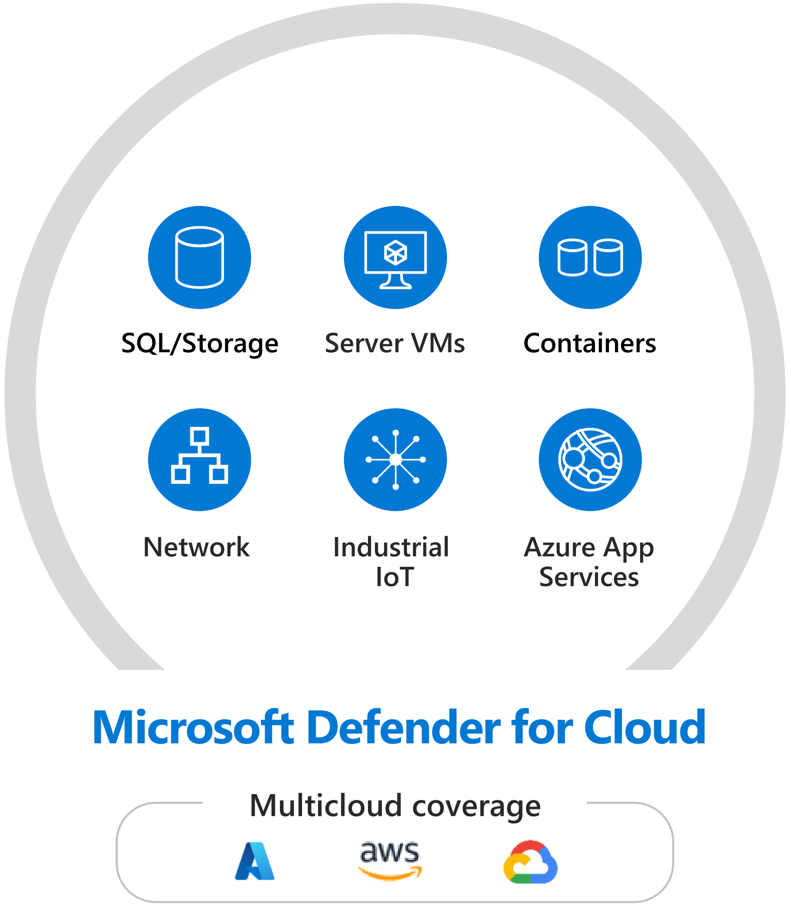
Microsoft Security

Microsoft Defender for Cloud

A Quick Start Guide



A Quick Summary and an ask for help

What are we achieving with this guide?

To goal of this guide is to help you accelerate your initial deployment of Microsoft Defender for Cloud, get the most value from Defender as quickly as possible leveraging the built-in capabilities such as Cloud Security Posture Management, Workload Protection, Security Recommendations, Monitoring Secure Score and Threat Detection. Along with these key enablement steps this guide provides learning and documentation references to several key areas of Defender for Cloud from Microsoft and the Community.

What the guide is not for

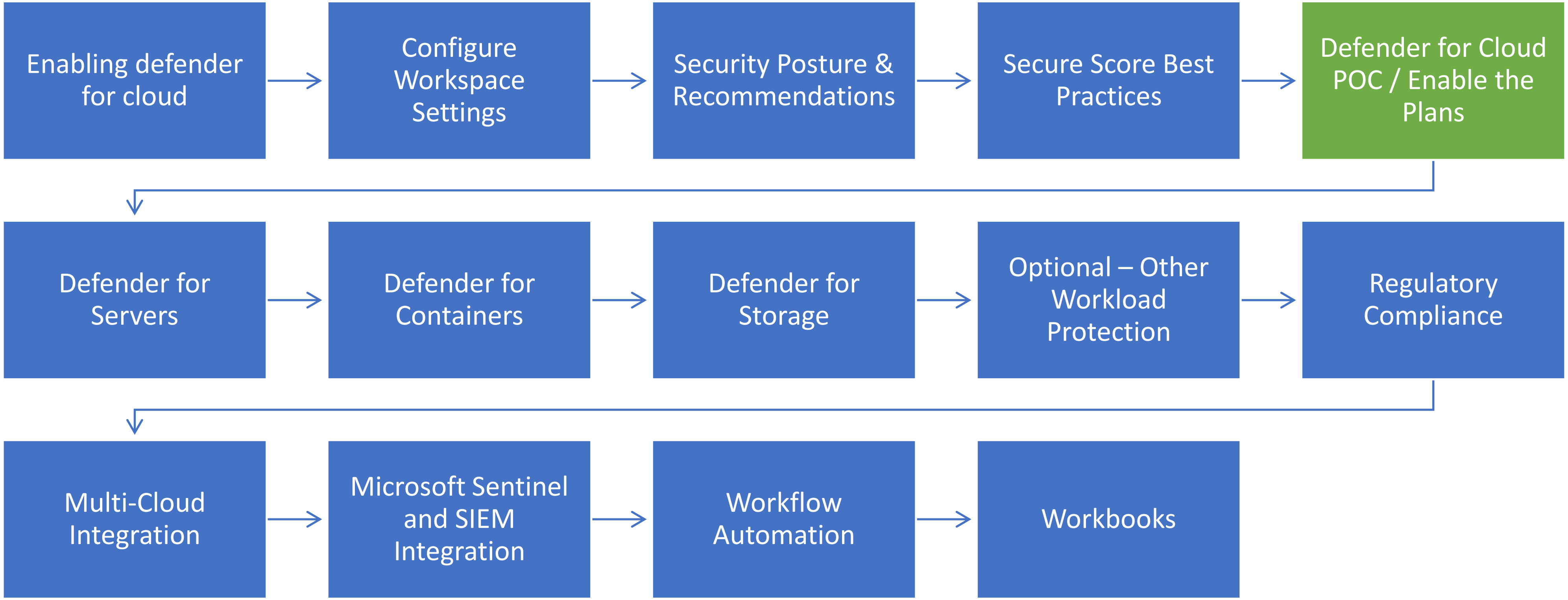
In-depth configuration steps, advanced architecture, training, or to cover specific use cases. The content is intentionally generalized to set you up for success with your Defender for Cloud deployment.

What can I do to help?

As a customer, partner, or @Microsoft please provide feedback about this guide. Did we miss any critical start components? Are the links out of date? Is the content out of date?

Using this Guide

- This getting started guide is intended to augment our official Microsoft Defender for Cloud documentation | Microsoft Docs as a resource to quickly get started with Microsoft Defender.
- Content is in order of operation and intended to follow common tasks for Defender for Cloud enablement
- You may find links in the notes section on each slide that provide further learning and documentation resources



Enabling defender for cloud

Configure Workspace Settings

Security Posture & Recommendations

Secure Score Best Practices

Defender for Cloud POC / Enable the Plans

Defender for Servers

Defender for Containers

Defender for Storage

Optional – Other Workload Protection

Regulatory Compliance

Multi-Cloud Integration

Microsoft Sentinel and SIEM Integration

Workflow Automation

Workbooks

Enabling Defender for Cloud

Requirements

- To get started with Defender for Cloud, you must have a subscription to Microsoft Azure. If you don't have a subscription, you can sign up for a free account.

- Log Analytics workspace.

- To enable enhanced security features on a subscription, you must be assigned the role of Subscription Owner, Subscription Contributor, or Security Admin.

Go Do

1. Enable Microsoft Defender for Cloud

Key Tips and Strategies

- Enabled on your Azure subscriptions

- Email notifications set up for security alerts

- Use the same workspace for both **Microsoft Sentinel** and **Microsoft Defender for Cloud**

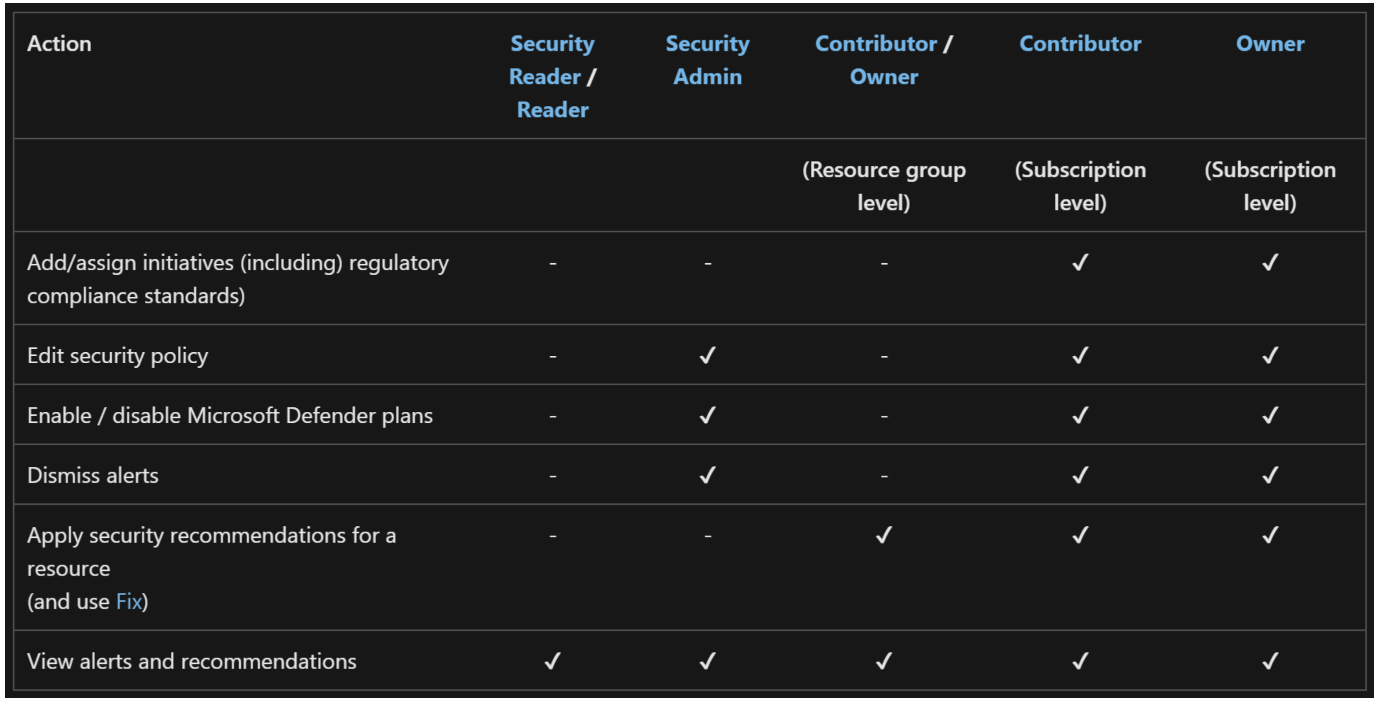
Role Based Access Controls

Key Tips and Strategies

- Defender for Cloud uses Role-based access control (Azure RBAC) to provide built-in roles that can be assigned to users, groups, and services in Azure.
- Permissions in Microsoft Defender for Cloud | Microsoft Docs
- Keep it simple, focus on custom or table level RBAC later

Go Do

1. Reference the Role Recommendations section and assign applicable roles to your team



Action	Security Reader / Reader	Security Admin	Contributor / Owner	Contributor	Owner
			(Resource group level)	(Subscription level)	(Subscription level)
Add/assign initiatives (including) regulatory compliance standards)	-	-	-	✓	✓
Edit security policy	-	✓	-	✓	✓
Enable / disable Microsoft Defender plans	-	✓	-	✓	✓
Dismiss alerts	-	✓	-	✓	✓
Apply security recommendations for a resource (and use Fix)	-	-	✓	✓	✓
View alerts and recommendations	✓	✓	✓	✓	✓

Configure Log Analytics Settings

Log Analytics Workspaces

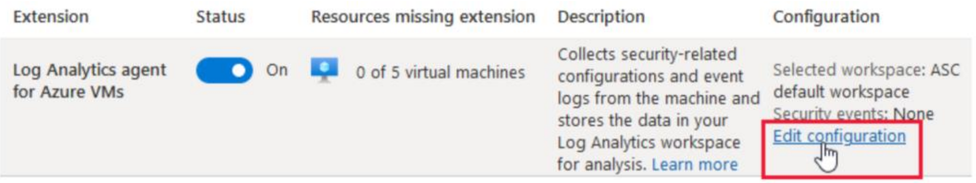
- A Log Analytics workspace is required for Microsoft Defender for Cloud
- By default, Microsoft Defender for Cloud will create a separate workspace per region in each subscription where it is enabled.

Existing Workspaces

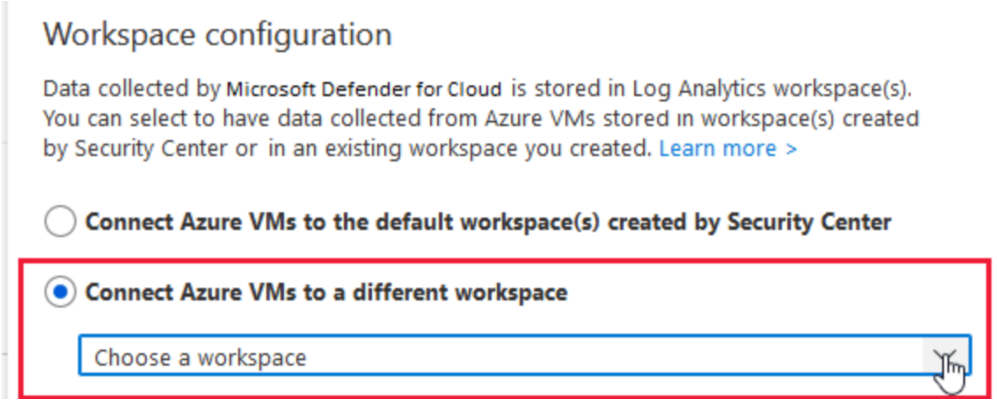
- You can also select an existing Log Analytics workspace to store data collected by Defender for Cloud.
- It’s a best practice to use the same workspace for both Sentinel and Defender for Cloud, so that all logs collected by Defender for Cloud can also be ingested and used by Sentinel.

Go Do

1. If you have Microsoft Sentinel, see how you can use your existing Log Analytics workspace



Extension	Status	Resources missing extension	Description	Configuration
Log Analytics agent for Azure VMs	On	0 of 5 virtual machines	Collects security-related configurations and event logs from the machine and stores the data in your Log Analytics workspace for analysis. Learn more	Selected workspace: ASC default workspace Security events: None Edit configuration



Workspace configuration

Data collected by Microsoft Defender for Cloud is stored in Log Analytics workspace(s). You can select to have data collected from Azure VMs stored in workspace(s) created by Security Center or in an existing workspace you created. Learn more >

○ Connect Azure VMs to the default workspace(s) created by Security Center

● Connect Azure VMs to a different workspace

Choose a workspace

Security posture & Recommendations

Security posture

Defender for Cloud displays your posture in the first main tile the overview page.

- Security Posture is part of the **Free Tier**.
- Defender for Cloud continually assesses your cross-cloud resources 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.

Recommendations

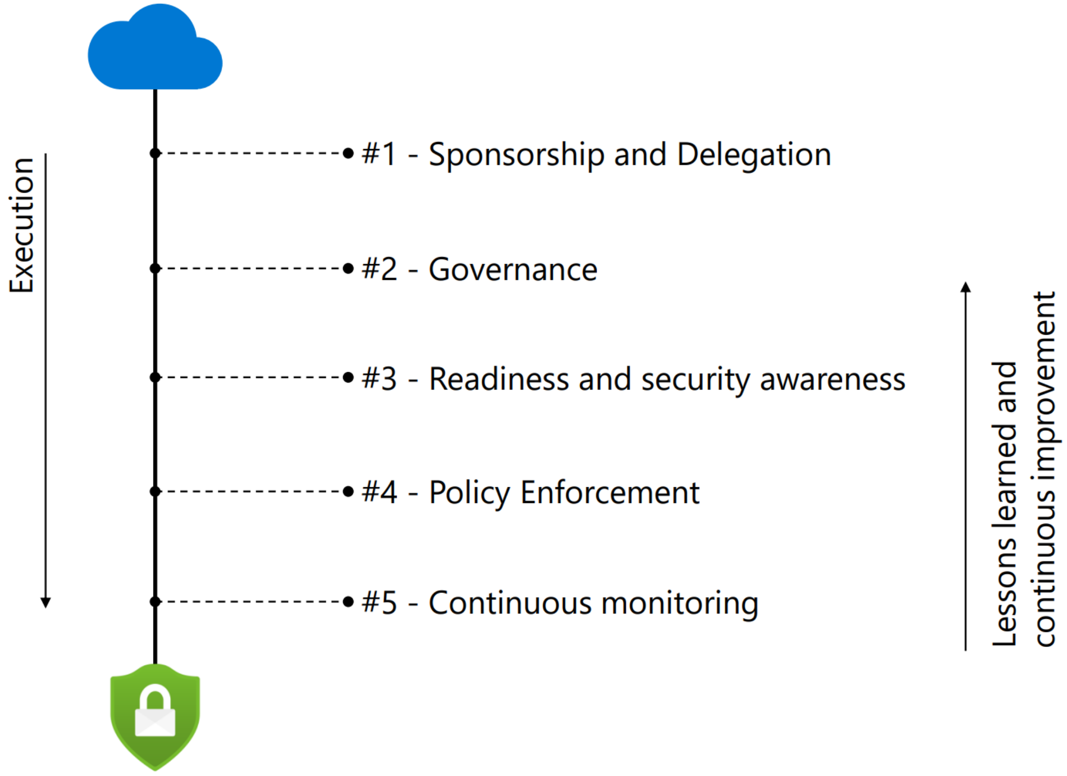
- It shows your Secure Score, not only for Azure, but also GCP and AWS.
- To increase your security, review Defender for Cloud's recommendations page and remediate the recommendation by implementing the remediation instructions for each issue.
- Recommendations are grouped into **security controls**.
- Each control is a logical group of related security recommendations and reflects your vulnerable attack surfaces.
- Your score only improves when you remediate all the recommendations for a single resource within a control.
- To see how well your organization is securing each individual attack surface, review the scores for each security control.

Key Tips and Strategies

- Access and track your secure score.
- If you have a multi-cloud environment, connect GCP and AWS to Defender for Cloud.
- You can get your secure score from the REST API, Azure Resource Graph or through Power BI Pro dashboards.
- Use the Secure Score Over Time report in workbooks page.
- Determine when to use custom security initiatives and policies according to your own governance and requirements.
- Determine when to exempt resources and recommendations from your secure score.

Secure Score Best Practices

Key Tips and Strategies



Execution

- #1 - Sponsorship and Delegation
- #2 - Governance
- #3 - Readiness and security awareness
- #4 - Policy Enforcement
- #5 - Continuous monitoring

Lessons learned and continuous improvement

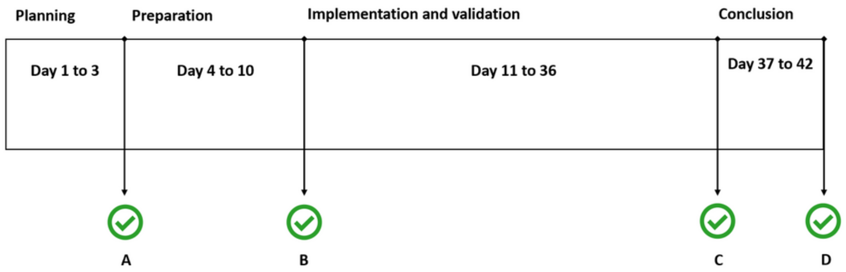
Go Do

- Review Defender for Cloud Recommendation
  - Secure Score Over Time Reports
- Prioritize the security controls that have a highest secure score impact
- Remediate the recommendations that belong to this security control
- Create exemptions when necessary and document the “why” those exceptions were created
- Configure the Secure Score PowerBI dashboard
- Automate the process to notify workload owners that new recommendations were created for their workloads
- Automate the secure score progress report via email
  - Deliver a Security Score weekly briefing
- Establish a cadence to review progress, take notes of what is working and what needs to improve
  - Microsoft Defender for Cloud Secure Score Reduction Alert
- Governance
  - Create custom security initiatives and policies
  - Azure security baseline for Microsoft Defender for Cloud
  - Organize subscriptions into management groups and assign roles to users

Defender for Cloud PoC

Microsoft Defender for Cloud PoC Series provides guidelines on how to perform a proof of concept for a specific Microsoft Defender plan.

- Use following schedule to perform their Microsoft Defender for Cloud PoC. Keep in mind that this is an example, and each organization may adequate this according to their needs.



Planning
Day 1 to 3
A

Preparation
Day 4 to 10
B

Implementation and validation
Day 11 to 36
C

Conclusion
Day 37 to 42
D

- Microsoft Defender for Kubernetes
- Microsoft Defender for Resource Manager
- Microsoft Defender for Storage
- Microsoft Defender for Key Vault
- Microsoft Defender for DNS
- Microsoft Defender for App Service
- Microsoft Defender for Container Registries
- Microsoft Defender for SQL
- Microsoft Defender for Servers

Go Do

1. You can enable any of the Microsoft Defender for Cloud plans for **30 days**, therefore enable it when you are ready to work on the PoC.

2. Use this link as guidance to perform their Microsoft Defender for Cloud PoC.

3. Determine if the type of deployment: single cloud (Azure) or multi-cloud. For AWS considerations, read this article. For GCP considerations, read this article.

Defender for Servers

Adding threat detection and advanced defenses to your Windows and Linux machines whether they're running in Azure, AWS, GCP, and on-premises environment.

- Extend Visibility and Protection to On-Premise and Multi-Cloud Workloads
- Advanced Protection and Detection Capabilities leveraging ML
- Harden machines against malware and comply with regulatory frameworks
- Mitigate network exposure of management ports
- Integration with Microsoft Defender for Endpoint
- It’s available in two plans: Defender for Servers Plan 1 and Plan 2

Go Do

1. Understand the plans available Defender for Server Plans.
2. Azure Arc for Windows and Linux Servers on-premises and multi-cloud.
3. Defender for Endpoint sensor is automatically enabled on Servers that are onboarded to Microsoft Defender for Cloud.
4. Enable JIT on your VMs.
5. Enable Qualys or Microsoft TVM vulnerability scanner.
6. Enable file integrity monitoring (FIM).
7. Use adaptive application controls to reduce your machines' attack surfaces.
8. Configure adaptive network hardening.
9. Run a detection test and simulation on a newly onboarded Microsoft Defender for Endpoint device

Defender for Containers

Defender for Containers protects your clusters whether they're running in AKS, EKS, GKE, Arc enabled CNCF clusters

Benefits

- Environment hardening
- Vulnerability assessment
- Run-time threat protection for nodes and clusters

You can also scan container images for vulnerabilities as the images are built in your CI/CD GitHub workflows

Reference

Alerts in Defender for Containers

List of Cloud recommendations

Containers feature availability by Environment

Go Do

1. Identity the clusters to be integrated with Defender for cloud.
2. Enable Microsoft Defender for Containers
3. Integrate Vulnerability scanner for container images in CI/CD workflows
4. Set Permissions
5. Verify Microsoft Defender for Containers is running properly by simulating an alert.
   - Alert validation
6. Enable for Amazon EKS
7. Protect Google Kubernetes Engine (GKE) clusters

Key Tips and Strategies

•Policy Add-on for Kubernetes - Azure Kubernetes Service clusters should have the Azure Policy Add-on for Kubernetes installed
•Azure Kubernetes Service profile - Azure Kubernetes Service clusters should have Defender profile enabled
•Azure Arc-enabled Kubernetes extension - Azure Arc-enabled Kubernetes clusters should have the Defender extension installed

If you choose to disable all of the auto provision configuration options, no agents, or components will be deployed to your clusters. Protection will be limited to the Agentless features only. Learn which features are Agentless in the **availability section** for Defender for Containers

Defender for Storage

Key Tips and Strategies

Azure Security Center

Azure Defender for Storage

- Recommends to disallow anonymous read access
- Recommends to allow only secure connections (HTTPS)

- Detects potential malware upload (hash reputation)
- Detects phishing content hosted
- Detects access from suspicious IP address (TI)
- Detects unusual anonymous access
- Detects unusual amount of data extraction

Go Do

1. Identify the use case scenarios that you want to validate.

2. You need at least Security Admin role to enable Microsoft Defender for Storage. For more information about roles and privileges, visit this article.

3. Common scenario: identify if the Storage account has any access from suspicious IP address, suspicious access patterns or even if there’s a malicious content upload on Storage accounts.

4. To test the Security alerts from Microsoft Defender for Storage follow the steps from here to trigger a test alert.

5. Review this article that will go over the steps to simulate an upload of a test malware (EICAR) to an Azure Storage account that has ATP for Azure Storage enabled.

Other Workloads

Microsoft Defender for Resource Manager

Automatically monitors all resource management operations performed in your organization, detects suspicious Azure Resource Management activities and sends alerts

Microsoft Defender for DNS

Continuously monitors all DNS queries from your Azure resources

Sends alerts when suspicious activity is detected

Microsoft Defender for Key Vault

Detect unusual and potentially harmful attempts to exploit Azure Key Vault

Microsoft Defender for Databases

Protect SQL Server anywhere: in Azure, other cloud, and on premises

Defender for Resource Manager

Microsoft Defender for Resource Manager

Automatically monitors all resource management operations performed in your organization

Detects suspicious Azure Resource Management activities and sends alerts

Go Do

1. Identify the use case scenarios that you want to validate.
2. A common scenario is cloud service discovery, where an adversary may try to enumerate the cloud services that are running via calls to Azure Resource Manager.
3. You can use the Alerts identified by Microsoft Defender for Resource Manager as your starting point to plan which actions you want to execute.
4. You need at least Security Admin role to enable Microsoft Defender for Resource Manager.
5. You can use the sample alert feature to validate Microsoft Defender for Resource Manager alerts, or you can use the procedures from this article to simulate an attack and see how Microsoft Defender for Resource Manager detects.
6. As you review each alert is important to understand how to make sense of the metadata available. Read this article for more information on how to respond to ARM alerts.

Defender for DNS

Microsoft Defender for DNS

Continuously monitors all DNS queries from your Azure resources

Sends alerts when suspicious activity is detected

Go Do

1. Identify the use case scenarios that you want to validate.

2. Common scenarios: to be notified when a DNS attack happens in your environment such as DNS tunneling trying to exfiltrate sensitive data from your Azure resources, DNS cache poisoning, or when an attacker is trying to redirect your communication to a malicious website.

3. You need at least Security Admin role to enable Microsoft Defender for Resource Manager.

4. To test and validate the Security alerts for Microsoft Defender for DNS follow the steps from this great article to trigger a test alert.

Defender for Key Vault

Microsoft Defender for Key Vault

Detect unusual and potentially harmful attempts to exploit Azure Key Vault

Go Do

1. Identify the use case scenarios that you want to validate.

2. Some common scenarios include access from an IP that was identified by Microsoft Threat Intelligence as suspicious, a user/service principal performing anomalous changes in policies or a high volume of operations – tailored to each tenant – within the Key Vault.

3. You can use the Alerts identified by Microsoft Defender for Key Vault as your starting point to plan which actions you want to execute.

4. You need at least **Security Admin** role to enable Microsoft Defender for Resource Manager.

5. You can use the sample alert feature to validate Microsoft Defender for Key Vault alerts, or you can simulate Microsoft Defender for Key Vault alerts by following the instructions in Validating Azure Key Vault threat detection in Microsoft Defender for Cloud.

Defender for Databases

Microsoft Defender for Databases

Protect SQL Server anywhere: in Azure, other cloud, and on premises

Go Do

1. Identify the use case scenarios that you want to validate.

2. Enable Microsoft Defender for SQL, and for this you need to have the role of Security Admin. For more information about roles and privileges, visit this article.

3. You can use the sample alert feature to validate . To create these sample alerts, you will need to have the role Security Admin or Subscription Contributor.

Multi Cloud integration - AWS

AWS

- **Defender for Cloud's CSPM features**
  - This agentless plan.
  - assesses your AWS resources according to AWS-specific security recommendations
  - Assessed for compliance with built-in standards specific to AWS (AWS CIS, AWS PCI DSS, and AWS Foundational Security Best Practices).
  - Asset inventory page helps to manage AWS resources alongside your Azure resources.
  - The **CSPM** plan is free.
- **Microsoft Defender for Containers**
  - Brings threat detection and advanced defenses to your Amazon EKS clusters.
  - Includes Kubernetes threat protection, behavioral analytics, Kubernetes best practices, admission control recommendations
- **Microsoft Defender for Servers**
  - Threat detection and advanced defenses to your Windows and Linux EC2 instances.
  - Microsoft Defender for Endpoint, security baselines and OS level assessments,
  - Vulnerability assessment scanning, adaptive application controls (AAC), file integrity monitoring (FIM), and more.

Go Do

1. Verify the feature capabilities:
   1. Features-Container-multicloud
   2. Features-Servers -multicloud
2. Enable Defender for Containers plan,
3. Enable Defender for Servers plan
4. Connect AWS : quickstart-onboard-aws
5. Configure auto-provisioning on your subscription.
6. CSPM : View the recommendations
7. Inventory - environments filter select AWS
8. Custom assessment: Enable Custom assessment

Key Tips and Strategies

Remove classic connectors

(Recommended) Use the auto provisioning process to install Azure Arc on all of your existing and future EC2 instances. If not Install Azure Arc for servers installed on your EC2 instances

Auto provisioning is managed by AWS Systems Manager (SSM) using the SSM agent.

If you want to manually install Azure Arc on your existing and future EC2 instances, use the EC2 instances should be connected to Azure Arc recommendation to identify instances that do not have Azure Arc installed

Multi Cloud integration - GCP

Google Cloud Platform

GCP

- **Defender for Cloud's CSPM features**
  - This agentless plan
  - Assesses your GCP resources according to GCP-specific security recommendations
  - Assessed for compliance with built-in standards specific to GCP.
  - Asset inventory page helps to manage GCP resources alongside your Azure resources.
  - The **CSPM** plan is free
- **Microsoft Defender for Containers**
  - Brings threat detection and advanced defenses to your Google GKE clusters.
  - Includes Kubernetes threat protection, behavioral analytics, Kubernetes best practices, admission control recommendations
- **Microsoft Defender for Servers**
  - Threat detection and advanced defenses to GCP VMs.
  - Microsoft Defender for Endpoint, security baselines and OS level assessments,
  - vulnerability assessment scanning, adaptive application controls (AAC), file integrity monitoring (FIM), and more.

Go Do

1. Verify the feature capabilities:
    1. Features-Servers –multicloud
    2. Containers feature GCP
2. Enable Defender for Containers plan
3. Enable Defender for Servers plan
4. Connect GCP : Connect your GCP
5. Enable Auto Provisioning: Configure Server plans
6. Configure Container Plans and auto provisioning
7. CSPM : View the recommendations
8. Inventory - environments filter select GCP

Key Tips and Strategies

Make sure these accounts are created in GCP
CSPM service account reader role
Microsoft Defender for Cloud identity federation
CSPM identity pool
Microsoft Defender for Servers service account (when the servers plan is enabled)
Azure-Arc for servers onboarding service account (when the Arc for servers auto-provisioning is enabled)

If you enabled auto-provisioning(recommended), Azure Arc, and any enabled extensions will install automatically for each new resource detected.

Regulatory Compliance

Microsoft Defender for Cloud 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 requirements

By default, every subscription has the **Azure Security Benchmark** assigned. This is the Microsoft-authored, Azure-specific guidelines for security and compliance best practices based on common compliance frameworks. Learn more about Azure Security Benchmark.

Available Regulatory Stds

- PCI-DSS v3.2.1:2018
- SOC TSP
- NIST SP 800-53 R4
- NIST SP 800 171 R2
- UK OFFICIAL and UK NHS
- Canada Federal PBMM
- Azure CIS 1.1.0
- HIPAA/HITRUST
- SWIFT CSP CSCF v2020
- ISO 27001:2013
- New Zealand ISM Restricted
- CMMC Level 3
- Azure CIS 1.3.0
- NIST SP 800-53 R5
- FedRAMP H
- FedRAMP M

Go Do

Enable Defender for Cloud's enhanced security features
Add a Dashboard
Access your Regulatory compliance: Tutorial: Regulatory compliance checks
Improve your Regulatory compliance: improve compliance-posture
Generate compliance status report: Report
Integrate with Azure Event hub for continuous export: Continous export

Run workflow automation for non-compliant scenarios: Automation

Assessments run approximately every 12 hours, so you will see the impact on your compliance data only after the next run of the relevant assessment.

Integration with Sentinel and 3rd party SIEM

Sentinel

- This connector allows you to stream security alerts from Defender for Cloud into Microsoft Sentinel.
- You can view, analyze, and respond to Defender alerts and incidents in a broader organizational threat context.

3rd party SIEM

- Defender for Cloud can stream your security alerts into the most popular SIEM, SOAR, and IT Service Management (ITSM) solutions.
- The export of security alerts to Splunk and QRadar uses Event Hubs and a built-in connector.
- You can either use a PowerShell script or the Azure portal to set up the requirements for exporting security alerts for your subscription or tenant.
- Then, you'll need to use the procedure specific to each SIEM to install the solution in the SIEM platform.

Go Do

1. If you use Microsoft Sentinel:
   a) Review Connect Microsoft Defender for Cloud alerts to Microsoft Sentinel guide.
   b) Understand Microsoft Sentinel alert synchronization and bi-directional alert sync.
   c) Verify all the pre-requisites.
   d) Use the same workspace for both Microsoft Sentinel and Microsoft Defender for Cloud

2. Use this link if you want to Stream alerts to QRadar and Splunk.

3. Review the Prepare Azure resources for exporting to Splunk and QRadar.

Workflow Automation

Automation

- Automate responses to Microsoft Defender for Cloud triggers.
- This feature can trigger Logic Apps on security alerts, recommendations, and changes to regulatory compliance.
- Automation reduces overhead and can also improve your security by ensuring the process steps are done quickly, consistently, and according to your predefined requirements.

Go Do

1. Validate scenarios where you need to automate a response for a recommendation and use the Workflow Automation feature to accomplish that.
2. Use the Workflow Automation feature to create automations for recommendations. You can test to send recommendation to workload owners using instructions from this article.
3. Configure workflow automation at scale using the supplied policies.
4. Review the FAQ for more information.

Workbooks

Workbooks

- Workbooks provide a rich set of capabilities for visualizing your Azure data.
- Within Microsoft Defender for Cloud, you can access the built-in workbooks to track your organization’s security posture.
- You can also build custom workbooks to view a wide range of data from Defender for Cloud or other supported data sources.
- With the integrated Azure Workbooks functionality, Microsoft Defender for Cloud makes it straightforward to build your own custom, interactive workbooks.

Go Do

1. Some workbooks you can configure and use:

   Secure Score Over Time workbook - Track your subscriptions' scores and changes to recommendations for your resources

   System Updates workbook - View missing system updates by resources, OS, severity, and more

   Vulnerability Assessment Findings workbook - View the findings of vulnerability scans of your Azure resources

   Compliance Over Time workbook - View the status of a subscription's compliance with the regulatory or industry standards you've selected

   Active Alerts workbook - view active alerts by severity, type, tag, MITRE ATT&CK tactics, and location.

   Ransomware Dashboard - Verify the Ransomware Dashboard Based on MITRE ATT&CK® Framework

Learning Resources

Stay Informed

- Join the Defender for Cloud - Microsoft Tech Community
- Register and watch Security Community Webinars
- Follow Microsoft Defender for Cloud Blog
- Follow Defender for Cloud in the Field channel
- Defender for Cloud in the Field videos
- Microsoft Security Blog | Digital Security Tips and Solutions
- Microsoft Security Intelligence (@MsftSecIntel) / Twitter

Learn and Achieve

- Become a Defender for Cloud Ninja
- Earn the SC-200: Microsoft Security Operations Analyst
- SC-200 Learning Path
- Defender for Cloud Interactive Guide

Get Involved

- Sign up to participate in the Microsoft Azure Security Private Community
- Contribute on GitHub

Thank you