dsa_query.cmd** file is found in the Installation Folder
 - Running **dsa_query.cmd** results with **Component.AM.mode: on - Trend Micro Deep Security Agent detected**

Symantec endpoint protection

Security Center recommends you "**Install endpoint protection solutions on virtual machine**" when any of the following checks aren't met:

- **HKLM:\Software\Symantec\Symantec Endpoint Protection\CurrentVersion\PRODUCTNAME = "Symantec Endpoint Protection"**
- **HKLM:\Software\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate\ASRunningStatus = 1**

Or

- **HKLM:\Software\Wow6432Node\Symantec\Symantec Endpoint Protection\CurrentVersion\PRODUCTNAME = "Symantec Endpoint Protection"**
- **HKLM:\Software\Wow6432Node\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate\ASRunningStatus = 1**

Security Center recommends you "**Resolve endpoint protection health issues on your machines**" when any of the following checks aren't met:

- Check Symantec Version >= 12: Registry location: **HKLM:\Software\Symantec\Symantec Endpoint Protection\CurrentVersion** -Value "**PRODUCTVERSION**"
- Check Real Time Protection status: **HKLM:\Software\Wow6432Node\Symantec\Symantec Endpoint Protection\AV\Storages\Filesystem\RealTimeScan\OnOff == 1**
- Check Signature Update status: **HKLM\Software\Symantec\Symantec Endpoint**

Protection\CurrentVersion\public-opstate\LatestVirusDefsDate <= 7 days

- Check Full Scan status: **HKLM:\Software\Symantec\Symantec Endpoint Protection\CurrentVersion\public-opstate\LastSuccessfulScanDateTime <= 7 days**
- Find signature version number Path to signature version for Symantec 12: **Registry Paths+ "CurrentVersion\SharedDefs" -Value "SRTSP"**
- Path to signature version for Symantec 14: **Registry Paths+ "CurrentVersion\SharedDefs\SDSDefs" -Value "SRTSP"**

Registry Paths:

- "**HKLM:\Software\Symantec\Symantec Endpoint Protection**" + \$Path;
- "**HKLM:\Software\Wow6432Node\Symantec\Symantec Endpoint Protection**" + \$Path

McAfee endpoint protection for Windows

Security Center recommends you "**Install endpoint protection solutions on virtual machine**" when any of the following checks aren't met:

- **HKLM:\SOFTWARE\McAfee\Endpoint\AV\ProductVersion** exists
- **HKLM:\SOFTWARE\McAfee\AVSolution\MCSHIELDGLOBAL\GLOBAL\enableoas = 1**

Security Center recommends you "**Resolve endpoint protection health issues on your machines**" when any of the following checks aren't met:

- McAfee Version: **HKLM:\SOFTWARE\McAfee\Endpoint\AV\ProductVersion >= 10**
- Find Signature Version: **HKLM:\Software\McAfee\AVSolution\DS\DS -Value "dwContentMajorVersion"**
- Find Signature date: **HKLM:\Software\McAfee\AVSolution\DS\DS -Value "szContentCreationDate" >= 7 days**
- Find Scan date: **HKLM:\Software\McAfee\Endpoint\AV\ODS -Value "LastFullScanOdsRunTime" >= 7 days**

McAfee Endpoint Security for Linux Threat Prevention

Security Center recommends you "**Install endpoint protection solutions on virtual machine**" when any of the following checks aren't met:

- File **/opt/isec/ens/threatprevention/bin/isecav** exits
- "**/opt/isec/ens/threatprevention/bin/isecav --version**" output is: **McAfee name = McAfee Endpoint Security for Linux Threat Prevention and McAfee version >= 10**

Security Center recommends you "**Resolve endpoint protection health issues on your machines**" when any of the following checks aren't met:

- "**/opt/isec/ens/threatprevention/bin/isecav --listtask**" returns **Quick scan, Full scan** and both of the scans <= 7 days
- "**/opt/isec/ens/threatprevention/bin/isecav --listtask**" returns **DAT and engine Update time** and both of them <= 7 days
- "**/opt/isec/ens/threatprevention/bin/isecav --getoasconfig --summary**" returns **On Access Scan** status

Sophos Antivirus for Linux

Security Center recommends you "**Install endpoint protection solutions on virtual machine**" when any of the following checks aren't met:

- File **/opt/sophos-av/bin/savdstatus** exists or search for customized location "**readlink \$(which savscan)**"
- "**/opt/sophos-av/bin/savdstatus --version**" returns Sophos name = **Sophos Anti-Virus and Sophos version >= 9**

Security Center recommends you "**Resolve endpoint protection health issues on your machines**" when any of the following checks aren't met:

- "**/opt/sophos-av/bin/savlog --maxage=7 | grep -i "Scheduled scan .* completed" | tail -1**", returns a value
- "**/opt/sophos-av/bin/savlog --maxage=7 | grep "scan finished"** | tail -1", returns a value
- "**/opt/sophos-av/bin/savdstatus --lastupdate**" returns lastUpdate, which should be <= 7 days
- "**/opt/sophos-av/bin/savdstatus -v**" is equal to "**On-access scanning is running**"
- "**/opt/sophos-av/bin/savconfig get LiveProtection**" returns enabled

Troubleshoot and support

Troubleshoot

Microsoft Antimalware extension logs are available at:

%Systemdrive%\WindowsAzure\Logs\Plugins\Microsoft.Azure.Security.IaaSAntimalware(Or PaaSAntimalware)\1.5.5.x(version#)\CommandExecution.log

Support

For more help, contact the Azure experts on the [MSDN Azure and Stack Overflow forums](#). Or file an Azure support incident. Go to the [Azure support site](#) and select Get support. For information about using Azure Support, read the [Microsoft Azure support FAQ](#).

Manage user data in Azure Security Center

1/14/2020 • 3 minutes to read • [Edit Online](#)

This article provides information about how you can manage the user data in Azure Security Center. Managing user data includes the ability to access, delete, or export data.

NOTE

This article provides steps for how to delete personal data from the device or service and can be used to support your obligations under the GDPR. If you're looking for general info about GDPR, see the [GDPR section of the Service Trust portal](#).

A Security Center user assigned the role of Reader, Owner, Contributor, or Account Administrator can access customer data within the tool. To learn more about the Account Administrator role, see [Built-in roles for Azure role-based access control](#) to learn more about the Reader, Owner, and Contributor roles. See [Azure subscription administrators](#).

Searching for and identifying personal data

A Security Center user can view their personal data through the Azure portal. Security Center only stores security contact details such as email addresses and phone numbers. For more information, see [Provide security contact details in Azure Security Center](#).

In the Azure portal, a user can view allowed IP configurations using Security Center's just-in-time VM access feature. For more information, see [Manage virtual machine access using just-in-time](#).

In the Azure portal, a user can view security alerts provided by Security Center including IP addresses and attacker details. For more information, see [Managing and responding to security alerts in Azure Security Center](#).

Classifying personal data

You don't need to classify personal data found in Security Center's security contact feature. The data saved is an email address (or multiple email addresses) and a phone number. [Contact data](#) is validated by Security Center.

You don't need to classify the IP addresses and port numbers saved by Security Center's [just-in-time](#) feature.

Only a user assigned the role of Administrator can classify personal data by [viewing alerts](#) in Security Center.

Securing and controlling access to personal data

A Security Center user assigned the role of Reader, Owner, Contributor, or Account Administrator can access [security contact data](#).

A Security Center user assigned the role of Reader, Owner, Contributor, or Account Administrator can access their [just-in-time](#) policies.

A Security Center user assigned the role of Reader, Owner, Contributor, or Account Administrator can view their [alerts](#).

Updating personal data

A Security Center user assigned the role of Owner, Contributor, or Account Administrator can update [security contact data](#) via the Azure portal.

A Security Center user assigned the role of Owner, Contributor, or Account Administrator can update their [just-in-time policies](#).

An Account Administrator can't edit alert incidents. An [alert incident](#) is considered security data and is read only.

Deleting personal data

A Security Center user assigned the role of Owner, Contributor, or Account Administrator can delete [security contact data](#) via the Azure portal.

A Security Center user assigned the role of Owner, Contributor, or Account Administrator can delete the [just-in-time policies](#) via the Azure portal.

A Security Center user can't delete alert incidents. For security reasons, an [alert incident](#) is considered read-only data.

Exporting personal data

A Security Center user assigned the role of Reader, Owner, Contributor, or Account Administrator can export [security contact data](#) by:

- Copying from the Azure portal
- Executing the Azure REST API call, GET HTTP:

```
GET https://<endpoint>/subscriptions/{subscriptionId}/providers/Microsoft.Security/securityContacts?api-version={api-version}
```

A Security Center user assigned the role of Account Administrator can export the [just-in-time policies](#) containing the IP addresses by:

- Copying from the Azure portal
- Executing the Azure REST API call, GET HTTP:

```
GET  
https://<endpoint>/subscriptions/{subscriptionId}/resourceGroups/{resourceGroup}/providers/Microsoft.Security/locations/{location}/jitNetworkAccessPolicies/default?api-version={api-version}
```

An Account Administrator can export the alert details by:

- Copying from the Azure portal
- Executing the Azure REST API call, GET HTTP:

```
GET https://<endpoint>/subscriptions/{subscriptionId}/providers/microsoft.Security/alerts?api-version={api-version}
```

For more information, see [Get Security Alerts \(GET Collection\)](#).

Restricting the use of personal data for profiling or marketing without consent

A Security Center user can choose to opt out by deleting their [security contact data](#).

[Just-in-time data](#) is considered non-identifiable data and is retained for a period of 30 days.

[Alert data](#) is considered security data and is retained for a period of two years.

Auditing and reporting

Audit logs of security contact, just-in-time, and alert updates are maintained in [Azure Activity Logs](#).

Next steps

For more information about managing user data, see [Manage user data found in an Azure Security Center investigation](#).

Azure Security Center Readiness Roadmap

1/20/2020 • 2 minutes to read • [Edit Online](#)

This document provides you a readiness roadmap that will assist you to get started with Azure Security Center.

Understanding Security Center

Azure Security Center provides unified security management and advanced threat protection for workloads running in Azure, on-premises, and in other clouds.

Use the following resources to get started with Security Center.

Articles

- [Introduction to Azure Security Center](#)
- [Azure Security Center quickstart guide](#)

Videos

- [Quick Introduction Video](#)
- [Overview of Security Center Prevention, Detection and Response Capabilities](#)

Planning and operations

To take full advantage of Security Center, it is important to understand how different individuals or teams in your organization use the service to meet secure operations, monitoring, governance, and incident response needs.

Use the following resources to assist you during the planning and operations processes.

Article

- [Azure Security Center planning and operations guide](#)

Video

- [Hybrid cloud workload protection with Security Center](#)

Onboarding computers to Security Center

Security Center automatically detects any Azure subscriptions or workspaces not enabled for Security Center Standard. This includes Azure subscriptions using Security Center Free and workspaces that do not have the Security solution enabled.

Use the following resources to assist you during the onboarding processes.

Article

- [Onboarding to Azure Security Center Standard for enhanced security](#)

Video

- [Azure Security Center Hybrid - Overview](#)

Mitigating security issues using Security Center

Security Center automatically collects, analyzes, and integrates log data from your Azure resources, the network,

and connected partner solutions, like firewall and endpoint protection solutions, to detect real threats and reduce false positives.

Use the following resources to assist you to manage security alerts and protect your resources.

Articles

- [Security health monitoring in Azure Security Center](#)
- [Protecting your machines and applications in Azure Security Center](#)
- [Protecting your network in Azure Security Center](#)
- [Protecting Azure SQL service and data in Azure Security Center](#)

Video

- [Mitigating Security Issues using Azure Security Center](#)

Security Center for incident response

To reduce costs and damage, it's important to have an incident response plan in place before an attack takes place. You can use Azure Security Center in different stages of an incident response.

Use the following resources to understand how Security Center can be incorporated in your incident response process.

Videos

- [Azure Security Center in Incident Response](#)
- [Respond quickly to threats with next-generation security operation, and investigation](#)

Articles

- [Using Azure Security Center for an incident response](#)
- [Automate response with Workflow Automation](#)

Advanced cloud defense

Azure VMs can take advantage of advanced cloud defense capabilities in Security Center. These capabilities include just-in-time virtual machine (VM) access, and adaptive application controls.

Use the following resources to learn how to use these capabilities in Security Center.

Videos

- [Azure Security Center – Just-in-time VM Access](#)
- [Azure Security Center - Adaptive Application Controls](#)

Articles

- [Manage virtual machine access using just-in-time](#)
- [Adaptive Application Controls in Azure Security Center](#)

Hands-on activities

- [Security Center hands-on lab](#)
- [Web Application Firewall \(WAF\) recommendation playbook in Security Center](#)
- [Azure Security Center Playbook: Security Alerts](#)

Additional resources

- [Security Center Documentation Page](#)
- [Security Center REST API Documentation Page](#)
- [Azure Security Center frequently asked questions \(FAQ\)](#)
- [Security Center Pricing Page](#)
- [Identity security best practices](#)
- [Network security best practices](#)
- [PaaS recommendations](#)
- [Compliance](#)
- [Log analytics customers can now use Azure Security Center to protect their hybrid cloud workloads](#)

Community Resources

- [Security Center UserVoice](#)
- [Security Center community forum](#)

Azure Security Center Troubleshooting Guide

2/25/2020 • 9 minutes to read • [Edit Online](#)

This guide is for information technology (IT) professionals, information security analysts, and cloud administrators whose organizations are using Azure Security Center and need to troubleshoot Security Center related issues.

Security Center uses the Microsoft Monitoring Agent to collect and store data. See [Azure Security Center Platform Migration](#) to learn more. The information in this article represents Security Center functionality after transition to the Microsoft Monitoring Agent.

Troubleshooting guide

This guide explains how to troubleshoot Security Center related issues.

Alert types:

- Virtual Machine Behavioral Analysis (VMBA)
- Network Analysis
- SQL Database and SQL Data Warehouse Analysis
- Contextual Information

Depending on the alert types, customers can gather the necessary information to investigate the alert by using the following resources:

- Security logs in the Virtual Machine (VM) event viewer in Windows
- AuditD in Linux
- The Azure activity logs, and the enable diagnostic logs on the attack resource.

For some alerts we also have a confidence score. The confidence score in **Security Center** can help your team triage and prioritize alerts. **Security Center** automatically applies industry best practices, intelligent algorithms, and processes used by analysts to determine whether a threat is legitimate and provides meaningful insights in the form of a confidence score.

Customers can share feedback for the alert description and relevance. Navigate to the alert itself, select the **Was This Useful** button, select the reason, and then enter a comment to explain which explains the feedback. We consistently monitor this feedback channel to improve our alerts.

Audit log

Most of the troubleshooting done in Security Center takes place by first looking at the [Audit Log](#) records for the failed component. Through audit logs, you can determine:

- Which operations were taken place
- Who initiated the operation
- When the operation occurred
- The status of the operation
- The values of other properties that might help you research the operation

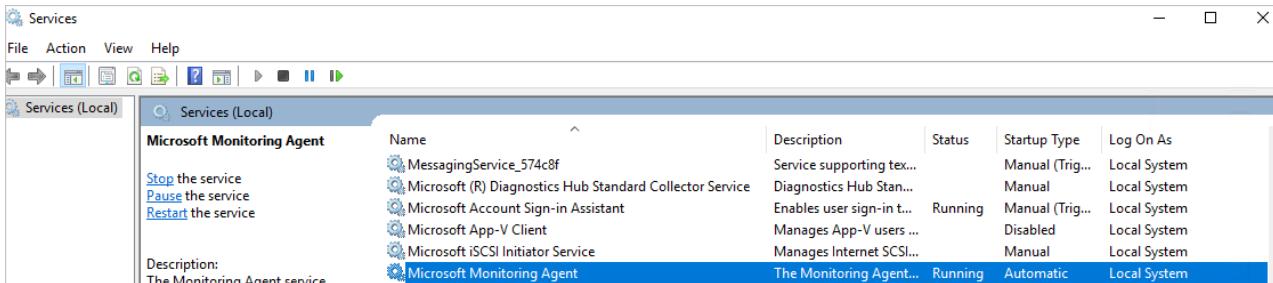
The audit log contains all write operations (PUT, POST, DELETE) performed on your resources, however it does not include read operations (GET).

Microsoft Monitoring Agent

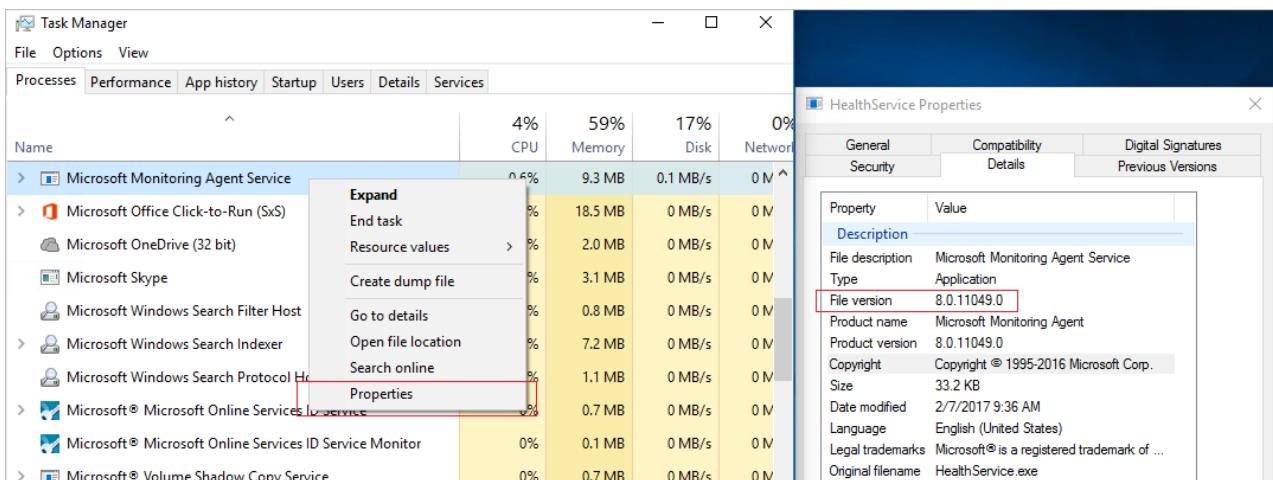
Security Center uses the Microsoft Monitoring Agent – this is the same agent used by the Azure Monitor service – to collect security data from your Azure virtual machines. After data collection is enabled and the agent is correctly installed in the target machine, the process below should be in execution:

- HealthService.exe

If you open the services management console (services.msc), you will also see the Microsoft Monitoring Agent service running as shown below:



To see which version of the agent you have, open **Task Manager**, in the **Processes** tab locate the **Microsoft Monitoring Agent Service**, right-click on it and click **Properties**. In the **Details** tab, look the file version as shown below:



Microsoft Monitoring Agent installation scenarios

There are two installation scenarios that can produce different results when installing the Microsoft Monitoring Agent on your computer. The supported scenarios are:

- **Agent installed automatically by Security Center:** in this scenario you will be able to view the alerts in both locations, Security Center and Log search. You will receive email notifications to the email address that was configured in the security policy for the subscription the resource belongs to.
- **Agent manually installed on a VM located in Azure:** in this scenario, if you are using agents downloaded and installed manually prior to February 2017, you can view the alerts in the Security Center portal only if you filter on the subscription the workspace belongs to. If you filter on the subscription the resource belongs to, you won't see any alerts. You'll receive email notifications to the email address that was configured in the security policy for the subscription the workspace belongs to.

NOTE

To avoid the behavior explained in the second scenario, make sure you download the latest version of the agent.

Monitoring agent health issues

Monitoring state defines the reason Security Center is unable to successfully monitor VMs and computers initialized for automatic provisioning. The following table shows the **Monitoring state** values, descriptions, and resolution steps.

| MONITORING STATE | DESCRIPTION | RESOLUTION STEPS |
|---|--|--|
| Pending agent installation | The Microsoft Monitoring Agent installation is still running. Installation can take up to a few hours. | Wait until automatic installation is complete. |
| Power state off | The VM is stopped. The Microsoft Monitoring Agent can only be installed on a VM that is running. | Restart the VM. |
| Missing or invalid Azure VM agent | The Microsoft Monitoring Agent is not installed yet. For Security Center to install the extension a valid Azure VM agent is required. | Install, reinstall or upgrade the Azure VM agent on the VM. |
| VM state not ready for installation | The Microsoft Monitoring Agent is not installed yet because the VM is not ready for installation. The VM is not ready for installation due to a problem with the VM agent or VM provisioning. | Check the status of your VM. Return to Virtual Machines in the portal and select the VM for status information. |
| Installation failed - general error | The Microsoft Monitoring Agent was installed but failed due to an error. | Manually install the extension or uninstall the extension so Security Center will try to install again. |
| Installation failed - local agent already installed | Microsoft Monitoring Agent install failed. Security Center identified a local agent (Log Analytics or System Center Operations Manager) already installed on the VM. To avoid multi-homing configuration, where the VM is reporting to two separate workspaces, the Microsoft Monitoring Agent installation stopped. | There are two ways to resolve: manually install the extension and connect it to your desired workspace. Or, set your desired workspace as your default workspace and enable automatic provisioning of the agent. See enable automatic provisioning . |
| Agent cannot connect to workspace | Microsoft Monitoring Agent installed but failed due to network connectivity. Check that there is internet access or that a valid HTTP proxy has been configured for the agent. | See monitoring agent network requirements. |

| MONITORING STATE | DESCRIPTION | RESOLUTION STEPS |
|---|---|---|
| Agent connected to missing or unknown workspace | Security Center identified that the Microsoft Monitoring Agent installed on the VM is connected to a workspace which it doesn't have access to. | This can happen in two cases. The workspace was deleted and no longer exists. Reinstall the agent with the correct workspace or uninstall the agent and allow Security Center to complete its automatic provisioning installation. The second case is where the workspace is part of a subscription that Security Center does not have permissions to. Security Center requires subscriptions to allow the Microsoft Security Resource Provider to access them. To enable, register the subscription to the Microsoft Security Resource Provider. This can be done by API, PowerShell, portal or by simply filtering on the subscription in the Security Center Overview dashboard. See Resource providers and types for more information. |
| Agent not responsive or missing ID | Security Center is unable to retrieve security data scanned from the VM, even though the agent is installed. | The agent is not reporting any data, including heartbeat. The agent might be damaged or something is blocking traffic. Or, the agent is reporting data but is missing an Azure resource ID so it's impossible to match the data to the Azure VM. To troubleshoot Linux, see Troubleshooting Guide for Log Analytics Agent for Linux . To troubleshoot Windows, see Troubleshooting Windows Virtual Machines . |
| Agent not installed | Data collection is disabled. | Turn on data collection in the security policy or manually install the Microsoft Monitoring Agent. |

Troubleshooting monitoring agent network requirements

For agents to connect to and register with Security Center, they must have access to network resources, including the port numbers and domain URLs.

- For proxy servers, you need to ensure that the appropriate proxy server resources are configured in agent settings. Read this article for more information on [how to change the proxy settings](#).
- For firewalls that restrict access to the Internet, you need to configure your firewall to permit access to Log Analytics. No action is needed in agent settings.

The following table shows resources needed for communication.

| AGENT RESOURCE | PORTS | BYPASS HTTPS INSPECTION |
|----------------------------|-------|-------------------------|
| *.ods.opinsights.azure.com | 443 | Yes |
| *.oms.opinsights.azure.com | 443 | Yes |
| *.blob.core.windows.net | 443 | Yes |

| AGENT RESOURCE | PORTS | BYPASS HTTPS INSPECTION |
|------------------------|-------|-------------------------|
| *.azure-automation.net | 443 | Yes |

If you encounter onboarding issues with the agent, make sure to read the article [How to troubleshoot Operations Management Suite onboarding issues](#).

Troubleshooting endpoint protection not working properly

The guest agent is the parent process of everything the [Microsoft Antimalware](#) extension does. When the guest agent process fails, the Microsoft Antimalware that runs as a child process of the guest agent may also fail. In scenarios like that is recommended to verify the following options:

- If the target VM is a custom image and the creator of the VM never installed guest agent.
- If the target is a Linux VM instead of a Windows VM then installing the Windows version of the antimalware extension on a Linux VM will fail. The Linux guest agent has specific requirements in terms of OS version and required packages, and if those requirements are not met the VM agent will not work there either.
- If the VM was created with an old version of guest agent. If it was, you should be aware that some old agents could not auto-update itself to the newer version and this could lead to this problem. Always use the latest version of guest agent if creating your own images.
- Some third-party administration software may disable the guest agent, or block access to certain file locations. If you have third-party installed on your VM, make sure that the agent is on the exclusion list.
- Certain firewall settings or Network Security Group (NSG) may block network traffic to and from guest agent.
- Certain Access Control List (ACL) may prevent disk access.
- Lack of disk space can block the guest agent from functioning properly.

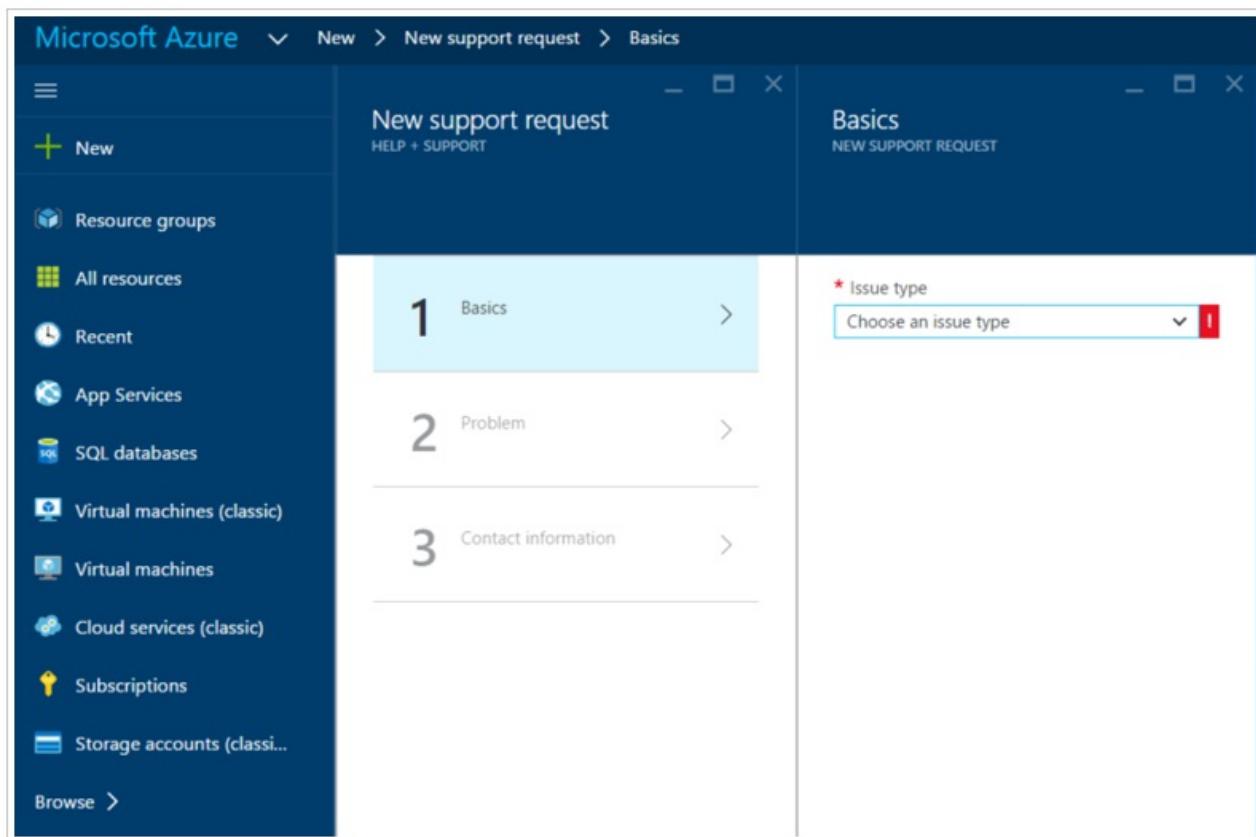
By default the Microsoft Antimalware User Interface is disabled, read [Enabling Microsoft Antimalware User Interface on Azure Resource Manager VMs Post Deployment](#) for more information on how to enable it if you need.

Troubleshooting problems loading the dashboard

If you experience issues loading the Security Center dashboard, ensure that the user that registers the subscription to Security Center (i.e. the first user one who opened Security Center with the subscription) and the user who would like to turn on data collection should be *Owner* or *Contributor* on the subscription. From that moment on also users with *Reader* on the subscription can see the dashboard/alerts/recommendation/policy.

Contacting Microsoft Support

Some issues can be identified using the guidelines provided in this article, others you can also find documented at the Security Center public [Forum](#). However if you need further troubleshooting, you can open a new support request using **Azure portal** as shown below:



See also

In this document, you learned how to configure security policies in Azure Security Center. To learn more about Azure Security Center, see the following:

- [Azure Security Center Planning and Operations Guide](#) — Learn how to plan and understand the design considerations to adopt Azure Security Center.
- [Security health monitoring in Azure Security Center](#) — Learn how to monitor the health of your Azure resources
- [Managing and responding to security alerts in Azure Security Center](#) — Learn how to manage and respond to security alerts
- [Understanding security alerts in Azure Security Center](#)
- [Tutorial: Respond to security incidents](#)
- [Alerts Validation in Azure Security Center](#)
- [Email Notifications in Azure Security Center](#)
- [Handling Security Incidents in Azure Security Center](#)
- [Alert confidence score](#)
- [Investigate Incidents and Alerts in Azure Security Center](#)
- [Azure Security Center detection capabilities](#)
- [Monitoring partner solutions with Azure Security Center](#) — Learn how to monitor the health status of your partner solutions.
- [Azure Security Center FAQ](#) — Find frequently asked questions about using the service
- [Azure Security Blog](#) — Find blog posts about Azure security and compliance