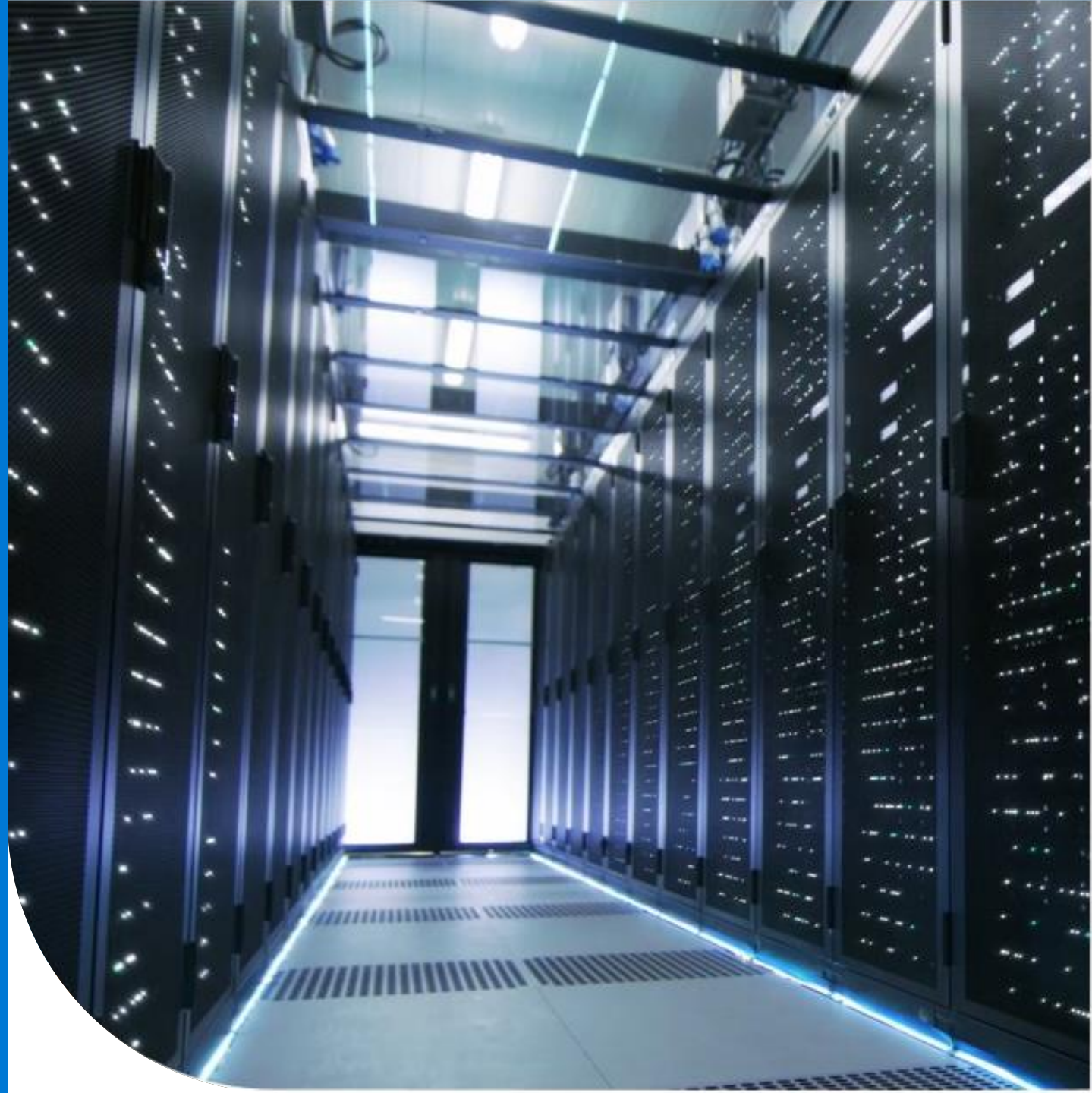


Planning for Microsoft Defender for Cloud

Nick Blackman

Senior Cloud Solutions Architect
US Global Partner Solutions



Microsoft Defender for Cloud

Microsoft Defender for Cloud

- Strengthens the security posture of your cloud resources
- Protects workloads running in Azure, hybrid, and other cloud platforms



Continuously Assess

Know your security posture.
Identify and track
vulnerabilities.



Secure

Harden resources and
services with
Azure Security Benchmark.



Defend

Detect and resolve threats to
resources, workloads, and
services.

Planning for Microsoft Defender for Cloud

The key areas to consider when planning to use Defender for Cloud are as follows:

- **Security Roles and Access Controls**
- **Security Policies and Recommendations**
- **Data Collection and Storage**
- **Onboarding non-Azure resources**
- **Ongoing Security Monitoring**
- **Incident Response**

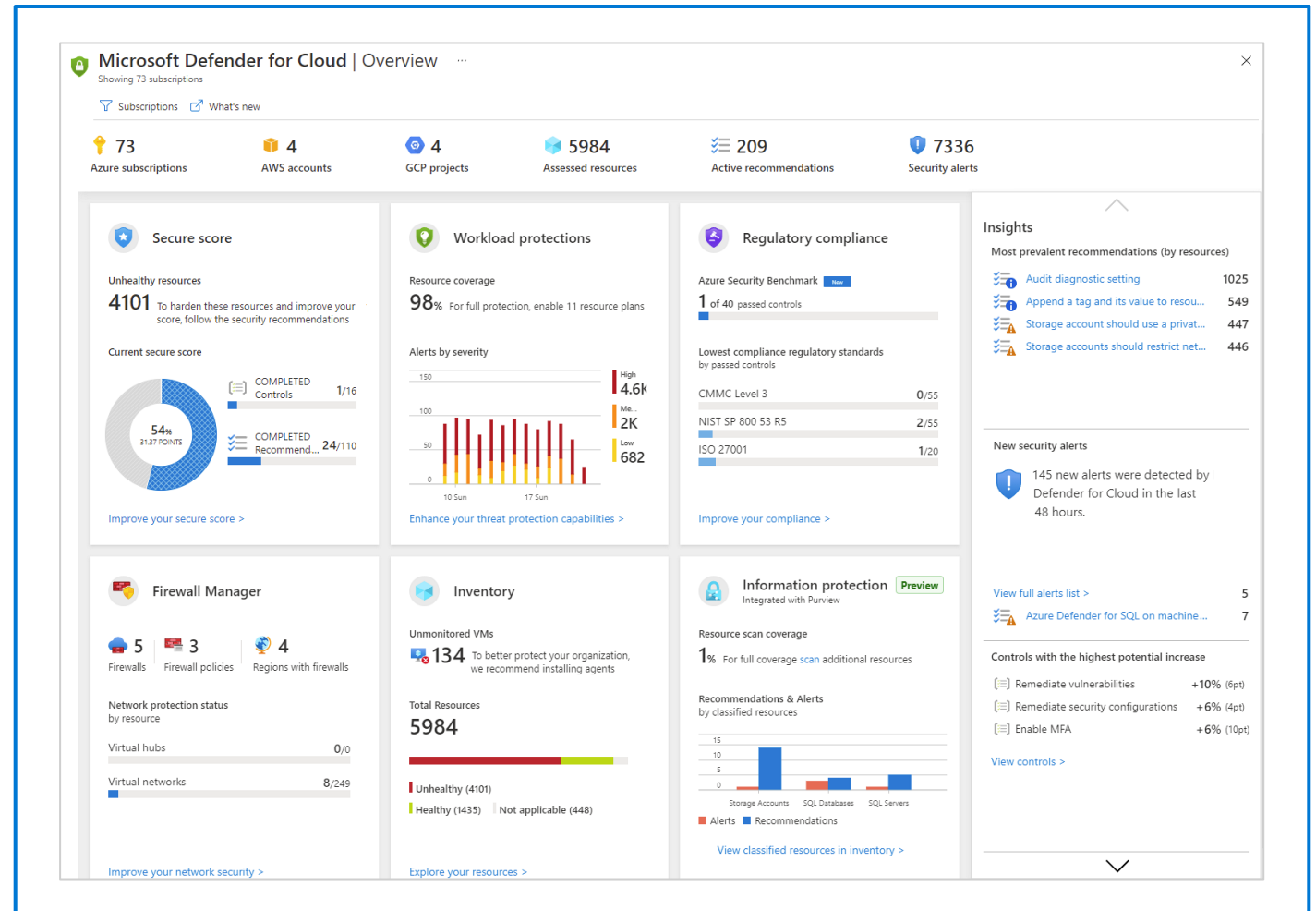


Enabling Microsoft Defender for Cloud on your Azure subscription

Sign into the Azure portal



From the portal's menu,
select **Microsoft Defender for Cloud**



Microsoft Defender for Cloud pricing

When you enable Microsoft Defender for Cloud, we automatically enroll and start protecting all your resources unless you explicitly decide to opt-out.

For any resource that is protected by Defender for Cloud, you will be charged per the pricing model below.

Microsoft Defender for Cloud is free for the first 30 days.

Any usage beyond 30 days will be automatically charged as per the pricing model.

Resource Type	Price
Microsoft Defender for Servers Plan 1	\$0.007/Server/hour
Microsoft Defender for Servers Plan 2	\$0.02/Server/hour Included data - 500 MB/day
Microsoft Defender for Containers	\$0.0095/vCore/hour ⁴
Microsoft Defender for SQL on Azure-connected databases	\$0.021/Instance/hour ²
Microsoft Defender for SQL outside Azure	\$0.015/vCore/hour ³
Microsoft Defender for MySQL	\$15/Instance/month
Microsoft Defender for PostgreSQL	\$15/Instance/month
Microsoft Defender for MariaDB	\$0.021/Instance/hour
Microsoft Defender for Azure Cosmos DB ^{5, 6}	\$0.0012 per 100 RUs/hour
Microsoft Defender for Storage ¹	\$0.02/10K transactions
Microsoft Defender for App Service	\$0.02/App Service/hour
Microsoft Defender for Key Vault	\$0.02/10K transactions
Microsoft Defender for ARM	\$4/1M API calls
Microsoft Defender for DNS	\$0.70/1M Queries

Connecting your non-Azure machines to Microsoft Defender for Cloud

Microsoft Defender for Cloud can monitor the security posture of your non-Azure computers, but first you need to connect them to Azure

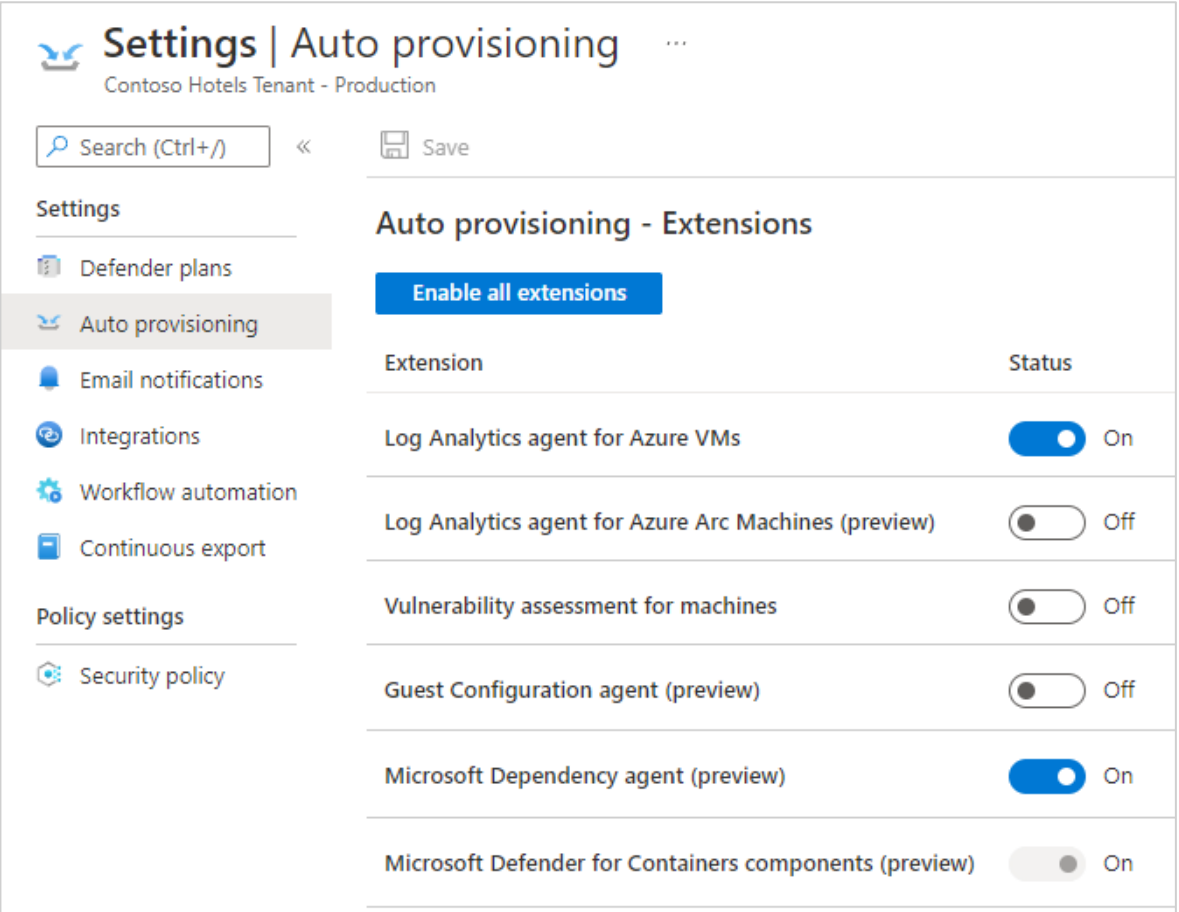
You can connect your non-Azure computers in any of the following ways

- Using Azure Arc-enabled servers (**recommended**)
- From Microsoft Defender for Cloud's pages in the Azure portal (**Getting started** and **Inventory**)

Auto provisioning for agents and extensions from Microsoft Defender for Cloud

Microsoft Defender for Cloud collects data from your resources using the relevant agent or extensions for that resource and the type of data collection you've enabled

Auto provisioning reduces management overhead by installing all required agents and extensions on existing - and new - machines to ensure faster security coverage for all supported resources



Settings | Auto provisioning ...
Contoso Hotels Tenant - Production

Search (Ctrl+/) << Save

Settings

- Defender plans
- Auto provisioning**
- Email notifications
- Integrations
- Workflow automation
- Continuous export

Policy settings

- Security policy

Auto provisioning - Extensions

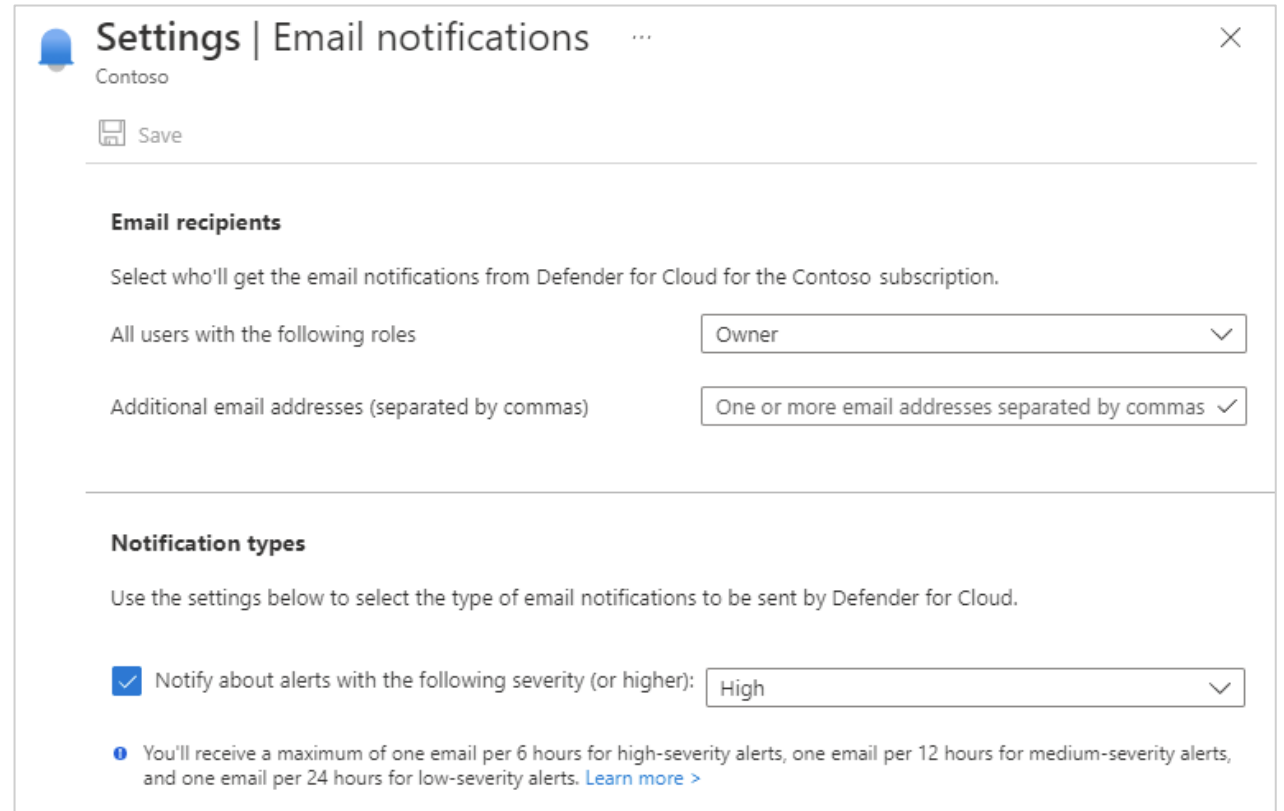
[Enable all extensions](#)

Extension	Status
Log Analytics agent for Azure VMs	<input checked="" type="checkbox"/> On
Log Analytics agent for Azure Arc Machines (preview)	<input type="checkbox"/> Off
Vulnerability assessment for machines	<input type="checkbox"/> Off
Guest Configuration agent (preview)	<input type="checkbox"/> Off
Microsoft Dependency agent (preview)	<input checked="" type="checkbox"/> On
Microsoft Defender for Containers components (preview)	<input type="checkbox"/> On

Email notifications for security alerts

Use Microsoft Defender for Cloud's **Email notifications** settings page to define preferences for notification emails including

- **Who should be notified** - Emails can be sent to select individuals or to anyone with a specified Azure role for a subscription
- **What they should be notified about** - Modify the severity levels for which Microsoft Defender for Cloud should send out notifications



The screenshot shows the 'Settings | Email notifications' interface for the 'Contoso' subscription. It includes a 'Save' button and two main sections: 'Email recipients' and 'Notification types'. In the 'Email recipients' section, 'All users with the following roles' is set to 'Owner', and 'Additional email addresses (separated by commas)' is set to 'One or more email addresses separated by commas'. In the 'Notification types' section, the checkbox 'Notify about alerts with the following severity (or higher):' is checked, and the severity is set to 'High'. A note at the bottom states: 'You'll receive a maximum of one email per 6 hours for high-severity alerts, one email per 12 hours for medium-severity alerts, and one email per 24 hours for low-severity alerts. [Learn more >](#)'

Settings | Email notifications Contoso

Save

Email recipients

Select who'll get the email notifications from Defender for Cloud for the Contoso subscription.

All users with the following roles Owner

Additional email addresses (separated by commas) One or more email addresses separated by commas

Notification types

Use the settings below to select the type of email notifications to be sent by Defender for Cloud.

☒ Notify about alerts with the following severity (or higher): High


i You'll receive a maximum of one email per 6 hours for high-severity alerts, one email per 12 hours for medium-severity alerts, and one email per 24 hours for low-severity alerts. [Learn more >](#)

Enabling enhanced security on multiple subscriptions or workspaces

Microsoft Defender for Cloud | Getting started

Showing 72 subscriptions


Upgrade Install agents Get started



Enable Microsoft Defender for Cloud on your subscriptions.


Get started with 30-day free trial

Upgrade to get advanced capabilities including hybrid support, networking, security policies, just-in-time administration and adaptive application controls. [Learn more >](#)




Cloud security posture management

Get continuous assessment and prioritized security recommendations with secure score, and verify compliance with regulatory standards



Cloud workload protection for machines

Protect Windows, Linux and on-prem servers. Protection includes: configuration and vulnerability management, workload hardening and server EDR



Advanced threat protection for PaaS

Prevent threats and detect unusual activities on PaaS workloads including App Service plans, Storage accounts, and SQL servers

Select subscriptions and workspaces to protect with Microsoft Defender for Cloud

<input type="checkbox"/>	Name	↑↓	Total resources	Microsoft Defender Plan
<input type="checkbox"/>	Stage		6	Trial expired
<input type="checkbox"/>	Production		124	Trial expired
<input type="checkbox"/>	Integrations - Dev		10	Trial expired
<input type="checkbox"/>	Export - Dev		93	Trial expired
<input type="checkbox"/>	solutiontest		0	On (partial)
<input type="checkbox"/>	e2e-dev		115	Off

Upgrade

Total: 0 resources

- 0 Servers Server/Month
- 0 App Service instances Instance/Month
- 0 Azure SQL Database Server/Month
- 0 SQL servers on machines Server/Month Core/Hour
- 0 Storage accounts 10k transactions
- 0 Kubernetes cores VM core/Month
- 0 Container registries Image
- 0 Key Vaults 10k transactions
- 0 SQL servers on machines Server/Month Core/Hour
- Resource Manager (Preview)
- DNS (Preview)

[To enable enhanced security features on your subscriptions and workspaces:](#)

Introduction to Microsoft Defender for Cloud's enhanced security features

Microsoft Defender for Cloud's enhanced security features

The enhanced security features are free for the first 30 days

At the end of 30 days, if you decide to continue using the service, you'll be charged for usage automatically

The screenshot displays the 'Settings | Defender plans' page for 'Contoso Infra2'. It features a toggle switch to 'Enable the enhanced security of Microsoft Defender for Cloud'. Below this, two panels compare feature availability. The left panel, 'Enhanced security off', shows that while 'Continuous assessment and security recommendations' and 'Secure score' are active (green checkmarks), '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)', and 'Threat protection for supported PaaS services' are disabled (red X marks). The right panel, 'Enable all Microsoft Defender for Cloud plans', shows that all these same features are enabled (green checkmarks).

Enhanced security off	Enable all Microsoft Defender for Cloud plans
✓ Continuous assessment and security recommendations	✓ Continuous assessment and security recommendations
✓ Secure score	✓ 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

Benefits of enabling enhanced security features (1/2)

Microsoft Defender for Endpoint	Microsoft Defender for servers includes Microsoft Defender for Endpoint for comprehensive endpoint detection and response (EDR)
Vulnerability assessment for virtual machines, container registries, and SQL resources	Easily enable vulnerability assessment solutions to discover, manage, and resolve vulnerabilities
Multi-cloud security	Connect your accounts from Amazon Web Services (AWS) and Google Cloud Platform (GCP) to protect resources and workloads on those platforms with a range of Microsoft Defender for Cloud security features
Hybrid security	Get a unified view of security across all of your on-premises and cloud workloads

Benefits of enabling enhanced security features (2/2)

Threat protection alerts	Built-in behavioral analytics and machine learning can identify attacks and zero-day exploits
Track compliance with a range of standards	Microsoft Defender for Cloud continuously assesses your hybrid cloud environment to analyze the risk factors according to the controls and best practices in Azure Security Benchmark
Access and application controls	Block malware and other unwanted applications by applying machine learning powered recommendations adapted to your specific workloads to create allow and blocklists
Container security features	Benefit from vulnerability management and real-time threat protection on your containerized environments
Breadth threat protection for resources connected to Azure	Cloud-native threat protection for the Azure services common to all of your resources: Azure Resource Manager, Azure DNS, Azure network layer, and Azure Key Vault

Enabling enhanced security features on one subscription

[To enable enhanced security features on your subscriptions and workspaces:](#)

Settings | Defender plans

Contoso Infra2

Save

Enable the enhanced security of Microsoft Defender for Cloud. [Learn more >](#)

Enhanced security off

✓ Continuous assessment and security recommendations

✓ 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

Enable all Microsoft Defender for Cloud plans

✓ Continuous assessment and security recommendations

✓ 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

Defender for Cloud plans will be enabled on 32 resources in this subscription

Select Defender plan by resource type

Enable all


Microsoft Defender for	Resource Quantity	Pricing	Plan
Servers	10 servers	Server/Month	<div>On</div> <div>Off</div>
App Service	0 instances	Instance/Month	<div>On</div> <div>Off</div>
Azure SQL Databases	0 servers	Server/Month	<div>On</div> <div>Off</div>
SQL servers on machines	0 servers	Server/Month Core/Hour	<div>On</div> <div>Off</div>
Open-source relational databases	0 servers	Server/Month	<div>On</div> <div>Off</div>
Storage	3 storage accounts	10k transactions	<div>On</div> <div>Off</div>
Kubernetes	18 kubernetes cores	VM core/Month	<div>On</div> <div>Off</div>
Container registries	0 container registries	Image	<div>On</div> <div>Off</div>
Key Vault	1 key vaults	10k transactions	<div>On</div> <div>Off</div>
Resource Manager		1M resource mana...	<div>On</div> <div>Off</div>
DNS		1M DNS queries	<div>On</div> <div>Off</div>

Enabling enhanced security on multiple subscriptions or workspaces

Microsoft Defender for Cloud | Getting started

Showing 72 subscriptions


Upgrade Install agents Get started



Enable Microsoft Defender for Cloud on your subscriptions.


Get started with 30-day free trial

Upgrade to get advanced capabilities including hybrid support, networking, security policies, just-in-time administration and adaptive application controls. [Learn more >](#)




Cloud security posture management

Get continuous assessment and prioritized security recommendations with secure score, and verify compliance with regulatory standards



Cloud workload protection for machines

Protect Windows, Linux and on-prem servers. Protection includes: configuration and vulnerability management, workload hardening and server EDR



Advanced threat protection for PaaS

Prevent threats and detect unusual activities on PaaS workloads including App Service plans, Storage accounts, and SQL servers

Select subscriptions and workspaces to protect with Microsoft Defender for Cloud

<input type="checkbox"/>	Name	↑↓	Total resources	Microsoft Defender Plan
<input type="checkbox"/>	🔑 Stage		6	Trial expired
<input type="checkbox"/>	🔑 Production		124	Trial expired
<input type="checkbox"/>	🔑 Integrations - Dev		10	Trial expired
<input type="checkbox"/>	🔑 Export - Dev		93	Trial expired
<input type="checkbox"/>	📊 solutiontest		0	On (partial)
<input type="checkbox"/>	📊 e2e-dev		115	Off

Upgrade

Total: 0 resources

- 0 Servers Server/Month
- 0 App Service instances Instance/Month
- 0 Azure SQL Database Server/Month
- 0 SQL servers on machines Server/Month Core/Hour
- 0 Storage accounts 10k transactions
- 0 Kubernetes cores VM core/Month
- 0 Container registries Image
- 0 Key Vaults 10k transactions
- 0 SQL servers on machines Server/Month Core/Hour
- Resource Manager (Preview)
- DNS (Preview)

[Reference: To enable enhanced security features on your subscriptions and workspaces:](#)

Disabling enhanced security features

The screenshot shows the 'Settings | Defender plans' page in the Azure portal. The left sidebar contains a 'Settings' section with a list of options: 'Defender plans' (selected), 'Auto provisioning', 'Email notifications', 'Integrations', 'Workflow automation', 'Continuous export', and 'Cloud connectors'. The main content area has a search bar, a 'Save' button, and a purple banner that reads 'Enable Azure Defender for enhanced security. Try it free for the first 30 days. Learn more >'. Below this, there are two panels. The left panel, titled 'Enhanced security off', is highlighted with a red border and a mouse cursor. It lists seven features: 'Continuous assessment and security recommendations' (checked), 'Secure score' (checked), 'Just in time VM Access' (unchecked), 'Adaptive application controls and network hardening' (unchecked), 'Regulatory compliance dashboard and reports' (unchecked), 'Threat protection for Azure VMs and non-Azure servers (including Server EDR)' (unchecked), and 'Threat protection for supported PaaS services' (unchecked). The right panel, titled 'Enable all Microsoft Defender for Cloud plans', lists the same seven features, all of which are checked.

Settings | Defender plans ...

Search (Ctrl+/) << Save

Settings

- Defender plans
- Auto provisioning
- Email notifications
- Integrations
- Workflow automation
- Continuous export
- Cloud connectors

Enhanced security off

- ✓ Continuous assessment and security recommendations
- ✓ 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

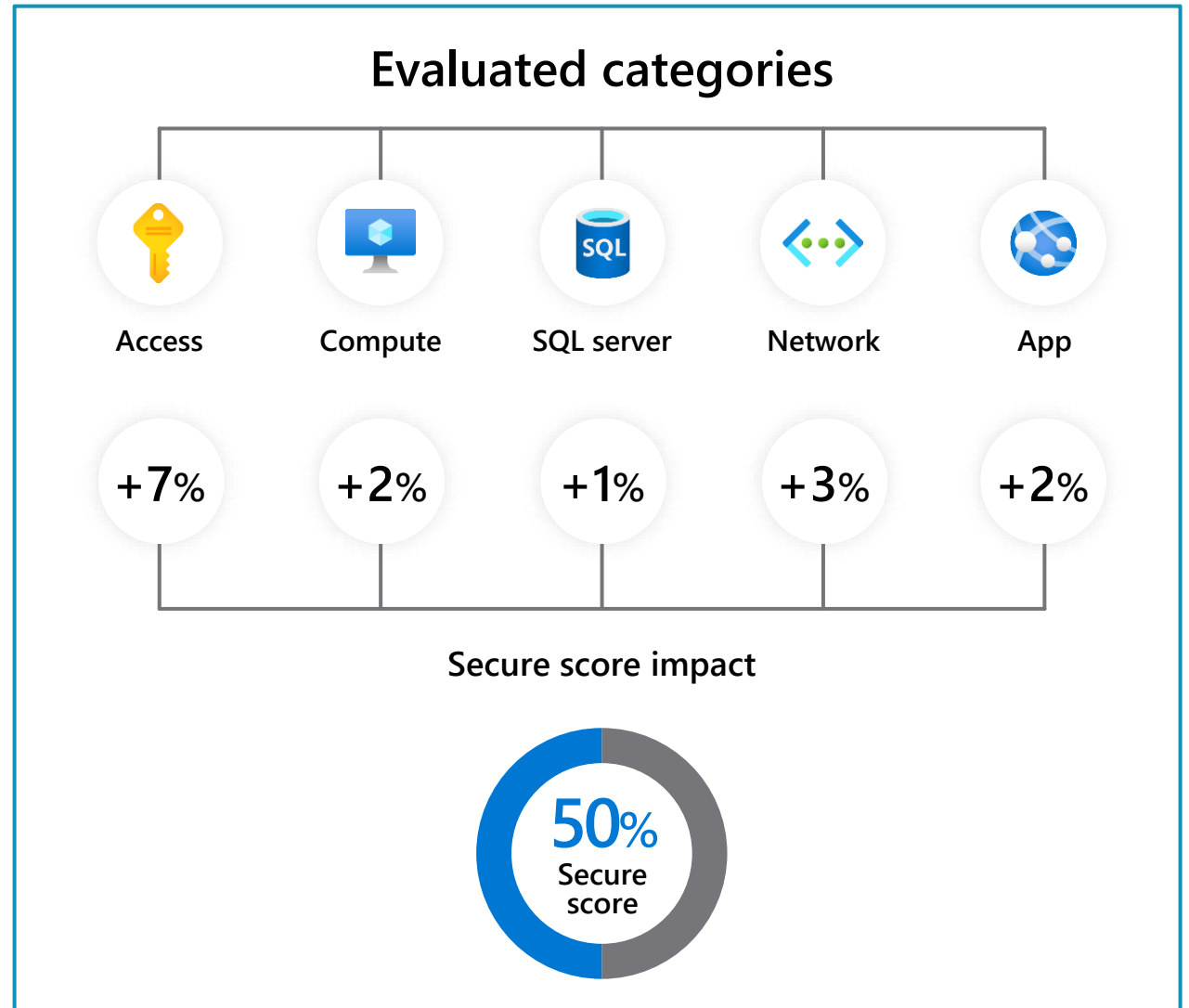
Enable all Microsoft Defender for Cloud plans

- ✓ Continuous assessment and security recommendations
- ✓ 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

Using Secure Score to drive Security Posture Management

Security posture management with secure score

- Gain insights into the security state of your cloud workloads across Azure and AWS
- Address security vulnerabilities with prioritized recommendations
- Improve your secure score and overall security posture in minutes
- Speed up regulatory compliance
- Granular control of secure score

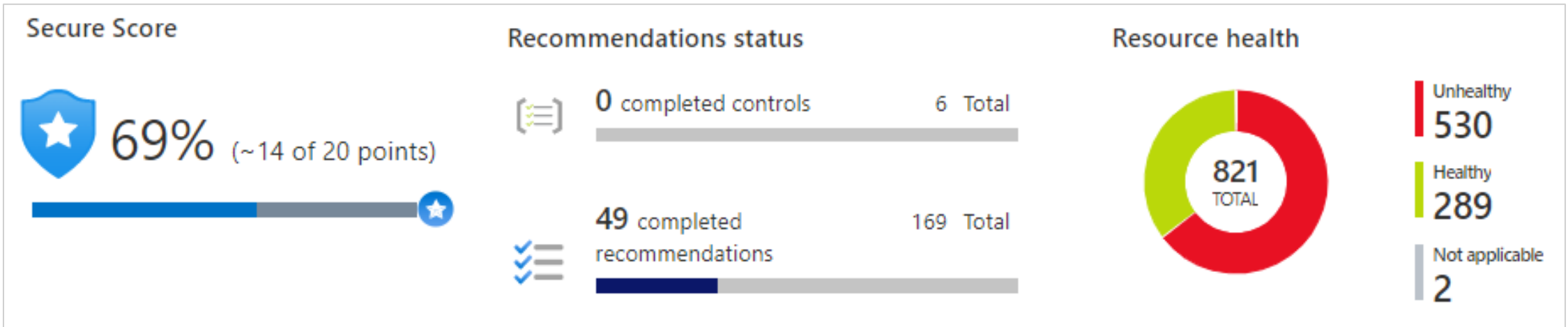


Introduction to Secure score

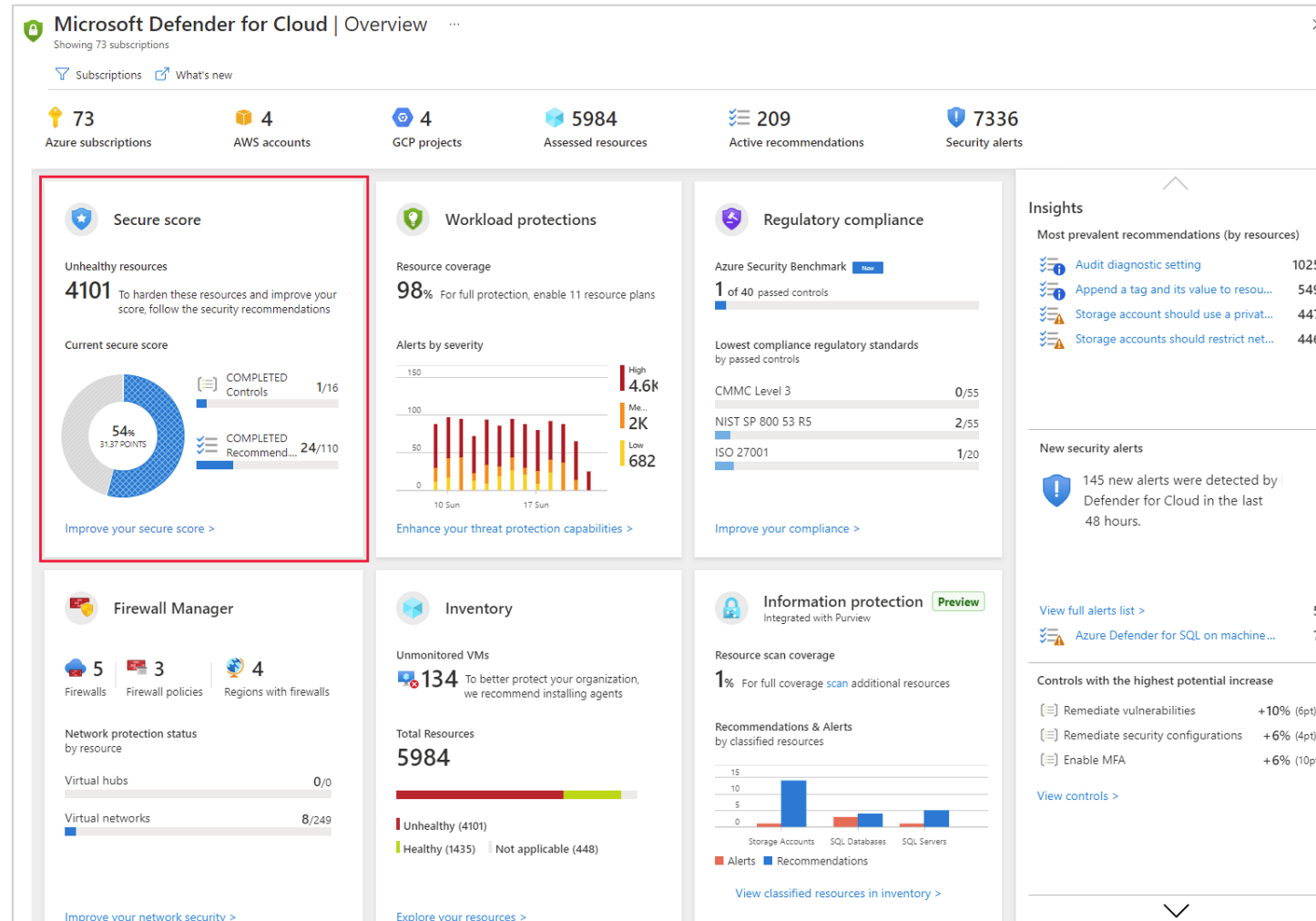
Microsoft Defender for Cloud has two main goals

- To help you understand your current security situation
- To help you efficiently and effectively improve your security

Secure score enables you to achieve those goals

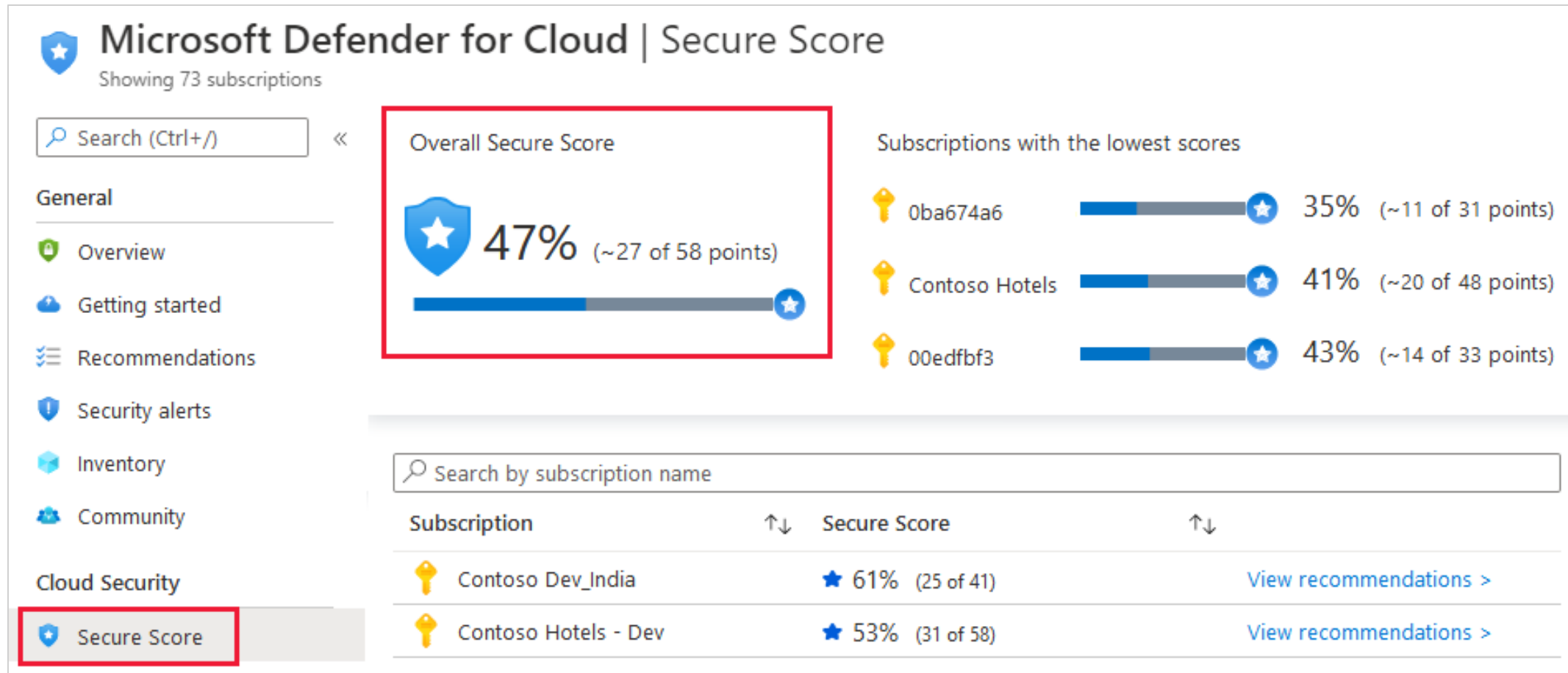


Getting your secure score from the portal



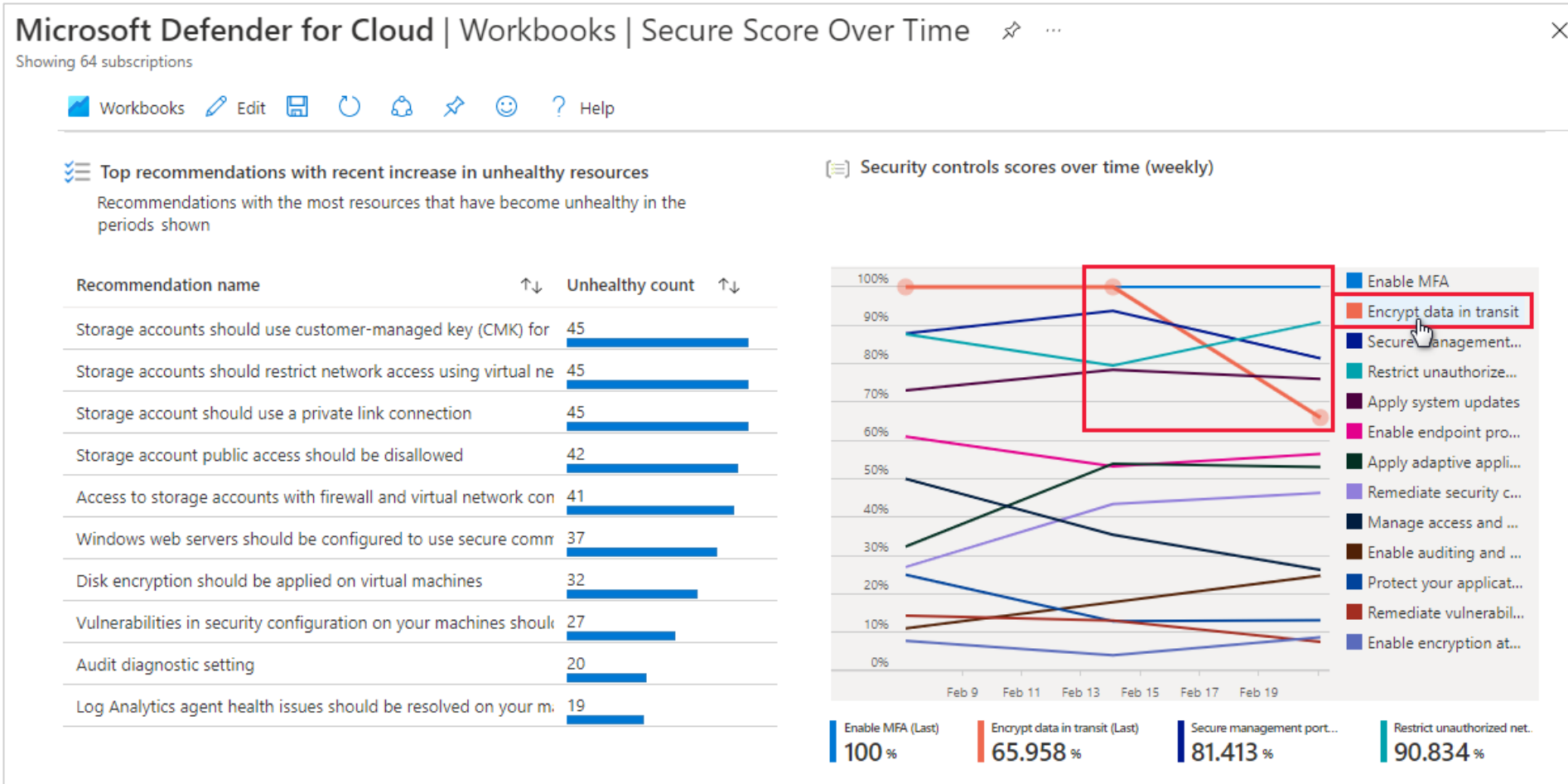
[Access and track your secure score](#)

Getting your secure score from the portal



Tracking your secure score over time

Secure Score Over Time report in workbooks page

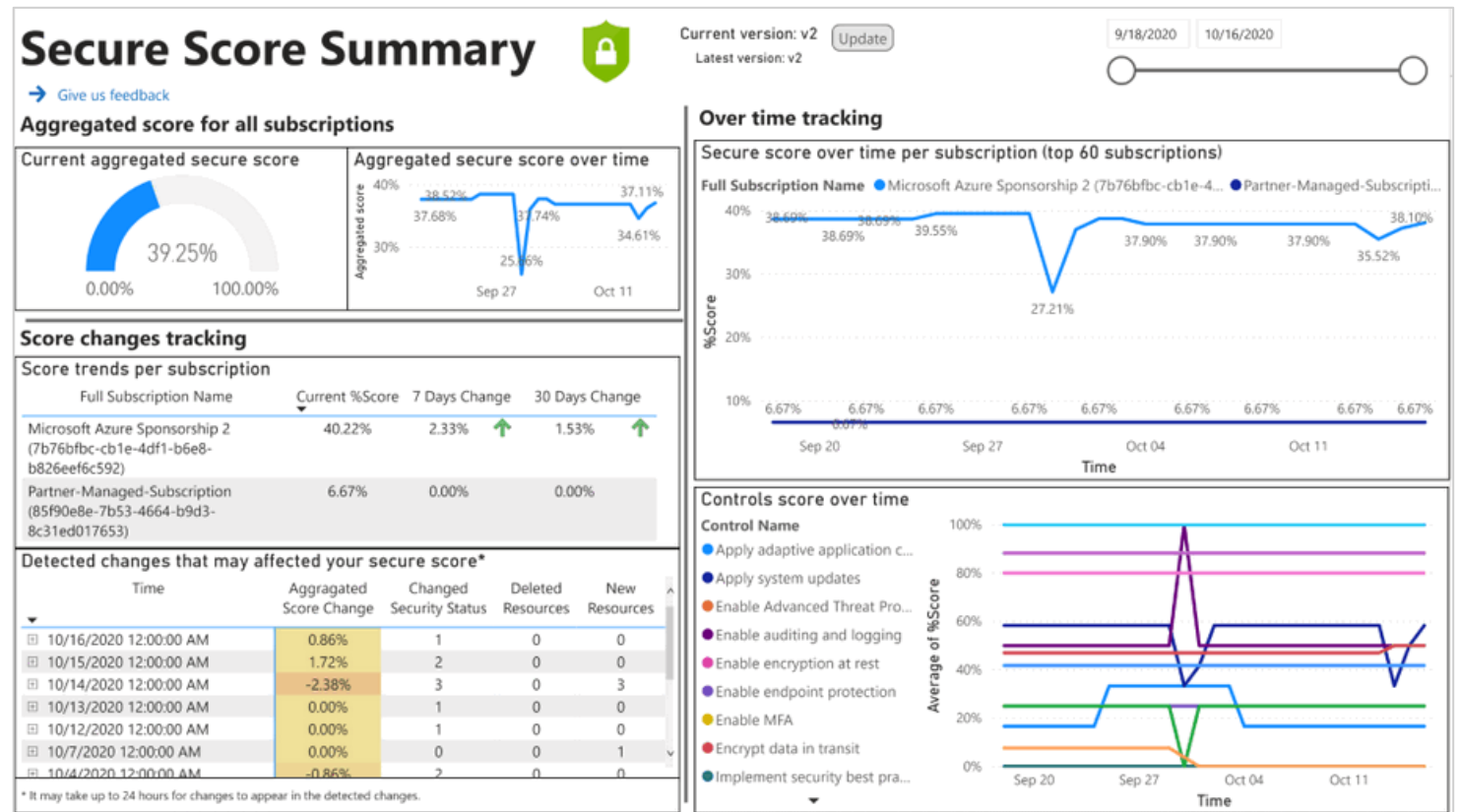


[Create rich, interactive reports of Defender for Cloud data](#)

Tracking your secure score over time

Power BI Pro dashboards

If you're a Power BI user with a Pro account, you can use the **Secure Score Over Time** Power BI dashboard to track your secure score over time and investigate any changes

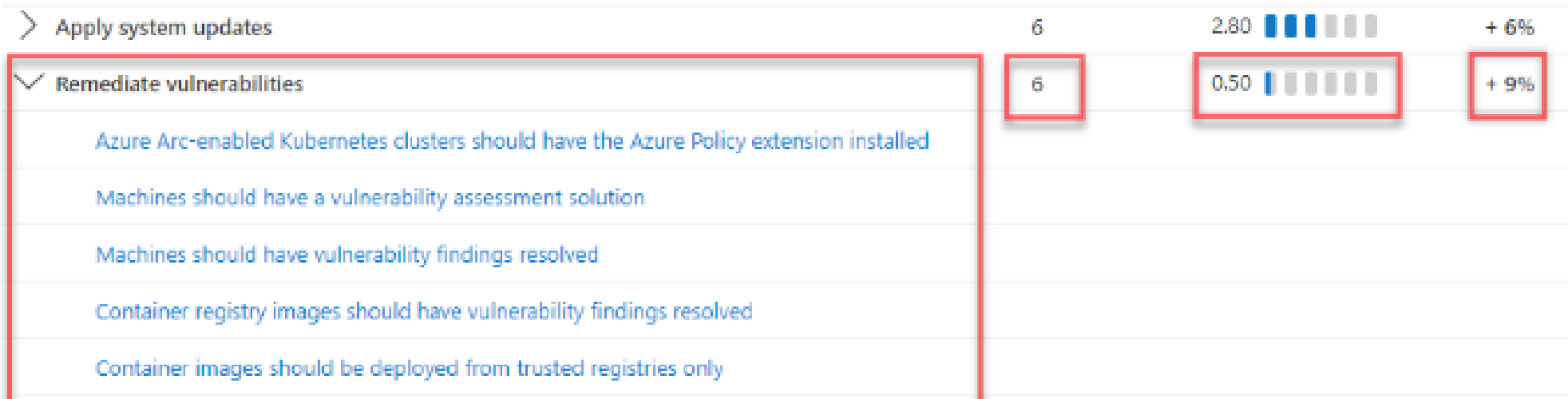


Security controls

Recommendations are grouped into **security controls**

Each control is a logical group of related security recommendations, and reflects your vulnerable attack surfaces

Your score only improves when you remediate *all* of the recommendations for a single resource within a control



How your secure score is calculated

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 the security recommendations within the security control

Security Center | Recommendations ...
Showing subscription 'Ben Kliger'
[Download CSV report](#) [Guides & Feedback](#)







Controls	Max score	Current Score	Potential score increase
> Secure management ports	8	7.52	+ 1% (0.48 points)
> Remediate vulnerabilities	6	0.86	+ 11% (5.14 points)
> Apply system updates	6	4.83	+ 2% (1.17 points)
> Manage access and permissions	4	0	+ 8% (4 points)
> Enable encryption at rest	4	0.31	+ 8% (3.69 points)
> Remediate security configurations	4	0.8	+ 7% (3.2 points)
> Restrict unauthorized network access	4	3.71	+ 1% (0.29 points)
> Encrypt data in transit	4	4	+ 0% (0 points)
> Apply adaptive application control	3	0.88	+ 4% (2.12 points)
> Protect applications against DDoS attacks	2	0.5	+ 3% (1.5 points)
> Enable endpoint protection	2	1.33	+ 1% (0.67 points)
> Enable auditing and logging	1	0.11	+ 2% (0.89 points)
> Apply data classification	Not scored	Not scored	+ 0% (0 points)
> Enable Azure Defender	Not scored	Not scored	+ 0% (0 points)
> Implement security best practices	Not scored	Not scored	+ 0% (0 points)

Example scores for a control

1. Remediate vulnerabilities security control
2. Max score
3. Number of resources
4. Current score
5. Potential score increase

 **Security Center** | Recommendations ...
Showing 5 subscriptions

[Download CSV report](#) [Guides & Feedback](#)



Controls	Max score	Current Score	Potential score increase	Unhealthy resources
> Enable MFA 	10	10 	+ 0% (0 points)	None
> Secure management ports	8	2.13 	+ 10% (5.87 points)	11 of 24 resources
▼ Remediate vulnerabilities	6	0.86 	+ 9% (5.14 points)	30 of 35 resources
1 Azure Defender for SQL should be enabled on your SQL servers	2	4	5	4 3 SQL servers
A vulnerability assessment solution should be enabled on your virtual machines				25 of 25 VMs & s...
Container images should be deployed from trusted registries only				1 of 5 managed cl...
Azure Policy Add-on for Kubernetes should be installed and enabled on your clusters 				None
> Apply system updates	6	3.23 	+ 5% (2.77 points)	12 of 31 resources


Improving your secure score


To improve your secure score, remediate security recommendations from your recommendations list



Don't allow users to create resources that may negatively impact your score by configuring the **Enforce** and **Deny** options on the relevant recommendations


Secure transfer to storage accounts should be enabled ×

 Deny 

Severity: **High** Freshness interval:  30 Min

Auditing on SQL server should be enabled  ×

 Enforce 

Severity: **High** Freshness interval:  30 Min

[Prevent misconfigurations with Enforce/Deny recommendations](#)

Thank you