

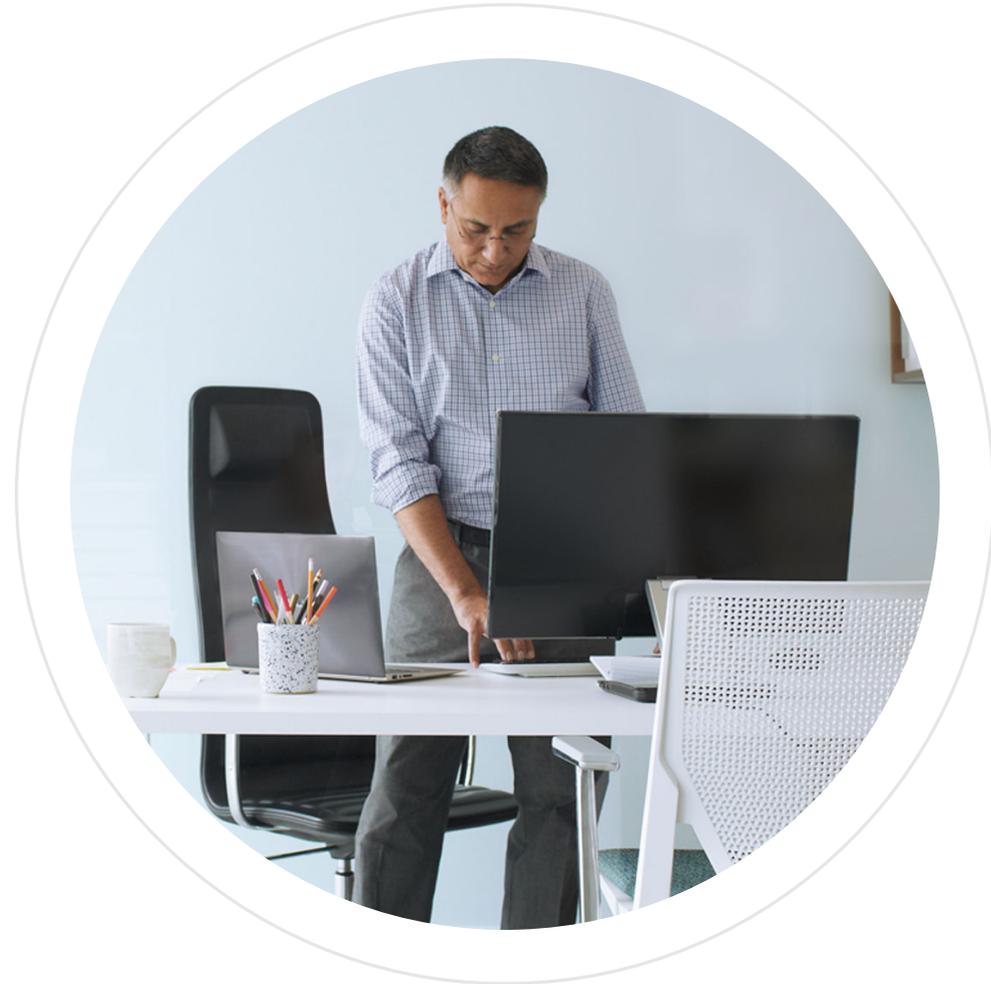


SC-200

Microsoft Security Operations Analyst

Author name

Date





Module 3: Mitigate threats using Microsoft Defender for Cloud

© Copyright Microsoft Corporation. All rights reserved.



Module agenda



Plan for cloud workload protections using Microsoft Defender for Cloud



Workload protections in Microsoft Defender for Cloud



Connect Azure assets to Microsoft Defender for Cloud



Connect non-Azure resources to Microsoft Defender for Cloud



Remediate security alerts using Microsoft Defender for Cloud

Lesson 1: Plan for cloud workload protections using Microsoft Defender for Cloud



Lesson introduction

After this lesson, you will be able to:



Describe Microsoft Defender for Cloud features



Explain Microsoft Defender for Cloud workload protections



Enable Microsoft Defender for Cloud



Explain Microsoft Defender for Cloud

-  Strengthen security posture
-  Manage organization security policy and compliance
-  Continuous assessments
-  Optimize and improve security by configuring recommended controls
-  Network map
-  Automatically discover and onboard Azure resources with automatic provisioning

Guided demonstration – Microsoft Defender for Cloud

Scenario:

You are the security operations analyst and must protect your hybrid cloud with Microsoft Defender for Cloud.

Task 1

Manage cloud security posture

Task 2

Protect against threats

Task 3

Get advanced insights

Microsoft Defender for Cloud workload protections

Microsoft Defender for Cloud, brings advanced, intelligent protection to your Azure and hybrid resources and workloads.

 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	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
 App Service	0 instances	Instance/Month	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
 Azure SQL Databases	0 servers	Server/Month	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off
 SQL servers on machines	0 servers	Server/Month Core/Hour	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off
 Open-source relational databases	0 servers	Server/Month	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off
 Storage	3 storage accounts	10k transactions	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
 Kubernetes	18 kubernetes cores	VM core/Month	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
 Container registries	0 container registries	Image	<input type="checkbox"/> On <input checked="" type="checkbox"/> Off
 Key Vault	1 key vaults	10k transactions	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
 Resource Manager		1M resource mana...	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off
 DNS		1M DNS queries	<input checked="" type="checkbox"/> On <input type="checkbox"/> Off

Enable Microsoft Defender for Cloud

To enable all Defender for Cloud features including threat protection capabilities, you must enable enhanced security features on the subscription containing the applicable workloads.

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)

Lesson 2: Workload protections in Microsoft Defender for Cloud



Lesson introduction

After this lesson, you will be able to:



Explain which workloads are protected by Microsoft Defender for Cloud



Describe the benefits of the protections offered by Microsoft Defender for Cloud



Explain how Microsoft Defender for Cloud protection's function



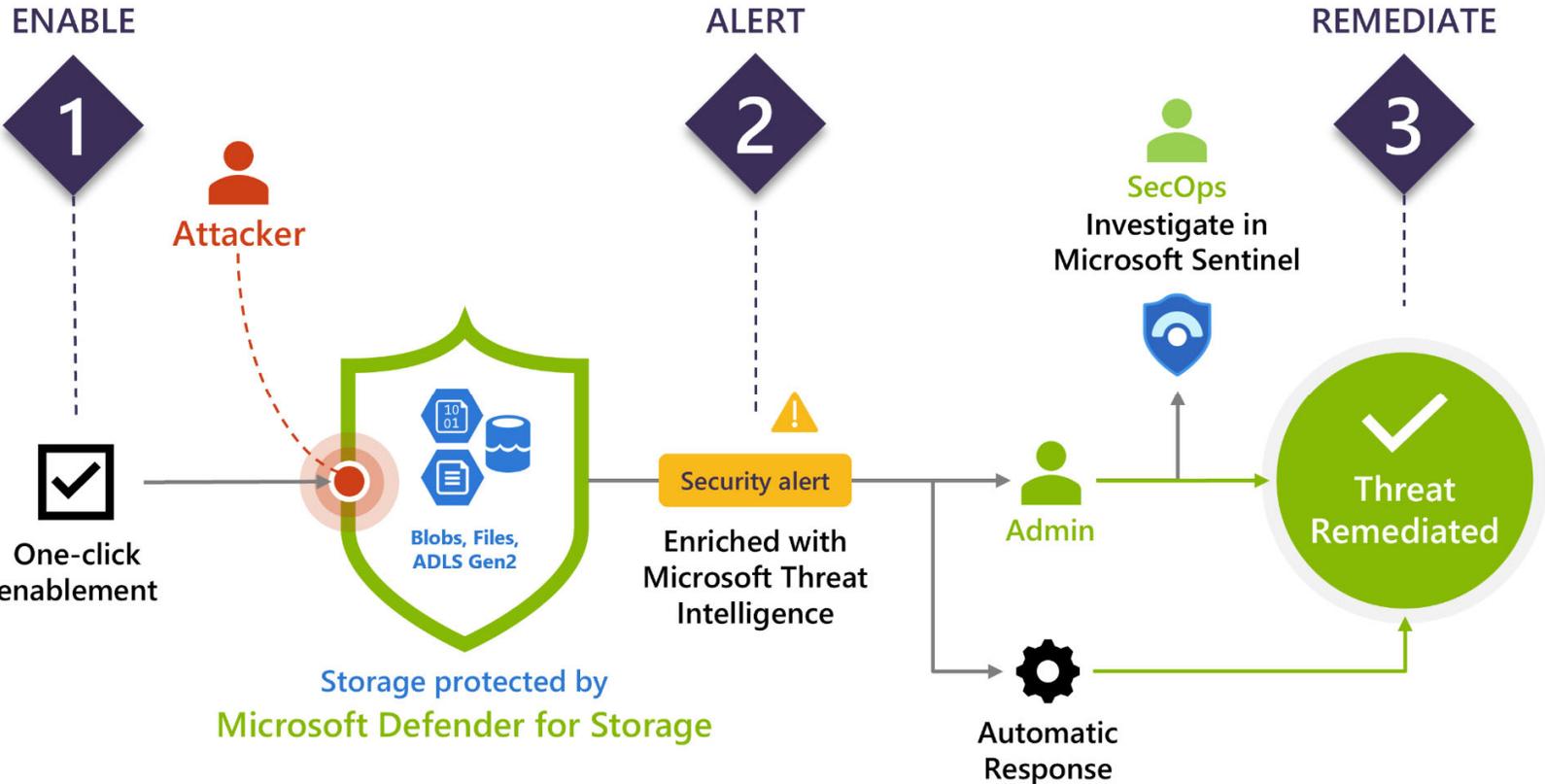
Microsoft Defender for servers

- Microsoft Defender for servers adds threat detection and advanced defenses for your Windows and Linux machines.
- For Windows, Microsoft Defender for Cloud integrates with Azure services to monitor and protect your Windows-based machines. Microsoft Defender for Cloud presents the alerts and remediation suggestions from all these services in an easy-to-use format.
- For Linux, Microsoft Defender for Cloud collects audit records from Linux machines by using auditd, one of the most common Linux auditing frameworks. auditd lives in the mainline kernel.

Microsoft Defender for App Service

- Microsoft Defender for App Service 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 learn new patterns that will be used later.

Microsoft Defender for Storage



Microsoft Defender for SQL

Microsoft Defender for SQL comprises two separate Microsoft Defender plans:

Microsoft Defender for Azure SQL database servers protects:

- Azure SQL Database
- Azure SQL Managed Instance
- Dedicated SQL pool in Azure Synapse

Microsoft Defender for SQL servers on machines extends the protections for your Azure-native SQL Servers to fully support hybrid environments and protect SQL servers (all supported version) hosted in Azure, other cloud environments, and even on-premises machines:

- SQL Server on Virtual Machines
- On-premises SQL servers:
 - Azure Arc enabled SQL Server
 - SQL Server running on Windows machines without Azure Arc

Microsoft Defender for open-source relational databases

protections for the following open-source relational databases are available for:

- Azure Database for PostgreSQL
- Azure Database for MySQL
- Azure Database for MariaDB

Microsoft Defender for Key Vault

Microsoft Defender 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.
- Address threats without the need to manage third-party security monitoring systems.

When anomalous activities occur, Microsoft Defender shows alerts and optionally sends them via email to relevant members of your organization. These alerts include the details of the suspicious activity and recommendations on how to investigate and remediate threats.

Microsoft Defender for Resource Manager

Microsoft Defender for Resource Manager automatically monitors the resource management operations in your organization, whether they're performed through:

- Azure portal
- Azure REST APIs
- Azure CLI
- other Azure programmatic clients

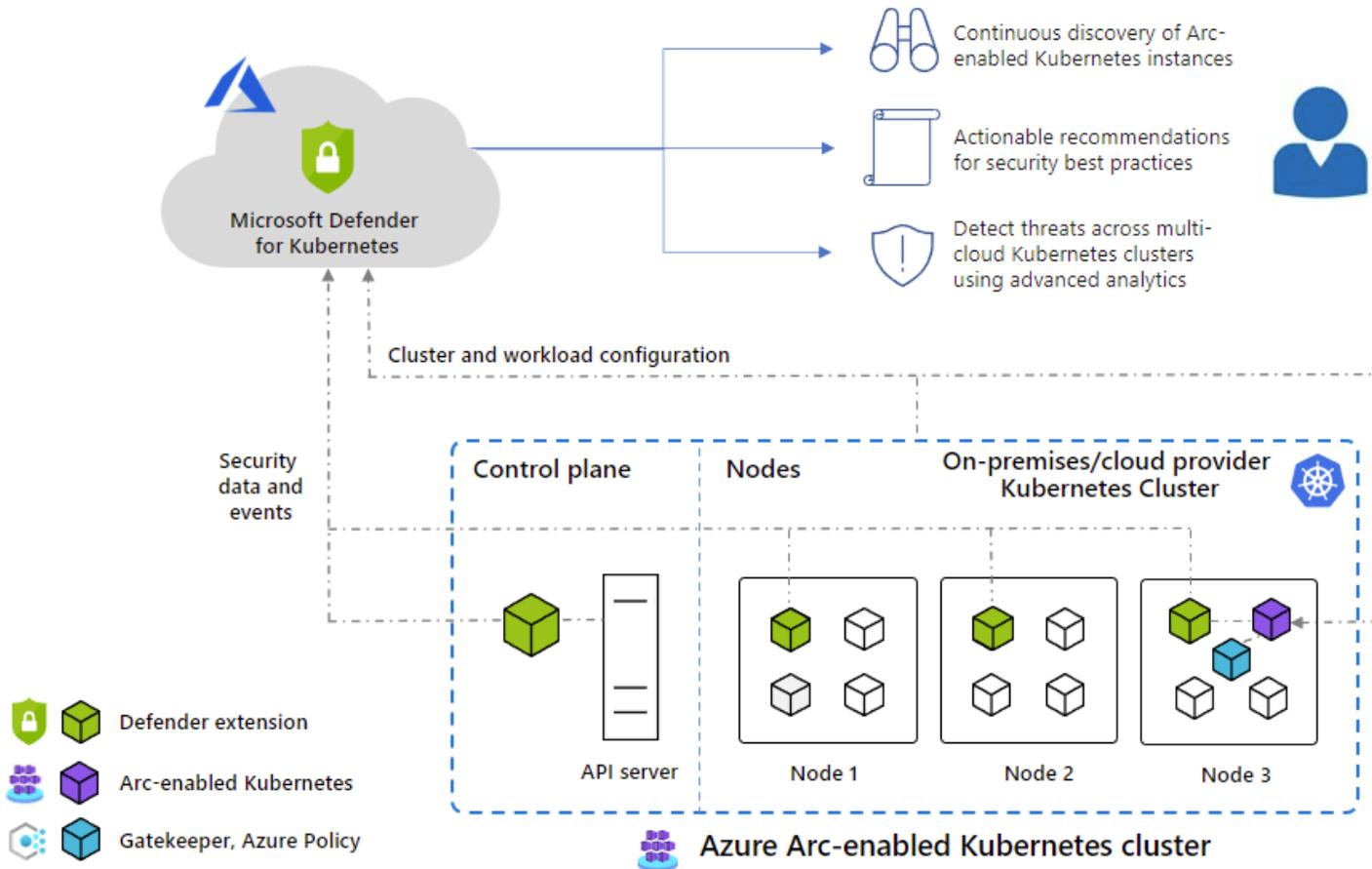
Microsoft Defender runs advanced security analytics to detect threats and alert you about suspicious activity.

Microsoft Defender for DNS

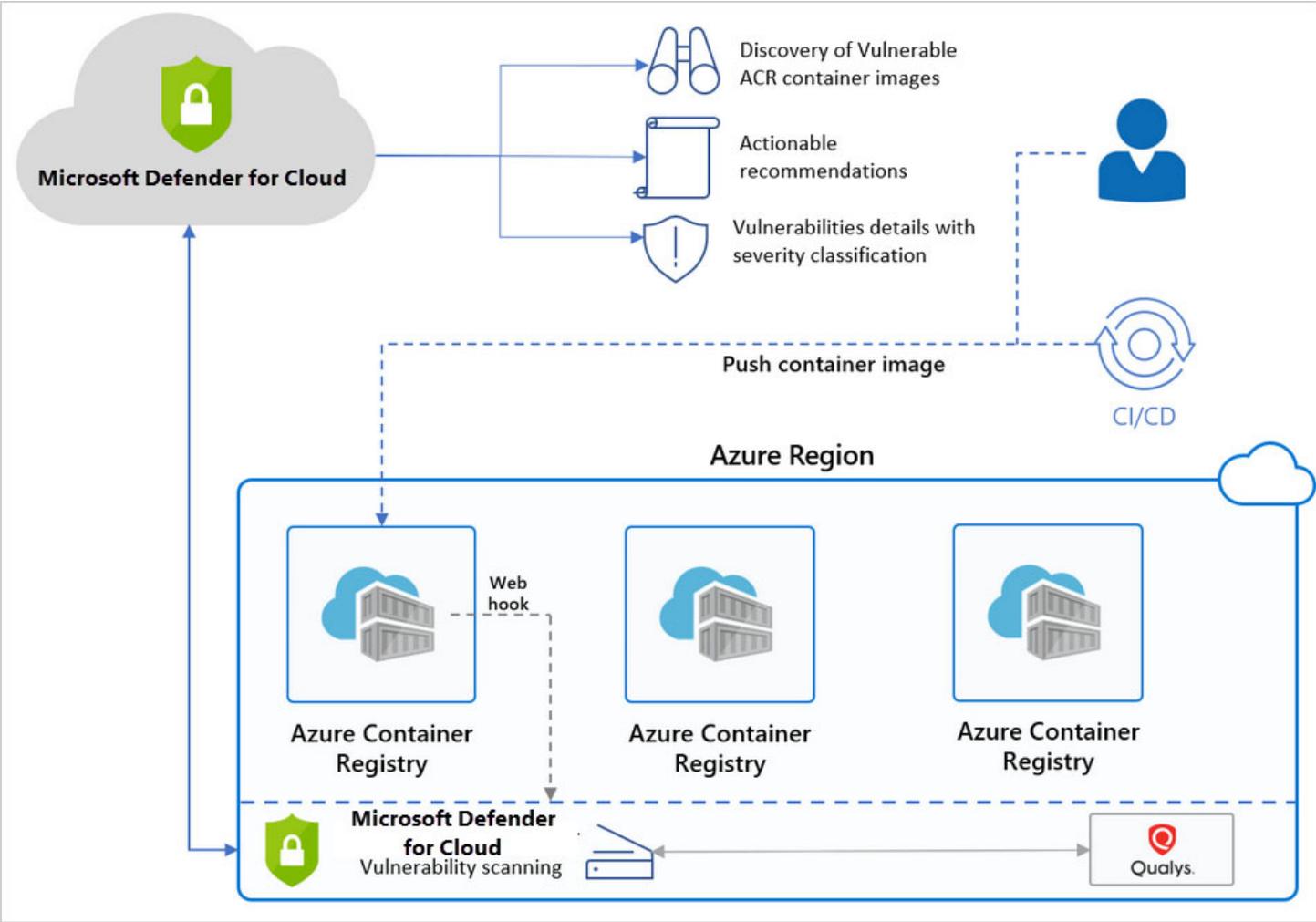
Microsoft Defender for DNS provides an extra layer of protection for your cloud resources by:

- Continuously monitoring all DNS queries from your Azure resources
- Running advanced security analytics to alert you about suspicious activity

Microsoft Defender for Kubernetes



Microsoft Defender for container registries



Microsoft Defender for Cloud more protections

Microsoft Defender for Cloud also offers the following threat protection capabilities:



Threat protection for Azure network layer



Threat protection for Azure Cosmos DB (Preview)



Display Azure WAF alerts in Microsoft Defender for Cloud



Display Azure DDoS Protection alerts in Microsoft Defender for Cloud



Display Microsoft Defender for Cloud recommendations in Defender for Cloud Apps

Lesson 3: Connect Azure assets to Microsoft Defender for Cloud



Lesson introduction

After this lesson, you will be able to:



Explore Azure assets



Configure auto-provisioning in Microsoft Defender for Cloud



Describe manual provisioning in Microsoft Defender for Cloud



Explore and manage your resources with asset inventory

Inventory Summary



Total Resources



Unhealthy Resources



Unmonitored Resources



Unregistered Subscriptions

Status For each Resource



Agent monitoring



Microsoft Defender for Cloud



Body Recommendations

Configure auto provisioning

Microsoft Defender for Cloud collects data from your Azure virtual machines (VMs), virtual machine scale sets, IaaS containers, and non-Azure (including on-premises) machines to monitor for security vulnerabilities and threats.

Settings | Auto provisioning

Search (Ctrl+/) << Save

Settings

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

Auto provisioning - Extensions

Defender for Cloud collects security data and events from your resources and services to help you prevent, detect, and respond to threats. When you enable an extension, it will be installed on any new or existing resource, by assigning a security policy. [Learn more](#)

Enable all extensions

Extension	Status	Resources missing extension	Description	Configuration
Log Analytics agent for Azure VMs	<input checked="" type="checkbox"/> On	7 of 13 virtual machines Show in inventory	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
Vulnerability assessment for machines (preview)	<input type="checkbox"/> Off ⓘ	13 of 13 virtual machines Show in inventory	Deploys vulnerability assessment to your Azure and hybrid machines. Learn more	-
Guest Configuration agent (preview)	<input type="checkbox"/> On ⓘ	8 of 13 virtual machines Show in inventory	Checks machines running in Azure and Arc Connected Machines for security misconfigurations. Settings such as configuration of the operating system, application configurations, and environment settings are all validated. To learn more, see Understand Azure Policy's Guest Configuration .	-
Microsoft Dependency agent (preview)	<input type="checkbox"/> Off ⓘ	6 of 7 virtual machines Show in inventory	You can collect and store network traffic data by onboarding to the VM Insights service. Learn more	-
Policy Add-on for Kubernetes	<input type="checkbox"/> Off ⓘ	1 of 8 managed cluster Show in inventory	Extends Gatekeeper v3, to apply at-scale enforcements and safeguards on your clusters in a centralized, consistent manner. Requires Kubernetes v1.14.0 or later. Learn more .	-

Manual log analytics agent provisioning

To manually install the Log Analytics agent on Azure VMs:

1. Disable auto provisioning.
2. Optionally, create a workspace.
3. Enable Microsoft Defender for Cloud on the workspace on which you're installing the Log Analytics agent.
4. Deploy agents on new VMs using a Resource Manager template, install the Log Analytics agent.
5. Deploy agents on your existing VMs.

Lesson 4: Connect non-Azure resources to Microsoft Defender for Cloud



Lesson introduction

After this lesson, you will be able to:



Connect non-Azure machines to Microsoft Defender for Cloud



Connect AWS accounts to Microsoft Defender for Cloud

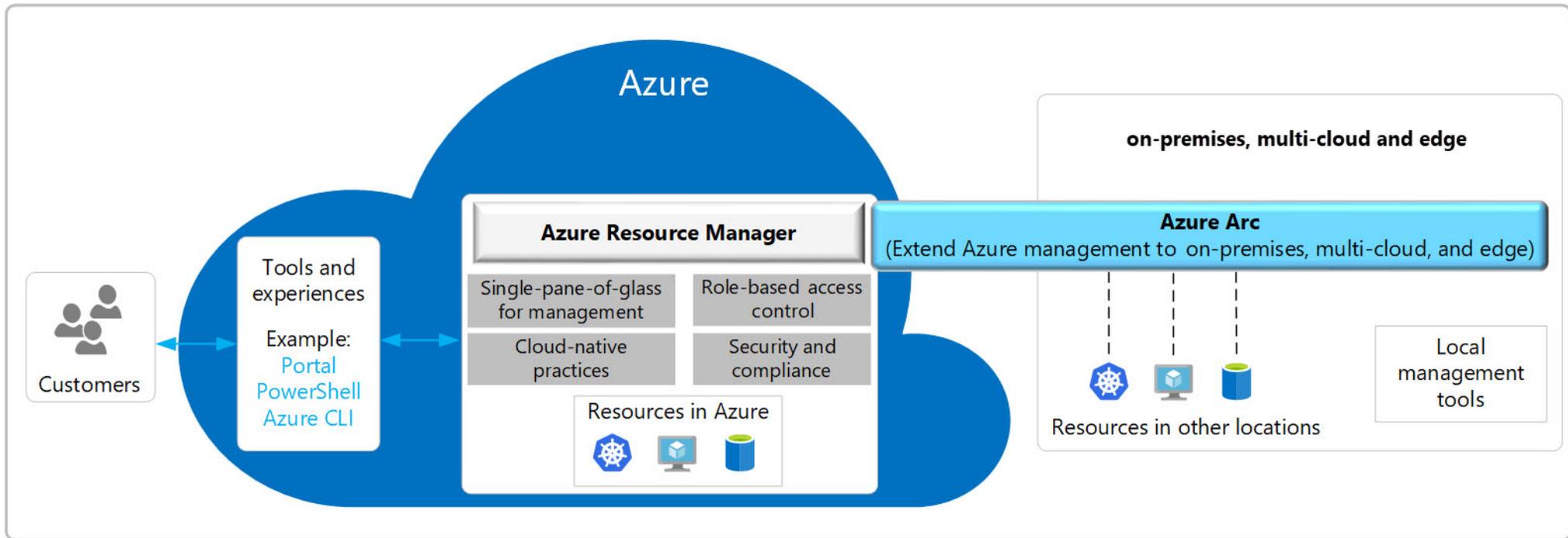


Connect GCP accounts to Microsoft Defender for Cloud



Protect non-Azure resources

Azure Arc simplifies governance and management by delivering a consistent multi-cloud and on-premises management platform.



Connect non-Azure machines

Azure Arc Enabled

Install Azure Arc agent on Host

In the Azure Portal, Connect the host.

Without Azure Arc

Manually deploy Log Analytics agent to Windows Host

Manually deploy Log Analytics agent to Linux Host

Manually deploy Log Analytics agent to Azure Stack VMs

Connect AWS accounts

Onboarding your AWS account into Microsoft Defender for Cloud, integrates AWS Security Hub. Microsoft Defender for Cloud thus provides visibility and protection across both cloud environments.

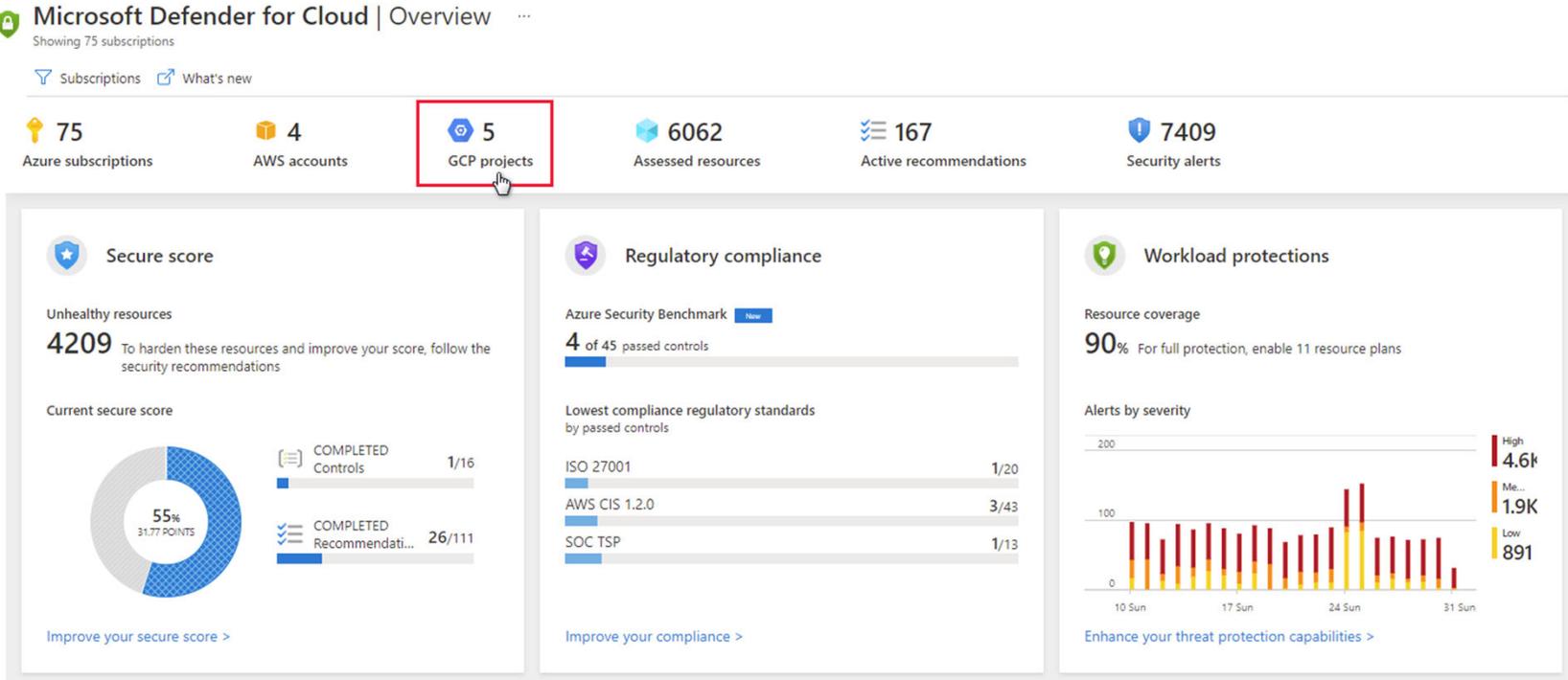
The screenshot shows the Microsoft Defender for Cloud Overview page. At the top, it says "Microsoft Defender for Cloud | Overview" and "Showing 75 subscriptions". Below this are navigation links for "Subscriptions" and "What's new". A row of metrics is displayed: "75 Azure subscriptions", "4 AWS accounts" (highlighted with a red box), "5 GCP projects", "6062 Assessed resources", "167 Active recommendations", and "7409 Security alerts".

The main content area is divided into three panels:

- Secure score:** Shows an "Unhealthy resources" score of 4209. The current secure score is 55% (31.77 points). It lists "COMPLETED Controls" as 1/16 and "COMPLETED Recommendation..." as 26/111.
- Regulatory compliance:** Shows "Azure Security Benchmark" with "4 of 45 passed controls". It lists "Lowest compliance regulatory standards by passed controls": ISO 27001 (1/20), AWS CIS 1.2.0 (3/43), and SOC TSP (1/13).
- Workload protections:** Shows "Resource coverage" at 90%. It includes a bar chart for "Alerts by severity" with a legend for High (4.6k), Medium (1.9K), and Low (891).

Connect your GCP accounts

Onboarding your GCP account into Microsoft Defender for Cloud, integrates GCP Security Commands. Microsoft Defender for Cloud thus provides visibility and protection across both cloud environments.



Lesson 5: Remediate security alerts using Microsoft Defender for Cloud



Lesson introduction

After this lesson, you will be able to:



Describe alerts in Microsoft Defender for Cloud



Remediate alerts in Microsoft Defender for Cloud



Automate responses in Microsoft Defender for Cloud



Explain security alerts



Security alerts and incidents



Detecting Threats



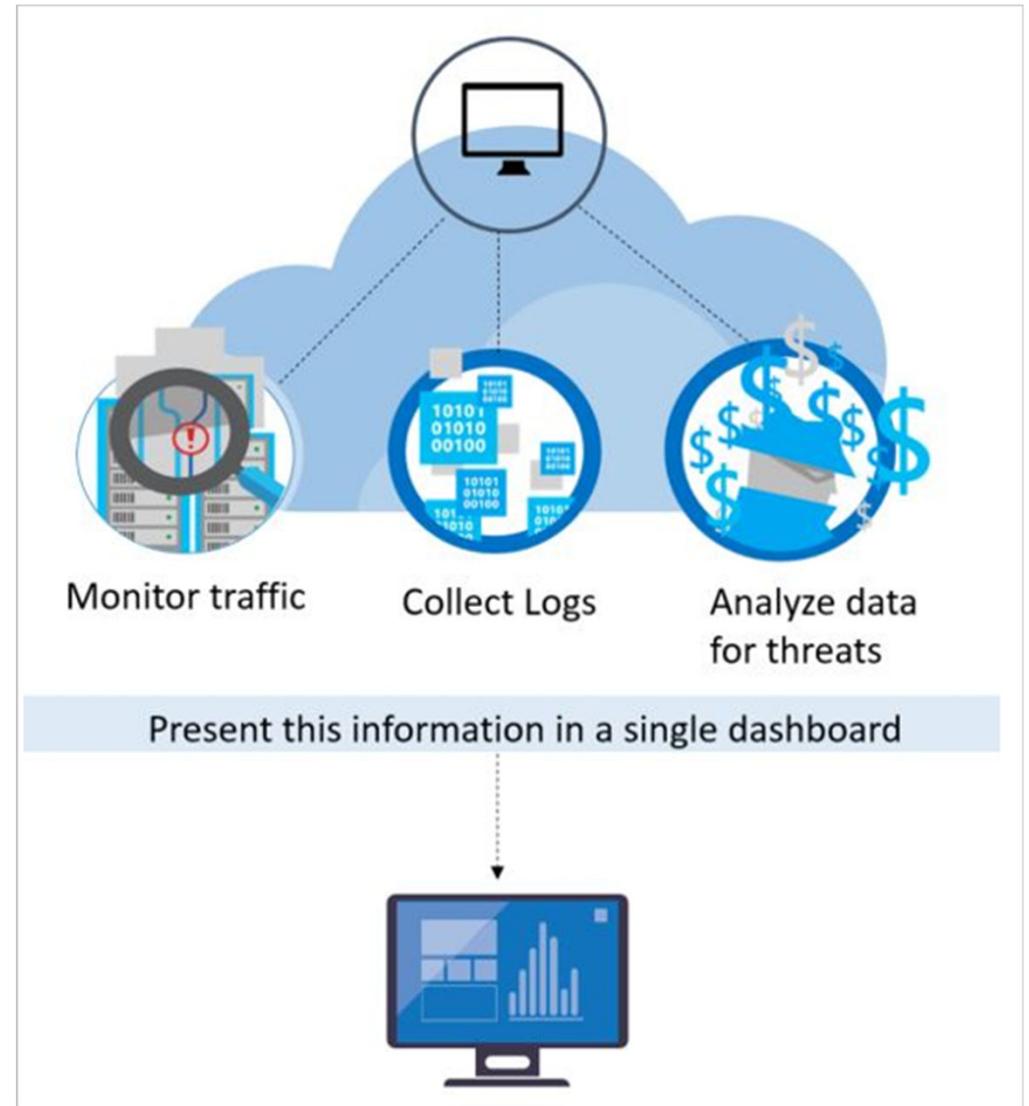
Alert classification



Continuous monitoring and assessments



Alert types



Remediate alerts

Microsoft Defender for Cloud provides actionable tasks to mitigate the threat, prevent future attacks, trigger automated response, suppress similar alerts.

The screenshot displays the Microsoft Defender for Cloud interface for a security alert. The alert is titled "Potential SQL Injection" with ID "25181-892ad5bb9a". It is categorized as "High Severity" and "Active" status, with an activity time of "06/11/20, 1...".

Alert description: Potential SQL Injection was detected on your database Demo on server R-DEV\SQLEXPRESS.

Affected resource:

- R-DEV (Azure Arc machine, Env: Development)
- DS-ThreatDetection_Demo (Subscription)

Intent: Pre-attack

Alert details and Take action options:

- Mitigate the threat:** Read more about SQL Injection threats and best practices for safe application code. You have 34 more alerts on the affected resource. [View all >>](#)
- Prevent future attacks:** Your top 2 active security recommendations on RONMAT-DEV:
 - Medium: Windows Defender Exploit Guard should be enabled on your machines
 - High: Vulnerabilities on your SQL servers on machine should be remediatedSolving security recommendations can prevent future attacks by reducing attack surface. [View all 2 recommendations >>](#)
- Trigger automated response**
- Suppress similar alerts (preview)**

Next: Take Action >>

Was this useful? Yes No

Remediate alerts (continued)

Create a logic app and define when it should automatically run.

The screenshot shows the Microsoft Defender for Cloud 'Workflow automation' page. The left sidebar has 'Workflow automation' selected (1). The main area has a '+ Add workflow automation' button (2). A dialog box titled 'Add workflow automation' (3) is open, showing the 'General' tab with fields for Name, Description, Subscription (ADF Test sub - App Model V2), and Resource group. The 'Trigger conditions' section has 'Defender for Cloud data type' set to 'Security alert'. The 'Alert name contains' and 'Alert severity' (All severities selected) fields are also visible. The 'Actions' section prompts for a Logic App name. 'Create' and 'Cancel' buttons are at the bottom of the dialog.

Name	Status	Scope
DuduTe...	Disabled	ASC DEV
DuduTe...	Disabled	ASC DEV
RonnyTest	Disabled	ASC DEV
rr_reg_c...	Disabled	ASC DEV
test	Disabled	private-b
yoafrTes...	Disabled	ASC DEV
EnabeA...	Enabled	ASC Mult
Encrypt...	Enabled	ASC Mult
KerenN...	Enabled	ASC DEV
KerenSh...	Enabled	ASC DEV
KerenTe...	Enabled	ASC DEV
MorAuto	Enabled	ASC DEV
NewDes...	Enabled	ASCDEM

Suppress alerts from Microsoft Defender for Cloud

A suppression rule can be useful to suppress alerts that you've identified as false positives or alerts that are being triggered too often to be useful.

Create suppression rule in order to automatically dismiss alerts by pre-defined conditions. [Learn more >](#)

Rule Conditions

Subscription *
ASC DEMO

Alerts * ⓘ
 Custom All

Exposed Kubernetes dashboard detected

Entities ⓘ
Type Field Value

Rule details

Rule name * ⓘ

State *
Enabled

Reason *
Select a reason

Comment
Add your comment

Rule expiration
Set an end date and time for this rule ⓘ
08/16/2021 12:01:47 PM

Test your rule Simulate

[Share your opinion regarding our new alert suppression rules. Click here to send us feedback >](#)

Manage threat intelligence reports

Reports include: Activity Group, Campaign, Threat Summary



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

Respond to alerts from Azure resources

Respond to Microsoft
Defender for Key Vault alerts



Respond to Microsoft
Defender for DNS alerts



Respond to Microsoft
Defender for Resource
Manager alerts





Knowledge check



Check your knowledge with the module quiz in your course viewer

Module 3, Lab 01 – Mitigate threats using Microsoft Defender for Cloud



Lab Exercises for module 3

1 Enable Microsoft Defender for Cloud

2 Mitigate threats using Microsoft Defender for Cloud

