CANAL DA CLOUD

Curso SC 200

Microsoft Security Operation Analitcs

Curso de Preparação para Realização do Exame de Certificação SC 200.

Instrutor: Célio Ramos

Formação: Graduado em Segurança da Informação e Pós-graduado em Gerenciamento de Projetos e MBA Gestão de Qualidade de Software e 14x Microsoft Azure

Microsoft 365
CERTIFIED
SECURITY ADMINISTRATOR
ASSOCIATE

Microsoft
CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

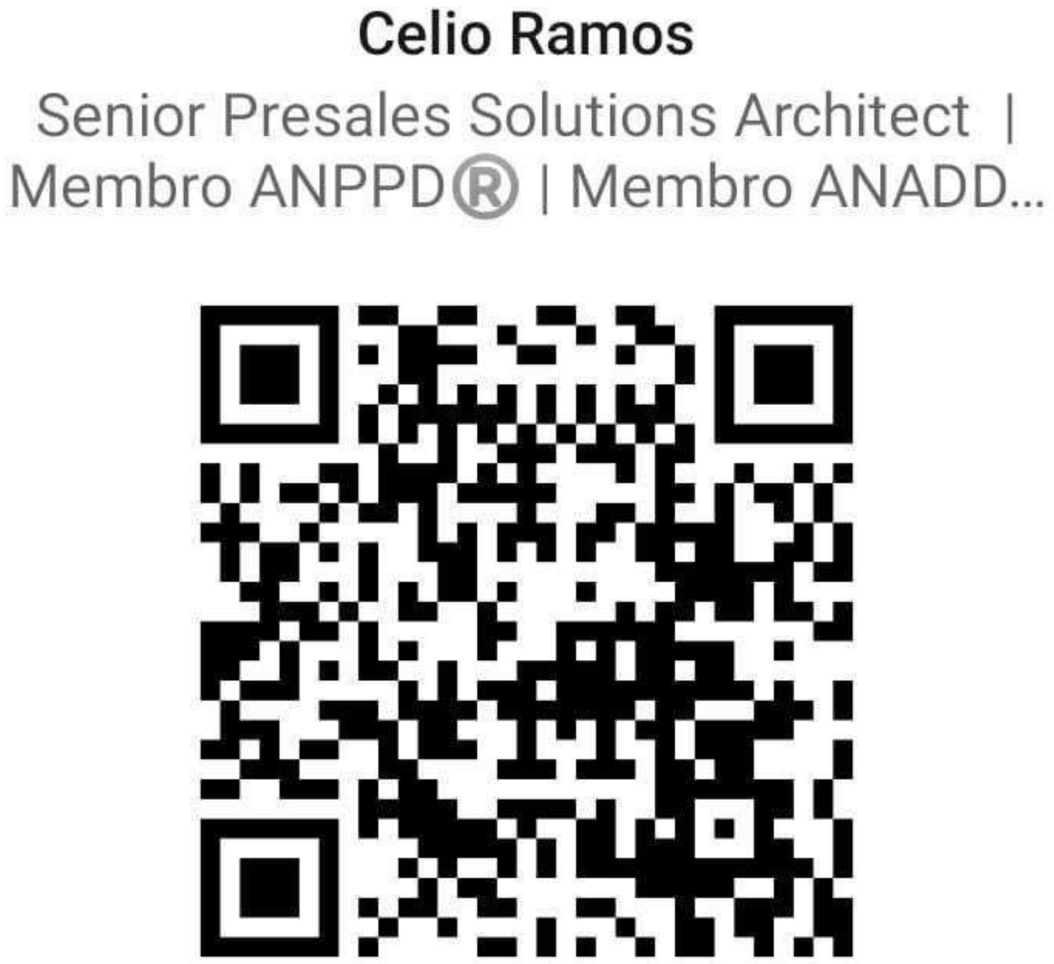
MICROSOFT CERTIFIED TRAINER
Microsoft
MCT
Trainer
2023 - 2024

Microsoft
CERTIFIED
DEVOPS ENGINEER
EXPERT

Microsoft
CERTIFIED
AZURE SOLUTIONS ARCHITECT
EXPERT

Microsoft
CERTIFIED
CYBERSECURITY ARCHITECT
EXPERT

Meio de Contato:



Celio Ramos

Senior Presales Solutions Architect | Membro ANPPD® | Membro ANADD...

bora
lá

Certification areas (SC-200)

Study areas	Weights
Mitigate threats using Microsoft 365 Defender	25-30%
Mitigate threats using Microsoft Defender for Cloud	25-30%
Mitigate threats using Microsoft Sentinel	40-45%

- This course maps to the exam SC-200: Microsoft Security Operations Analyst
- Percentages indicate the relative weight of each area on the exam.
- The higher the percentage, the more questions you are likely to see in that area.

Microsoft Security

Learning Path 3: Mitigate threats using Microsoft Defender for Cloud

© Copyright Microsoft Corporation. All rights reserved.

Certification areas (SC-200)

Study areas	Weights
Mitigate threats using Microsoft 365 Defender (OK)	25-30%
Mitigate threats using Microsoft Defender for Cloud	25-30%
Mitigate threats using Microsoft Sentinel	40-45%

- This course maps to the exam SC-200: Microsoft Security Operations Analyst
- Percentages indicate the relative weight of each area on the exam.
- The higher the percentage, the more questions you are likely to see in that area.

Learning Path agenda

- Plan for cloud workload protections using Microsoft Defender for Cloud
- Connect Azure assets to Microsoft Defender for Cloud
- Connect non-Azure assets to Microsoft Defender for Cloud
- Manage your cloud security posture management
- Workload protections in Microsoft Defender for Cloud
- Remediate security alerts using Microsoft Defender for Cloud

© Copyright Microsoft Corporation. All rights reserved.

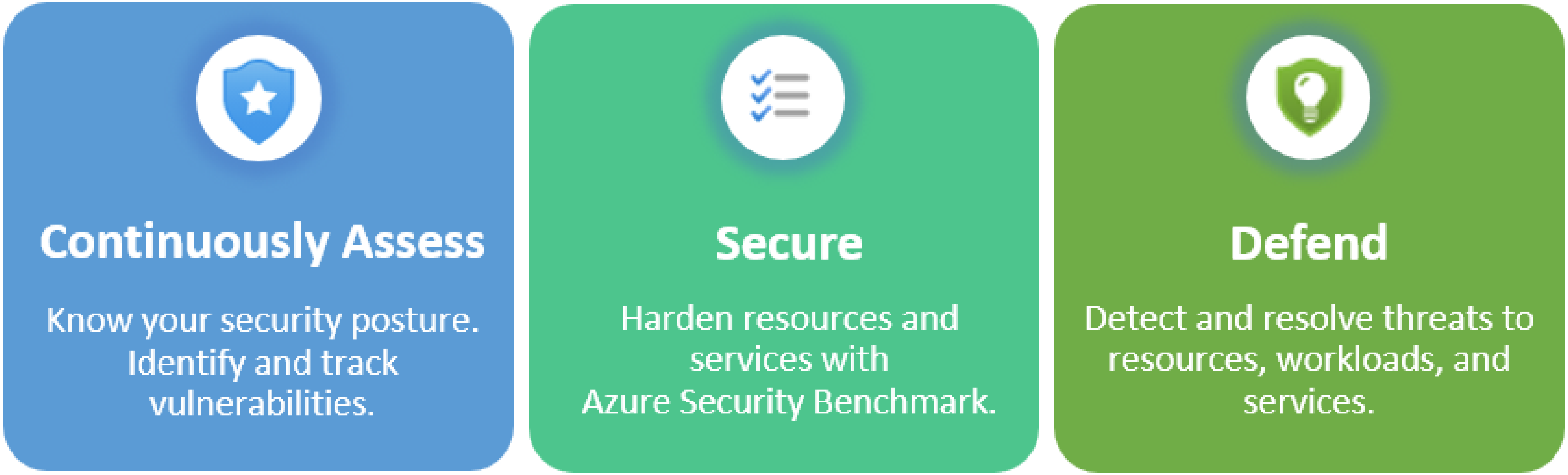
Plan for cloud workload protections using Microsoft Defender for Cloud

Introduction

After completing this module, 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



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.

A pontuação de segurança do Defender para Nuvem avalia continuamente sua postura de segurança para que você possa acompanhar novas oportunidades de segurança e relatar com precisão o andamento de suas iniciativas de segurança.

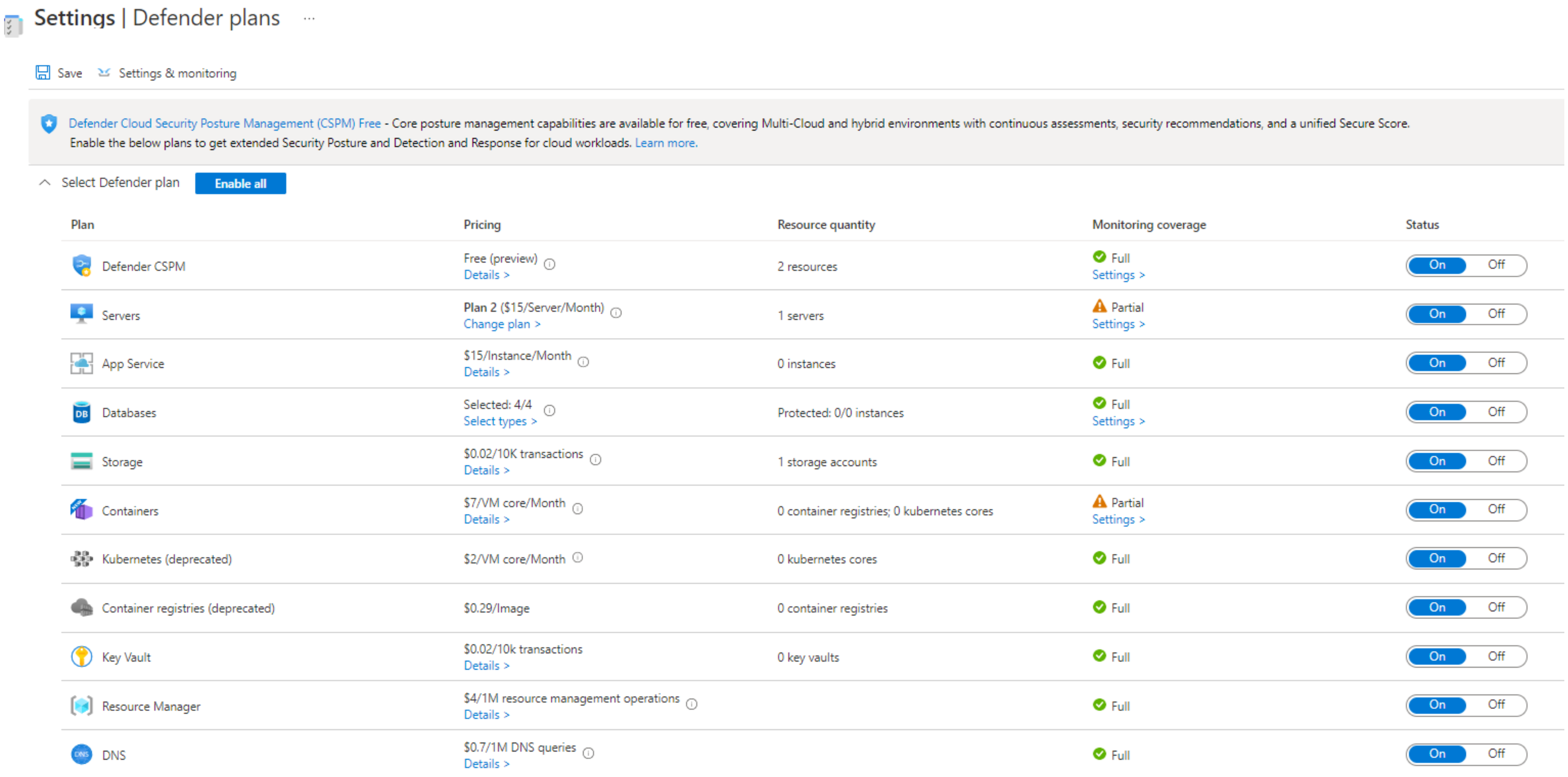
As recomendações do Defender para Nuvem protegem suas cargas de trabalho com ações detalhadas para proteger cargas de trabalho contra riscos de segurança conhecidos.

Os alertas do Defender para Nuvem defendem suas cargas de trabalho em tempo real para que você possa reagir imediatamente e evitar o desenvolvimento de eventos de segurança.

© Copyright Microsoft Corporation. All rights reserved.

Microsoft Defender for Cloud workload protection plans

O Microsoft Defender para Nuvem traz proteção avançada e inteligente para o Azure e recursos e cargas de trabalho híbridos.



Settings | Defender plans ···

Save Settings & monitoring

Defender Cloud Security Posture Management (CSPM) Free - Core posture management capabilities are available for free, covering Multi-Cloud and hybrid environments with continuous assessments, security recommendations, and a unified Secure Score. Enable the below plans to get extended Security Posture and Detection and Response for cloud workloads. Learn more.

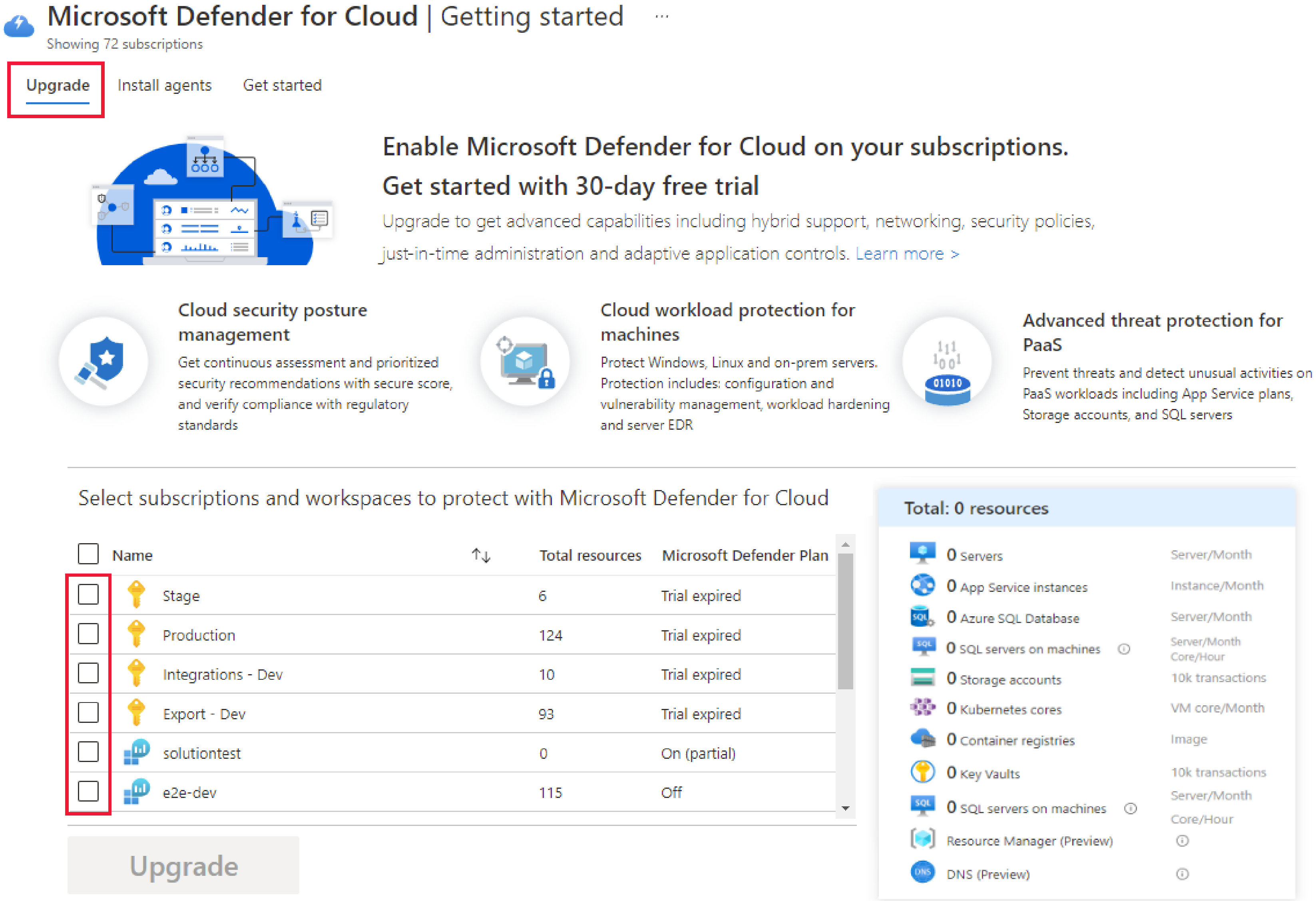
Select Defender plan Enable all

Plan	Pricing	Resource quantity	Monitoring coverage	Status
Defender CSPM	Free (preview) Details >	2 resources	✓ Full Settings >	On Off
Servers	Plan 2 ($15/Server/Month) Change plan >	1 servers	⚠ Partial Settings >	On Off
App Service	$15/Instance/Month Details >	0 instances	✓ Full	On Off
Databases	Selected: 4/4 Select types >	Protected: 0/0 instances	✓ Full Settings >	On Off
Storage	$0.02/10K transactions Details >	1 storage accounts	✓ Full	On Off
Containers	$7/VM core/Month Details >	0 container registries; 0 kubernetes cores	⚠ Partial Settings >	On Off
Kubernetes (deprecated)	$2/VM core/Month	0 kubernetes cores	✓ Full	On Off
Container registries (deprecated)	$0.29/Image	0 container registries	✓ Full	On Off
Key Vault	$0.02/10k transactions Details >	0 key vaults	✓ Full	On Off
Resource Manager	$4/1M resource management operations Details >		✓ Full	On Off
DNS	$0.7/1M DNS queries Details >		✓ Full	On Off

© Copyright Microsoft Corporation. All rights reserved.

Enable Microsoft Defender for Cloud

Para habilitar todos os recursos do Defender for Cloud, incluindo recursos de proteção contra ameaças, você deve habilitar recursos de segurança aprimorados na assinatura que contém as cargas de trabalho aplicáveis.



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

□	Name ↑↓	Total resources	Microsoft Defender Plan
□	Stage	6	Trial expired
□	Production	124	Trial expired
□	Integrations - Dev	10	Trial expired
□	Export - Dev	93	Trial expired
□	solutiontest	0	On (partial)
□	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)	ⓘ

© Copyright Microsoft Corporation. All rights reserved.

Connect Azure assets to Microsoft Defender for Cloud

Introduction

After completing this module, 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 de Recursos

Recursos insalubres

Recursos não monitorados

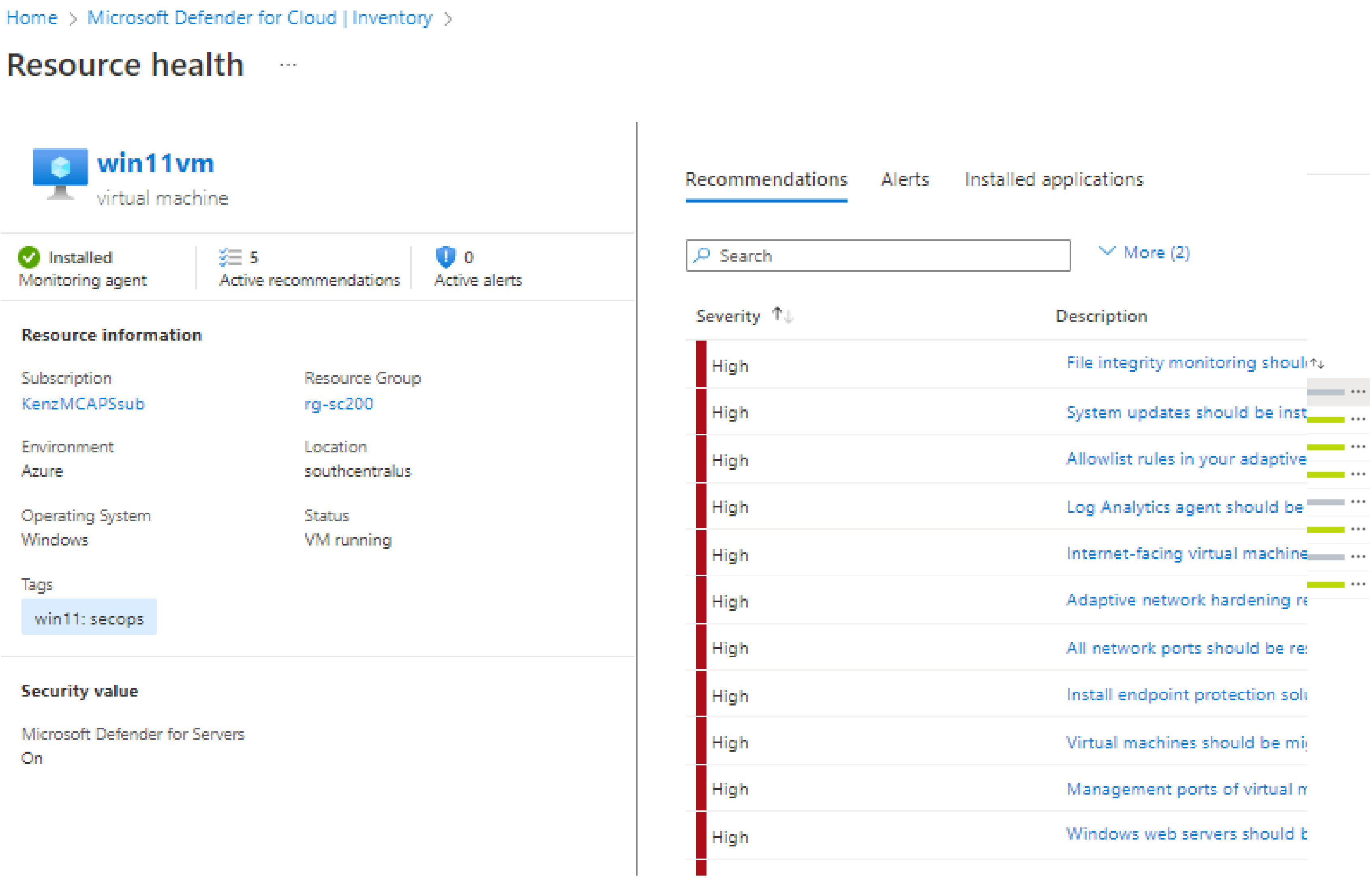
Assinaturas não registradas

Status For each Resource

Monitoramento de agentes

Microsoft Defender para nuvem

Recomendações do Corpo



Home > Microsoft Defender for Cloud | Inventory >

Resource health ...

win11vm
virtual machine

✓ Installed
Monitoring agent

5
Active recommendations

0
Active alerts

Resource information

Subscription
KenzMCAPSsub

Resource Group
rg-sc200

Environment
Azure

Location
southcentralus

Operating System
Windows

Status
VM running

Tags
win11: secops

Security value

Microsoft Defender for Servers
On

Recommendations | Alerts | Installed applications

Search

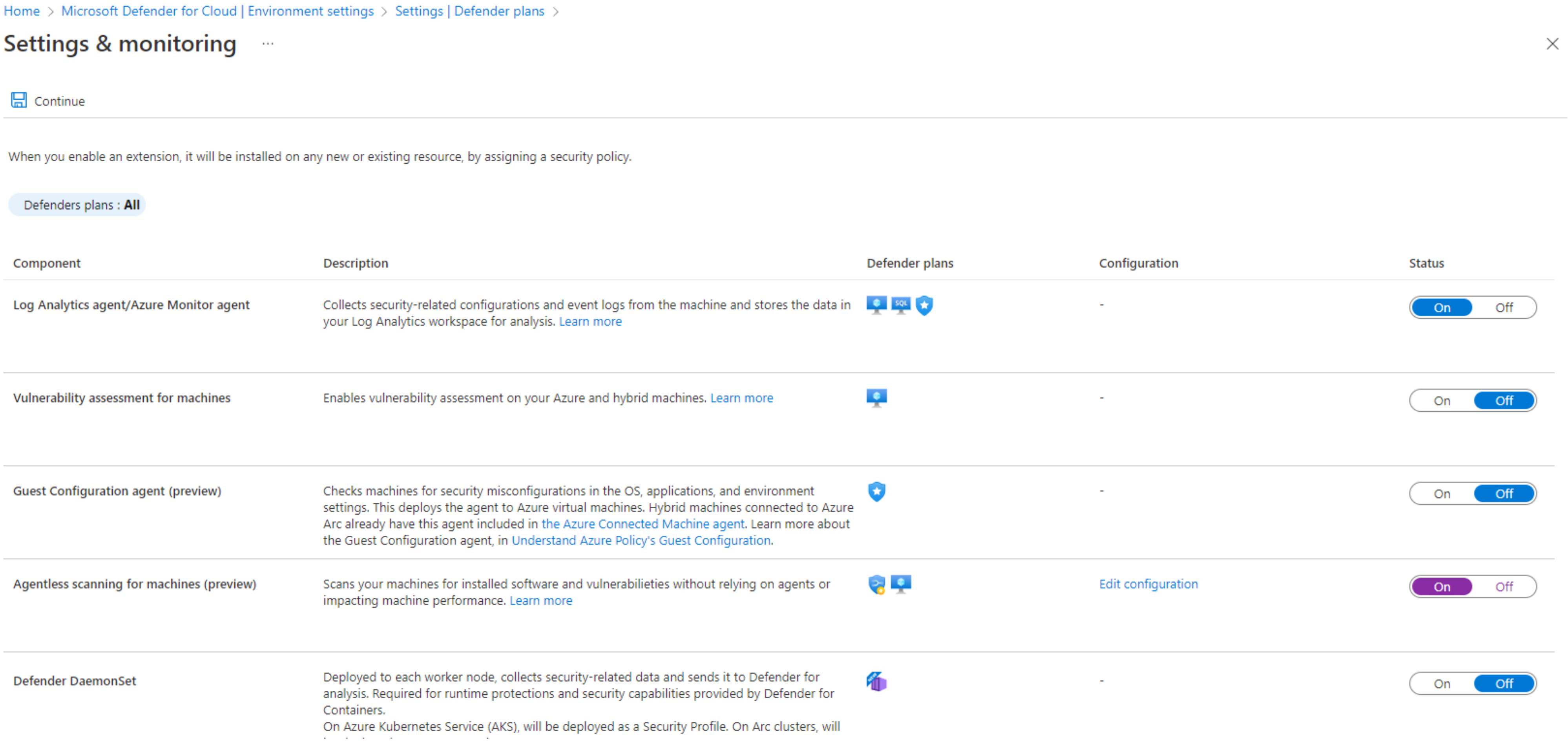
More (2)

Severity ↑↓	Description
High	File integrity monitoring shoul
High	System updates should be inst
High	Allowlist rules in your adaptive
High	Log Analytics agent should be
High	Internet-facing virtual machine
High	Adaptive network hardening re
High	All network ports should be re
High	Install endpoint protection solu
High	Virtual machines should be mi
High	Management ports of virtual m
High	Windows web servers should b

© Copyright Microsoft Corporation. All rights reserved.

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.



Home > Microsoft Defender for Cloud | Environment settings > Settings | Defender plans >

Settings & monitoring

When you enable an extension, it will be installed on any new or existing resource, by assigning a security policy.

Defenders plans : **All**

Component	Description	Defender plans	Configuration	Status
Log Analytics agent/Azure Monitor agent	Collects security-related configurations and event logs from the machine and stores the data in your Log Analytics workspace for analysis. Learn more		-	[✓ On] Off
Vulnerability assessment for machines	Enables vulnerability assessment on your Azure and hybrid machines. Learn more		-	On [✓ Off]
Guest Configuration agent (preview)	Checks machines for security misconfigurations in the OS, applications, and environment settings. This deploys the agent to Azure virtual machines. Hybrid machines connected to Azure Arc already have this agent included in the Azure Connected Machine agent. Learn more about the Guest Configuration agent, in Understand Azure Policy's Guest Configuration.		-	On [✓ Off]
Agentless scanning for machines (preview)	Scans your machines for installed software and vulnerabilieties without relying on agents or impacting machine performance. Learn more		Edit configuration	[✓ On] Off
Defender DaemonSet	Deployed to each worker node, collects security-related data and sends it to Defender for analysis. Required for runtime protections and security capabilities provided by Defender for Containers. On Azure Kubernetes Service (AKS), will be deployed as a Security Profile. On Arc clusters, will		-	On [✓ Off]

© Copyright Microsoft Corporation. All rights reserved.

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.

© Copyright Microsoft Corporation. All rights reserved.

Connect non-Azure assets to Microsoft Defender for Cloud

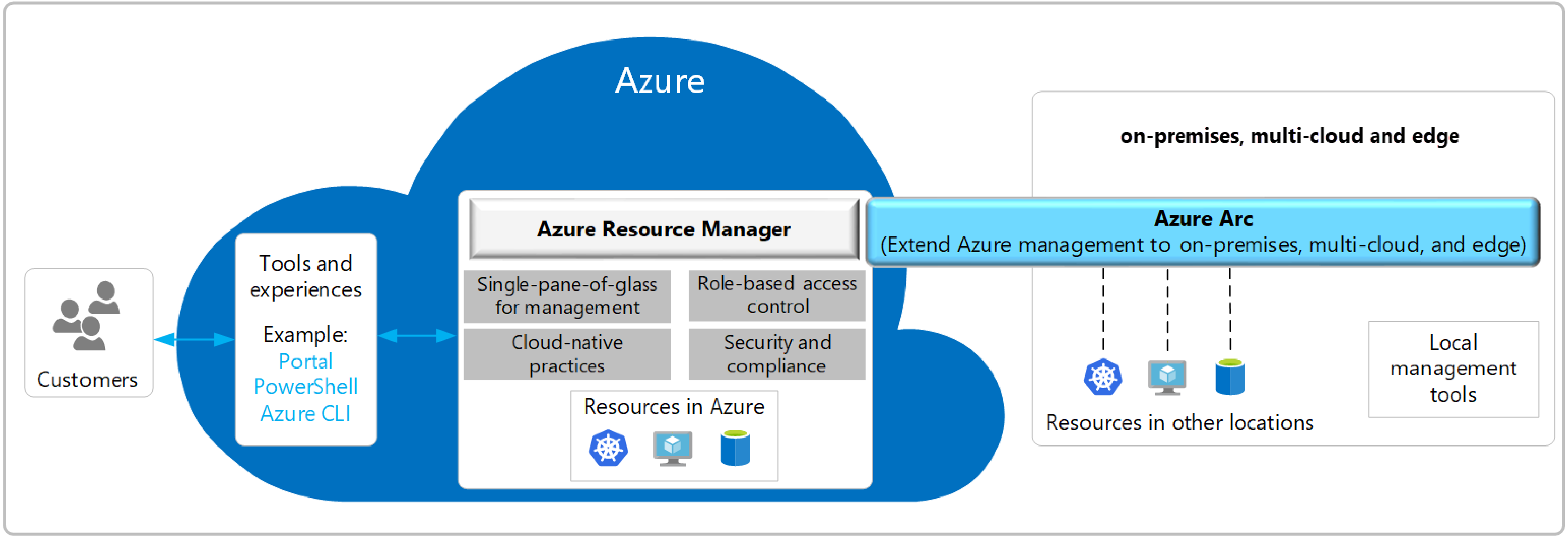
Introduction

After completing this module, you will be able to:

- Connect non-Azure machines to Microsoft Defender for Cloud
- Connect AWS accounts to Microsoft Defender for Cloud
- Connect GCP projects to Microsoft Defender for Cloud

Protect non-Azure resources

O Azure Arc simplifica a governança e o gerenciamento, fornecendo uma plataforma de gerenciamento consistente em várias nuvens e no local.


Azure
Customers
Tools and experiences
Example:
Portal
PowerShell
Azure CLI
Azure Resource Manager
Single-pane-of-glass for management
Role-based access control
Cloud-native practices
Security and compliance
Resources in Azure
on-premises, multi-cloud and edge
Azure Arc
(Extend Azure management to on-premises, multi-cloud, and edge)
Resources in other locations
Local management tools

© Copyright Microsoft Corporation. All rights reserved.

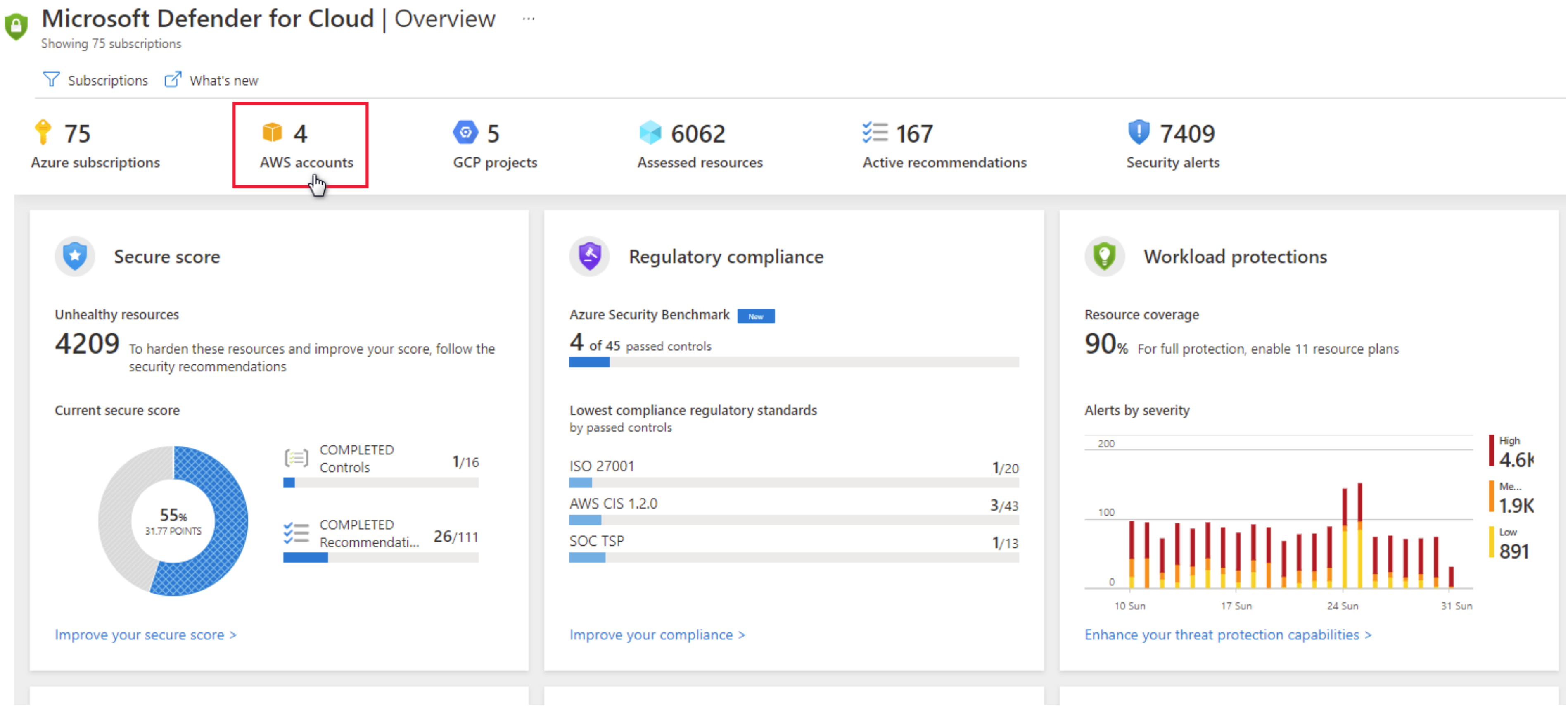
Connect non-Azure machines

Azure Arc Enabled	Without Azure Arc
Install Azure Arc agent on Host	Manually deploy Log Analytics agent to Windows Host
In the Azure Portal, Connect the host.	Manually deploy Log Analytics agent to Linux Host
	Manually deploy Log Analytics agent to Azure Stack VMs

© Copyright Microsoft Corporation. All rights reserved.

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.



Microsoft Defender for Cloud | Overview ···

Showing 75 subscriptions

Subscriptions What's new

75 Azure subscriptions

4 AWS accounts

5 GCP projects

6062 Assessed resources

167 Active recommendations

7409 Security alerts

Secure score

Unhealthy resources

4209 To harden these resources and improve your score, follow the security recommendations

Current secure score

55% 31.77 POINTS

COMPLETED Controls 1/16

COMPLETED Recommendati... 26/111

Improve your secure score >

Regulatory compliance

Azure Security Benchmark New

4 of 45 passed controls

Lowest compliance regulatory standards by passed controls

ISO 27001 1/20

AWS CIS 1.2.0 3/43

SOC TSP 1/13

Improve your compliance >

Workload protections

Resource coverage

90% For full protection, enable 11 resource plans

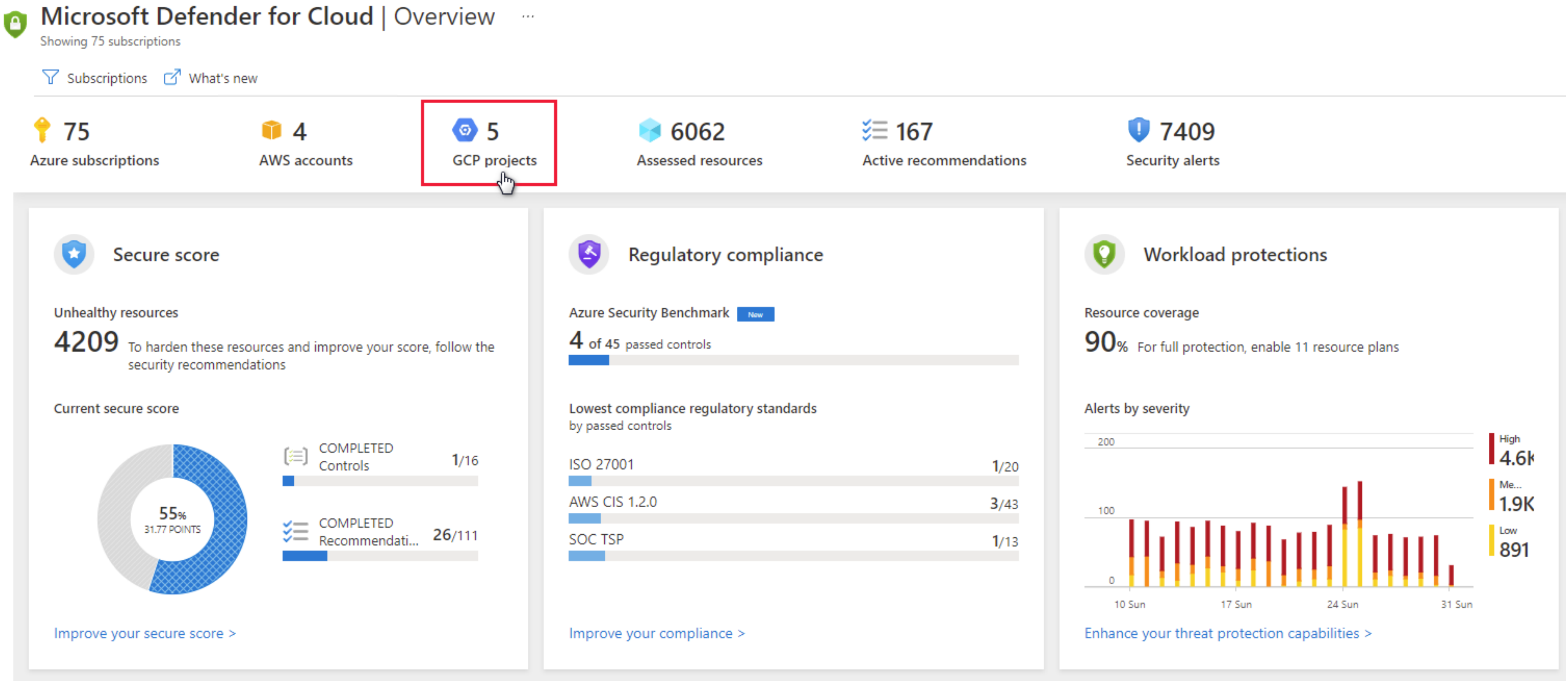
Alerts by severity

Enhance your threat protection capabilities >

© Copyright Microsoft Corporation. All rights reserved.

Connect your GCP projects

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



Microsoft Defender for Cloud | Overview ...

Showing 75 subscriptions

Subscriptions   What's new

75 Azure subscriptions | 4 AWS accounts | 5 GCP projects | 6062 Assessed resources | 167 Active recommendations | 7409 Security alerts

Secure score

Unhealthy resources

4209 To harden these resources and improve your score, follow the security recommendations

Current secure score

55% 31.77 POINTS

COMPLETED Controls 1/16

COMPLETED Recommendati... 26/111

Improve your secure score >

Regulatory compliance

Azure Security Benchmark New

4 of 45 passed controls

Lowest compliance regulatory standards by passed controls

ISO 27001 1/20

AWS CIS 1.2.0 3/43

SOC TSP 1/13

Improve your compliance >

Workload protections

Resource coverage

90% For full protection, enable 11 resource plans

Alerts by severity

Enhance your threat protection capabilities >

© Copyright Microsoft Corporation. All rights reserved.

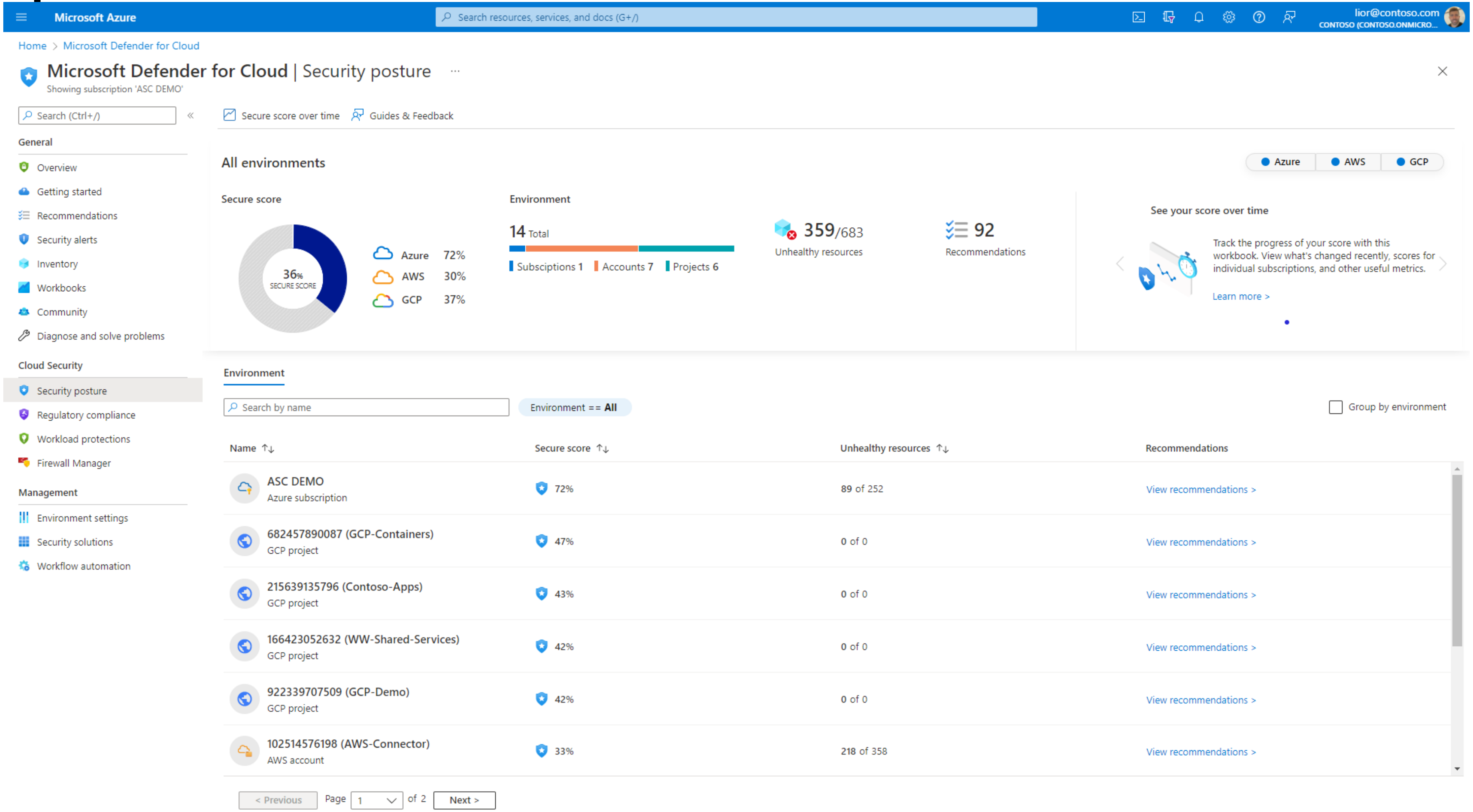
Manage cloud security posture management in Microsoft Defender for Cloud

Introduction

After completing this module, you will be able to:

- Describe the Microsoft Defender for Cloud Secure Score
- Describe how Microsoft Defender for Cloud works with industry standards, and benchmarks
- Explain the Microsoft Defender for Cloud security posture management protections for your resources

Explore Secure Score



Microsoft Defender for Cloud | Security posture

Showing subscription 'ASC DEMO'

All environments

Secure score

36% SECURE SCORE

Azure	72%
AWS	30%
GCP	37%

Environment

14 Total

Subscriptions 1 | Accounts 7 | Projects 6

359/683 Unhealthy resources

92 Recommendations

See your score over time

Track the progress of your score with this workbook. View what's changed recently, scores for individual subscriptions, and other useful metrics.

Learn more >

Environment

Search by name | Environment == **All** | □ Group by environment

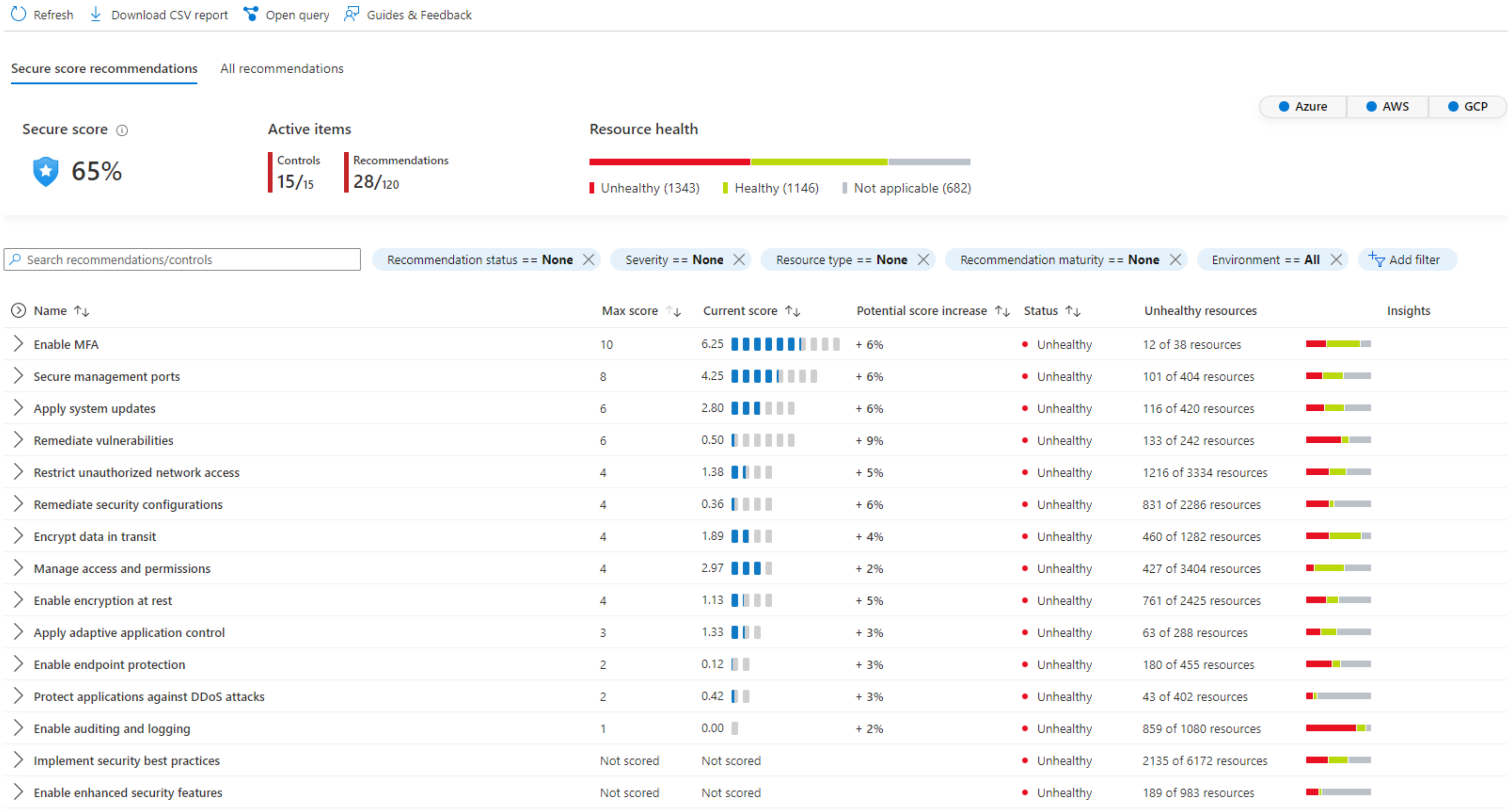
Name	Secure score	Unhealthy resources	Recommendations
ASC DEMO Azure subscription	72%	89 of 252	View recommendations >
682457890087 (GCP-Containers) GCP project	47%	0 of 0	View recommendations >
215639135796 (Contoso-Apps) GCP project	43%	0 of 0	View recommendations >
166423052632 (WW-Shared-Services) GCP project	42%	0 of 0	View recommendations >
922339707509 (GCP-Demo) GCP project	42%	0 of 0	View recommendations >
102514576198 (AWS-Connector) AWS account	33%	218 of 358	View recommendations >

Compare the different Secure Scores

Service Models	Cloud Computing Service Provider	Category	Name of Secure Score Functionality	Administration Portal
SaaS	Microsoft 365	Identity, Devices and Apps	Microsoft Secure Score	Microsoft 365 Security center
PaaS	Azure	Feature Coverage for Azure PaaS Services	Secure Score	Microsoft Defender for Cloud Dashboard
	AWS	Provided by AWS Security Hub		
	GCP	Provided by GCP Security Command Center		
IaaS	Azure	Supported Platforms	Secure Score	Microsoft Defender for Cloud Dashboard
	GCP, AWS	Supported Platforms		
	On-premises	Supported Platforms		

© Copyright Microsoft Corporation. All rights reserved.

View Recommendations



Refresh | Download CSV report | Open query | Guides & Feedback

Secure score recommendations | All recommendations

● Azure ● AWS ● GCP

Secure score ⓘ

65%

Active items

Controls 15/15

Recommendations 28/120

Resource health

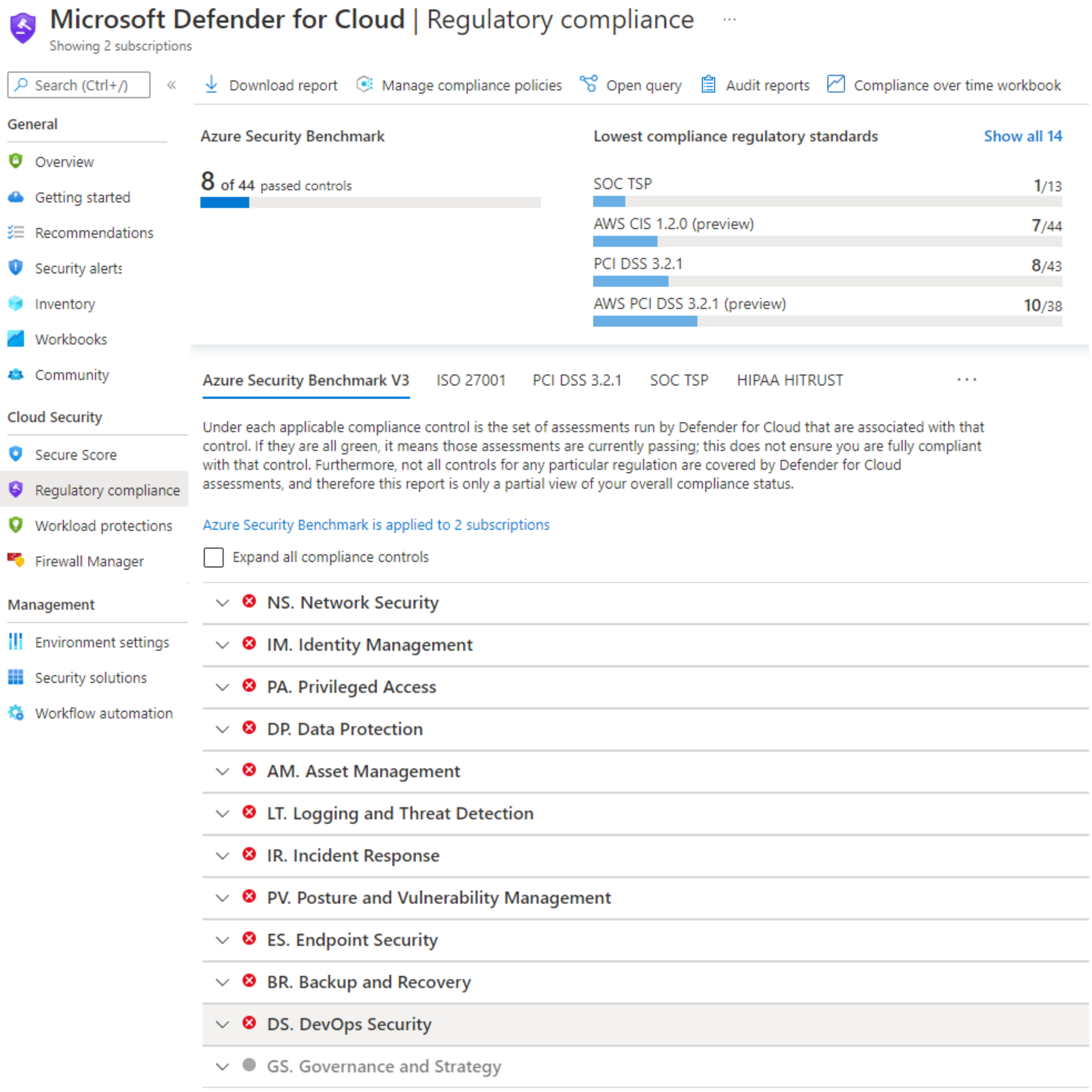
Unhealthy (1343) Healthy (1146) Not applicable (682)

Search recommendations/controls

Recommendation status == **None** ✕ | Severity == **None** ✕ | Resource type == **None** ✕ | Recommendation maturity == **None** ✕ | Environment == **All** ✕ | Add filter

Name ↑↓	Max score ↑↓	Current score ↑↓	Potential score increase ↑↓	Status ↑↓	Unhealthy resources	Insights
Enable MFA	10	6.25	+ 6%	● Unhealthy	12 of 38 resources	
Secure management ports	8	4.25	+ 6%	● Unhealthy	101 of 404 resources	
Apply system updates	6	2.80	+ 6%	● Unhealthy	116 of 420 resources	
Remediate vulnerabilities	6	0.50	+ 9%	● Unhealthy	133 of 242 resources	
Restrict unauthorized network access	4	1.38	+ 5%	● Unhealthy	1216 of 3334 resources	
Remediate security configurations	4	0.36	+ 6%	● Unhealthy	831 of 2286 resources	
Encrypt data in transit	4	1.89	+ 4%	● Unhealthy	460 of 1282 resources	
Manage access and permissions	4	2.97	+ 2%	● Unhealthy	427 of 3404 resources	
Enable encryption at rest	4	1.13	+ 5%	● Unhealthy	761 of 2425 resources	
Apply adaptive application control	3	1.33	+ 3%	● Unhealthy	63 of 288 resources	
Enable endpoint protection	2	0.12	+ 3%	● Unhealthy	180 of 455 resources	
Protect applications against DDoS attacks	2	0.42	+ 3%	● Unhealthy	43 of 402 resources	
Enable auditing and logging	1	0.00	+ 2%	● Unhealthy	859 of 1080 resources	
Implement security best practices	Not scored	Not scored		● Unhealthy	2135 of 6172 resources	
Enable enhanced security features	Not scored	Not scored		● Unhealthy	189 of 983 resources	

Measure Compliance



Microsoft Defender for Cloud | Regulatory compliance

Showing 2 subscriptions

Azure Security Benchmark

8 of 44 passed controls

Lowest compliance regulatory standards

SOC TSP	1/13
AWS CIS 1.2.0 (preview)	7/44
PCI DSS 3.2.1	8/43
AWS PCI DSS 3.2.1 (preview)	10/38

Under each applicable compliance control is the set of assessments run by Defender for Cloud 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 Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.

Azure Security Benchmark is applied to 2 subscriptions

☐ Expand all compliance controls

- NS. Network Security
- IM. Identity Management
- PA. Privileged Access
- DP. Data Protection
- AM. Asset Management
- LT. Logging and Threat Detection
- IR. Incident Response
- PV. Posture and Vulnerability Management
- ES. Endpoint Security
- BR. Backup and Recovery
- DS. DevOps Security
- GS. Governance and Strategy

© Copyright Microsoft Corporation. All rights reserved.

Use Workbooks

- Secure Score Over Time
- System Updates
- Vulnerability Assessment Findings
- Compliance Over Time
- Active Alerts

© Copyright Microsoft Corporation. All rights reserved.

Workload protections in Microsoft Defender for Cloud

Introduction

After completing this module, 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 Plan 1 - deploys Microsoft Defender for Endpoint to your servers and provides these capabilities:

- As licenças do Microsoft Defender for Endpoint são cobradas por hora em vez de por estação, reduzindo os custos de proteção de máquinas virtuais somente quando elas estão em uso.
- O Microsoft Defender for Endpoint é implantado automaticamente em todas as cargas de trabalho da nuvem para que você saiba que elas estão protegidas quando são giradas.
- Alertas e dados de vulnerabilidade do Microsoft Defender for Endpoint são mostrados no Microsoft Defender for Cloud

Microsoft Defender for Servers Plan 2 (formerly Defender for Servers) - includes the benefits of Plan 1 and support for all of the other Microsoft Defender for Servers features.

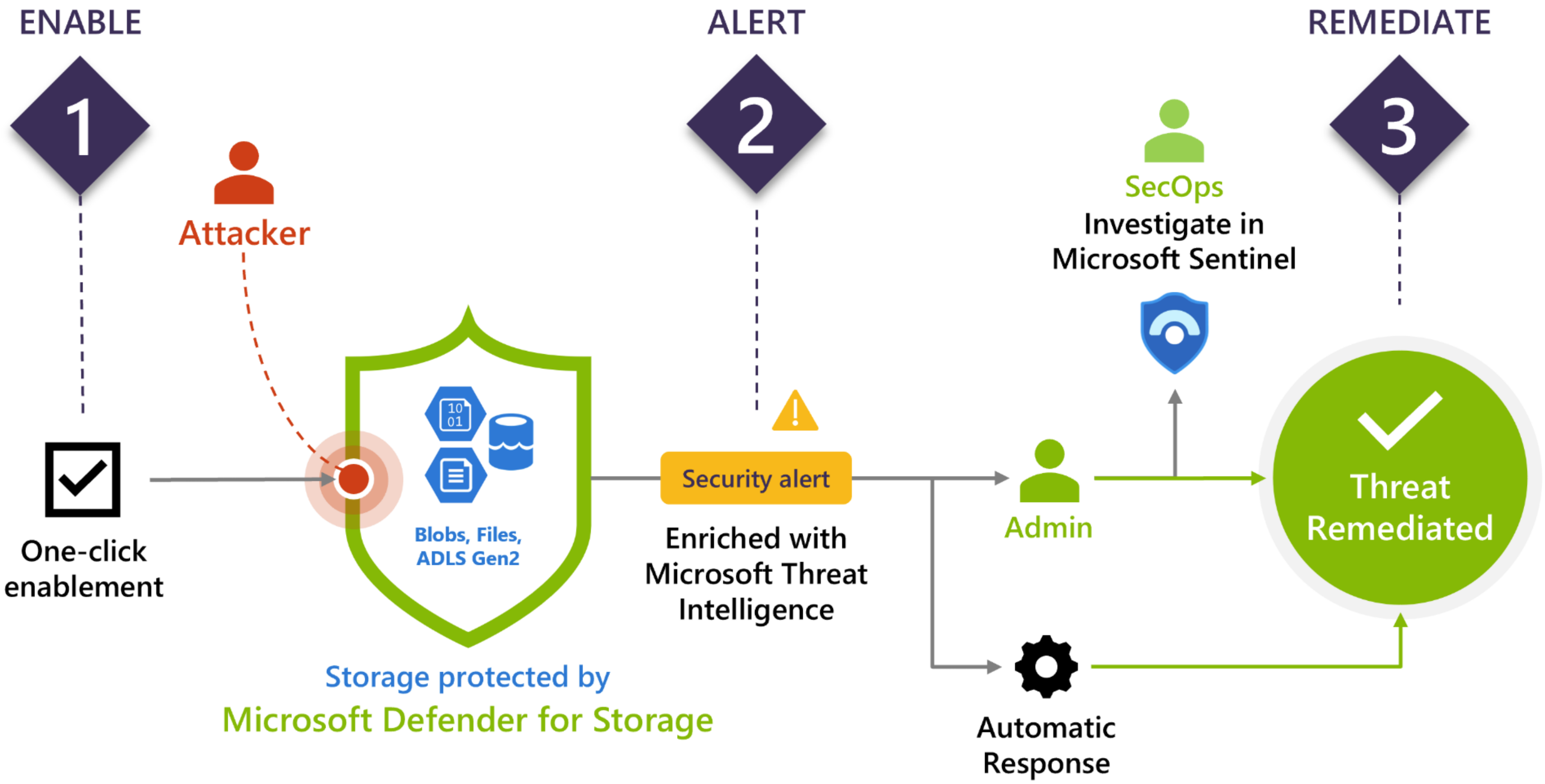
© Copyright Microsoft Corporation. All rights reserved.

Microsoft Defender for App Service

- O Microsoft Defender para o Serviço de Aplicativo usa a escala da nuvem para identificar ataques direcionados a aplicativos em execução no Serviço de Aplicativo.
- Os invasores investigam aplicativos da Web para encontrar e explorar pontos fracos. Antes de serem roteadas para ambientes específicos, as solicitações para aplicativos em execução no Azure passam por vários gateways, onde são inspecionadas e registradas.
- Esses dados são usados para identificar explorações e invasores e aprender novos padrões que serão usados posteriormente.
-

© Copyright Microsoft Corporation. All rights reserved.

Microsoft Defender for Storage



© Copyright Microsoft Corporation. All rights reserved.

Microsoft Defender for Databases - 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

© Copyright Microsoft Corporation. All rights reserved.

Microsoft Defender for Databases

Threat protection for Azure Cosmos DB

Threat protection for open-source relational databases are available for:

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

© Copyright Microsoft Corporation. All rights reserved.

Microsoft Defender for Key Vault

O Microsoft Defender detecta tentativas incomuns e potencialmente prejudiciais de acessar ou explorar contas do Cofre da Chave. Essa camada de proteção permite:

- Enfrente ameaças sem ser um especialista em segurança.
- Enfrente ameaças sem a necessidade de gerenciar sistemas de monitoramento de segurança de terceiros.

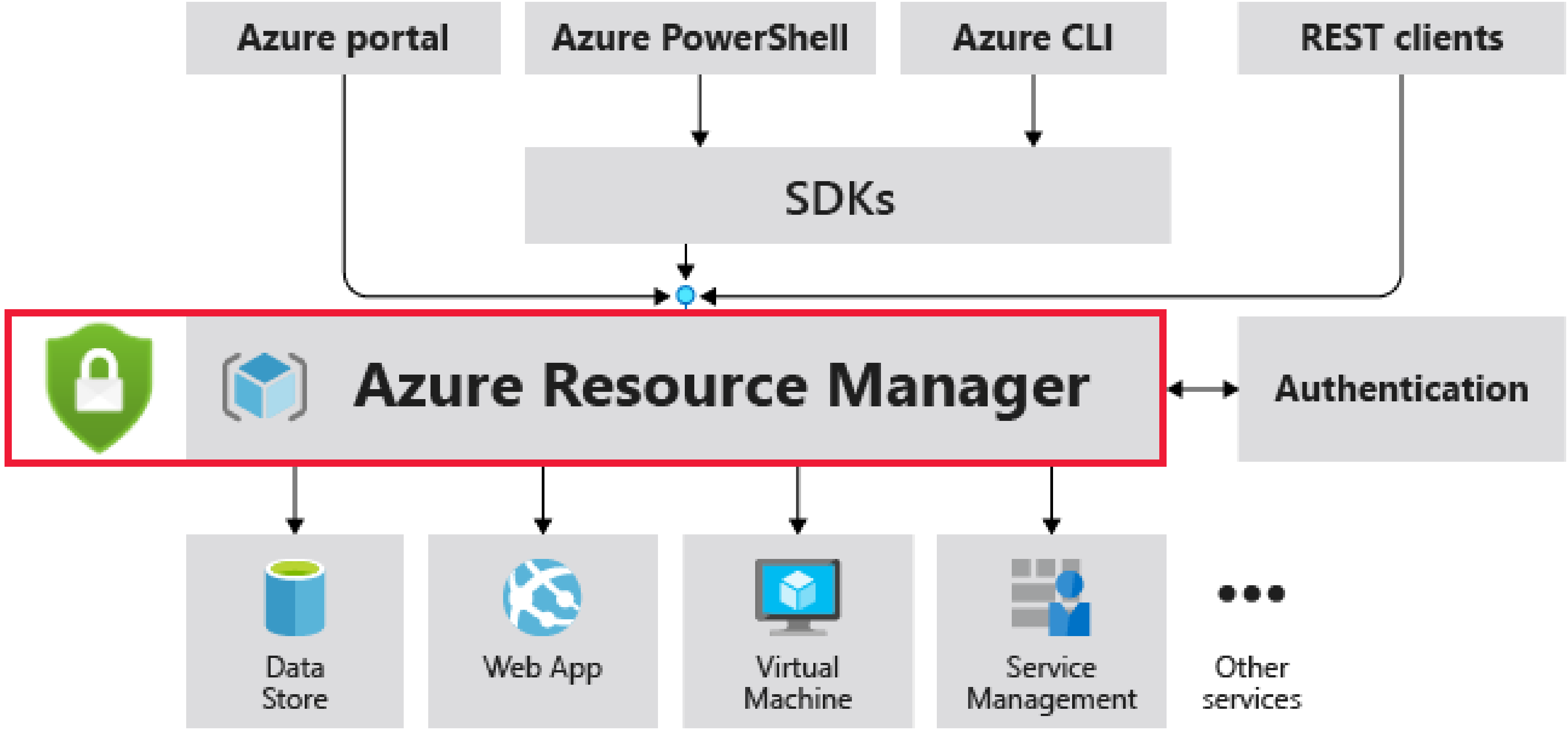
Quando ocorrem atividades anômalas, o Microsoft Defender mostra alertas e, opcionalmente, os envia por e-mail para membros relevantes da sua organização. Esses alertas incluem os detalhes da atividade suspeita e recomendações sobre como investigar e corrigir ameaças.

© Copyright Microsoft Corporation. All rights reserved.

Microsoft Defender for Resource Manager

Microsoft Defender for Resource Manager protects against issues including:

- **Suspicious resource management operations**, such as operations from malicious IP addresses, disabling antimalware, and suspicious scripts running in VM extensions
- **Use of exploitation toolkits** like Microburst or PowerZure
- **Lateral movement** from the Azure management layer to the Azure resources data plane



© Copyright Microsoft Corporation. All rights reserved.

Microsoft Defender for DNS

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

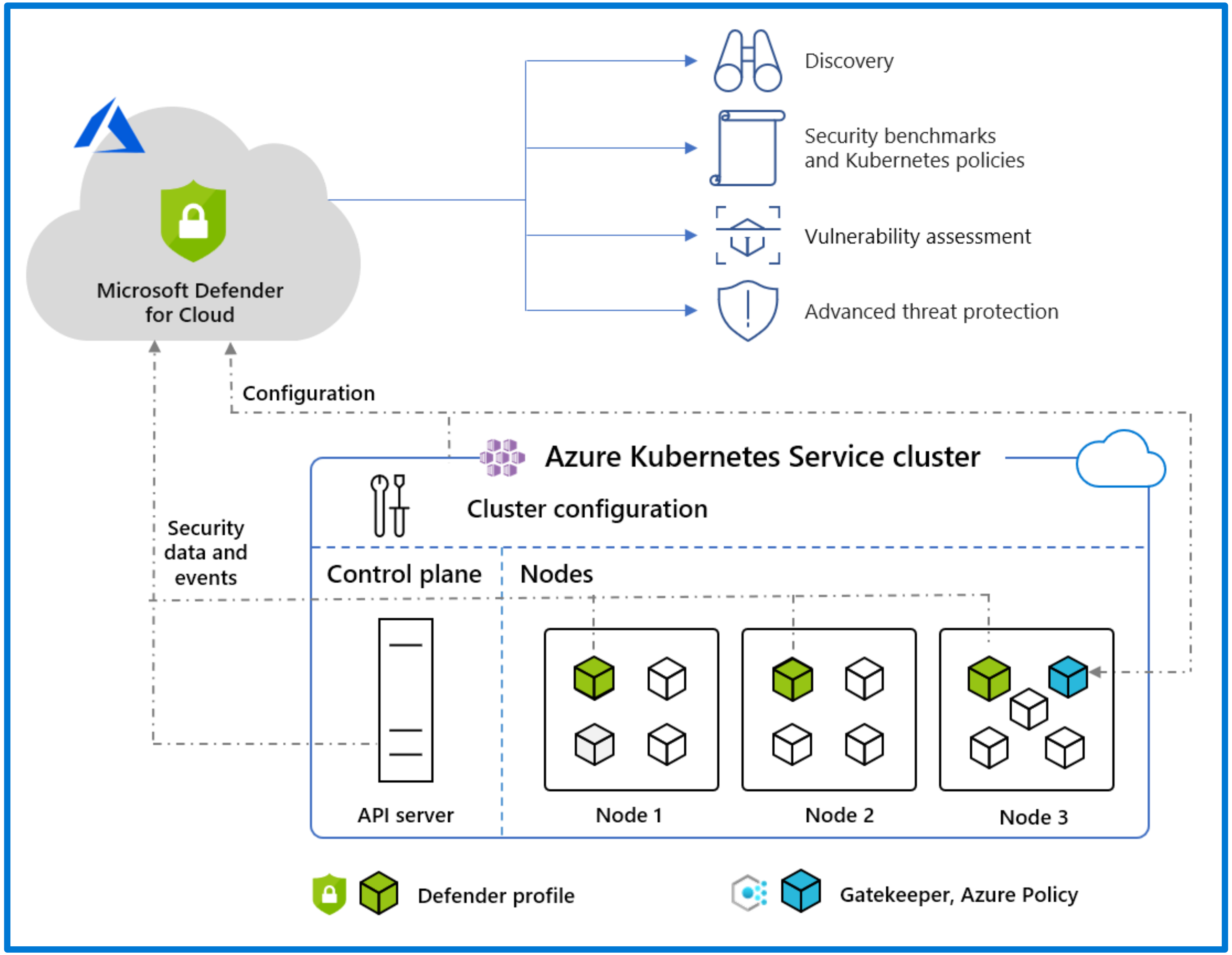
- Continuously monitoring all DNS queries from your Azure resources
- Running advanced security analytics to alert you about suspicious activity

© Copyright Microsoft Corporation. All rights reserved.

Microsoft Defender for Containers

Defender for Containers protects your clusters whether they're running in:

- Azure Kubernetes Service (AKS)
- Amazon Elastic Kubernetes Service (EKS) in a connected Amazon Web Services (AWS) account
- An unmanaged Kubernetes distribution (using Azure Arc-enabled Kubernetes)



© Copyright Microsoft Corporation. All rights reserved.

Remediate security alerts using Microsoft Defender for Cloud

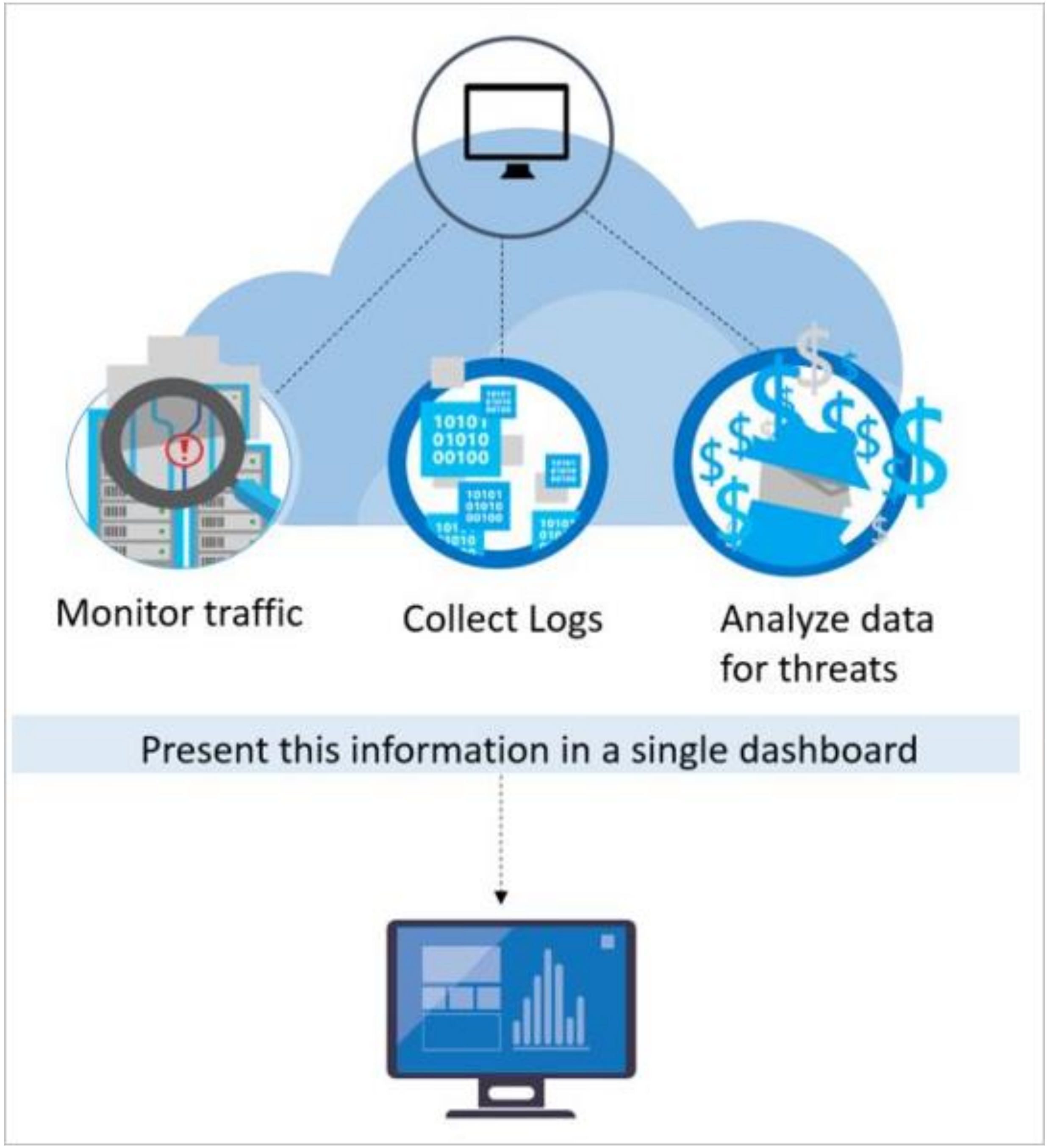
Introduction

After completing this module, 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

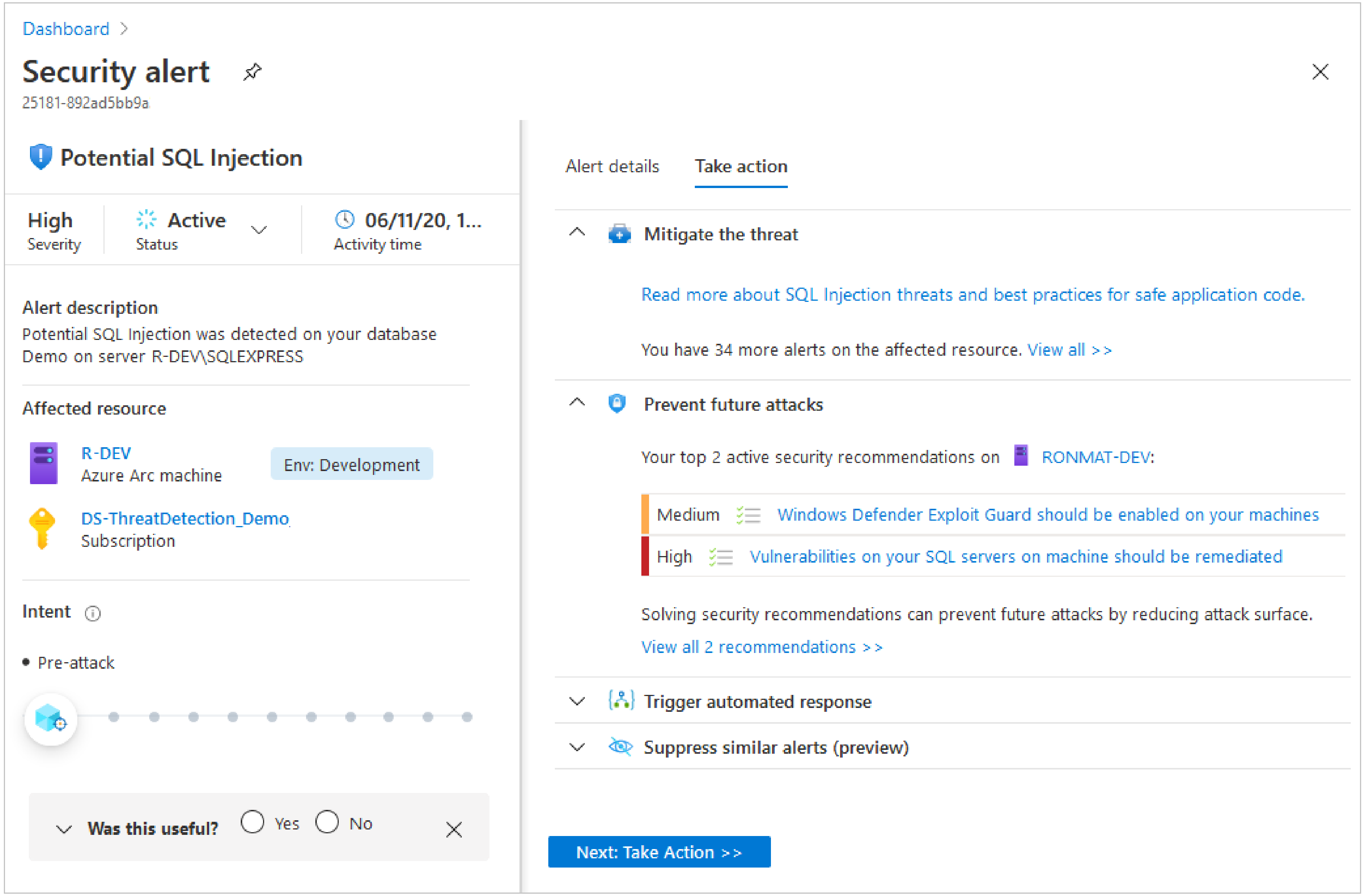
- Security alerts and incidents
- Detecting Threats
- Alert classification
- Continuous monitoring and assessments
- Alert types



© Copyright Microsoft Corporation. All rights reserved.

Remediate alerts

O Microsoft Defender for Cloud fornece tarefas acionáveis para Reduzir a ameaça, evitar ataques futuros, acionar respostas automatizadas e suprimir alertas semelhantes.



Dashboard >

Security alert

25181-892ad5bb9a

Potential SQL Injection

High
Severity

Active
Status

06/11/20, 1...
Activity time

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

Was this useful? ○ Yes ○ No

Alert details | Take action

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 remediated

Solving security recommendations can prevent future attacks by reducing attack surface.

View all 2 recommendations >>

Trigger automated response

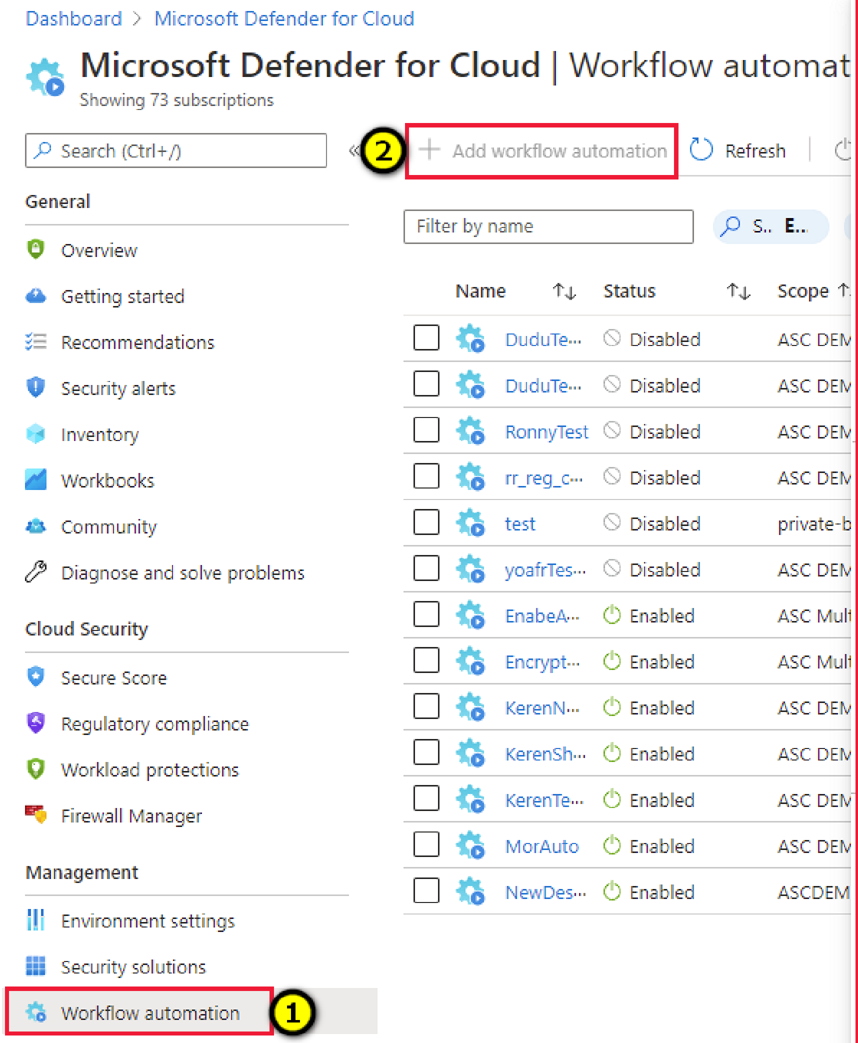
Suppress similar alerts (preview)

Next: Take Action >>

© Copyright Microsoft Corporation. All rights reserved.

Remediate alerts (continued)

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

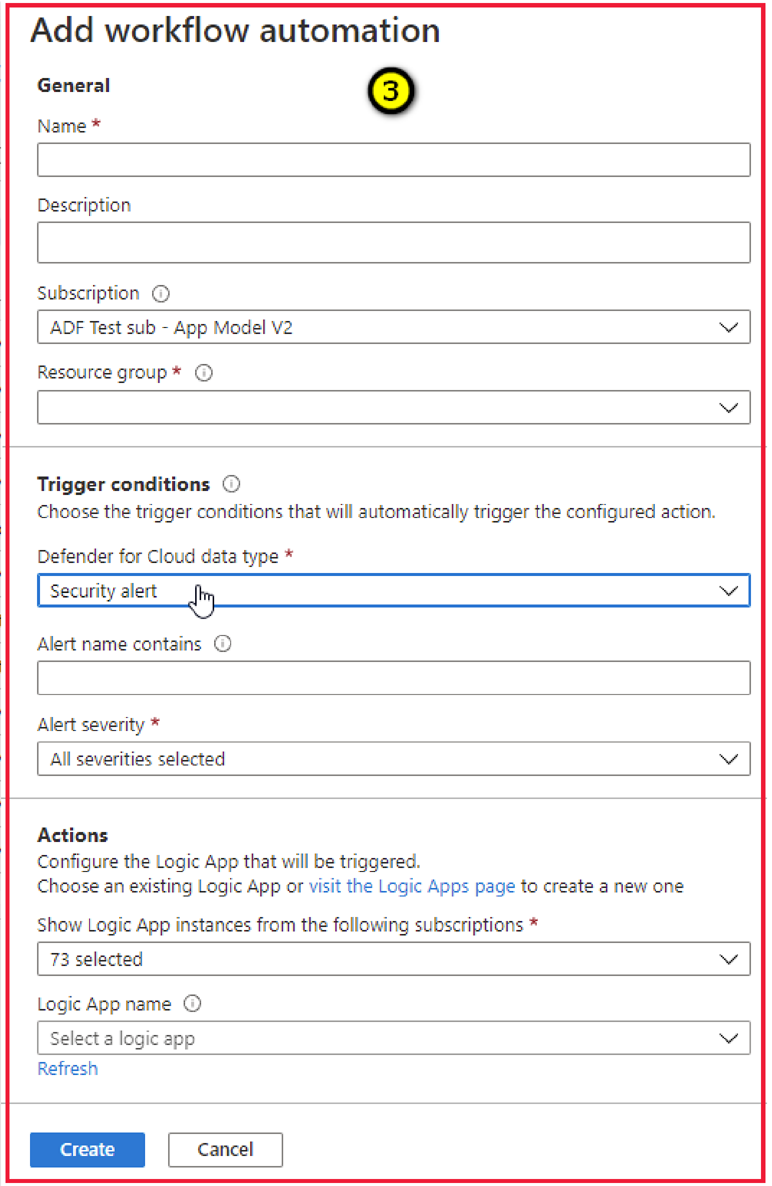


Dashboard > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Workflow automat

Showing 73 subscriptions

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



Add workflow automation

General

Name *

Description

Subscription: ADF Test sub - App Model V2

Resource group *

Trigger conditions

Choose the trigger conditions that will automatically trigger the configured action.

Defender for Cloud data type *: Security alert

Alert name contains

Alert severity *: All severities selected

Actions

Configure the Logic App that will be triggered.

Choose an existing Logic App or visit the Logic Apps page to create a new one

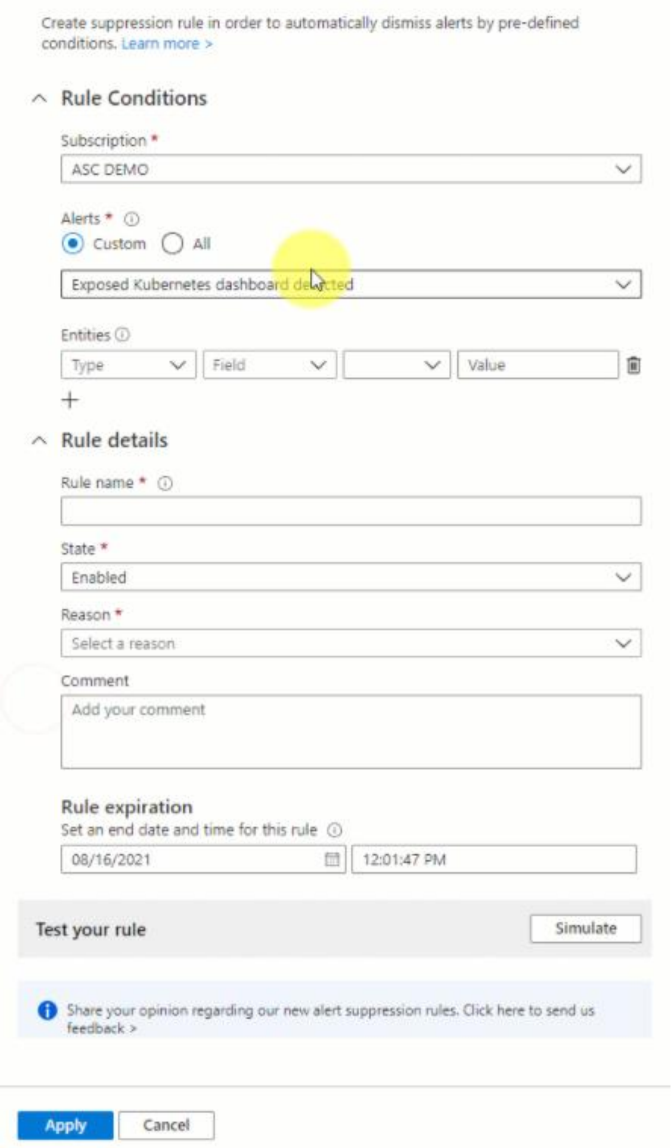
Show Logic App instances from the following subscriptions *: 73 selected

Logic App name: Select a logic app

© Copyright Microsoft Corporation. All rights reserved.

Suppress alerts from Microsoft Defender for Cloud

Uma regra de supressão pode ser útil para suprimir alertas que você identificou como falsos positivos ou alertas que estão sendo acionados com muita frequência para ser útil.



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

Share your opinion regarding our new alert suppression rules. Click here to send us feedback >

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

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

© Copyright Microsoft Corporation. All rights reserved.

Knowledge check

Check your knowledge with the module quiz in your course viewer

Microsoft Security

CANAL DA CLOUD

Obrigado!

Celio Ramos

Senior Presales Solutions Architect |
Membro ANPPD® | Membro ANADD...

© Copyright Microsoft Corporation. All rights reserved.