Microsoft Security

Microsoft Defender for Cloud

Not your parents' ASC – Updates from Microsoft Ignite 2021

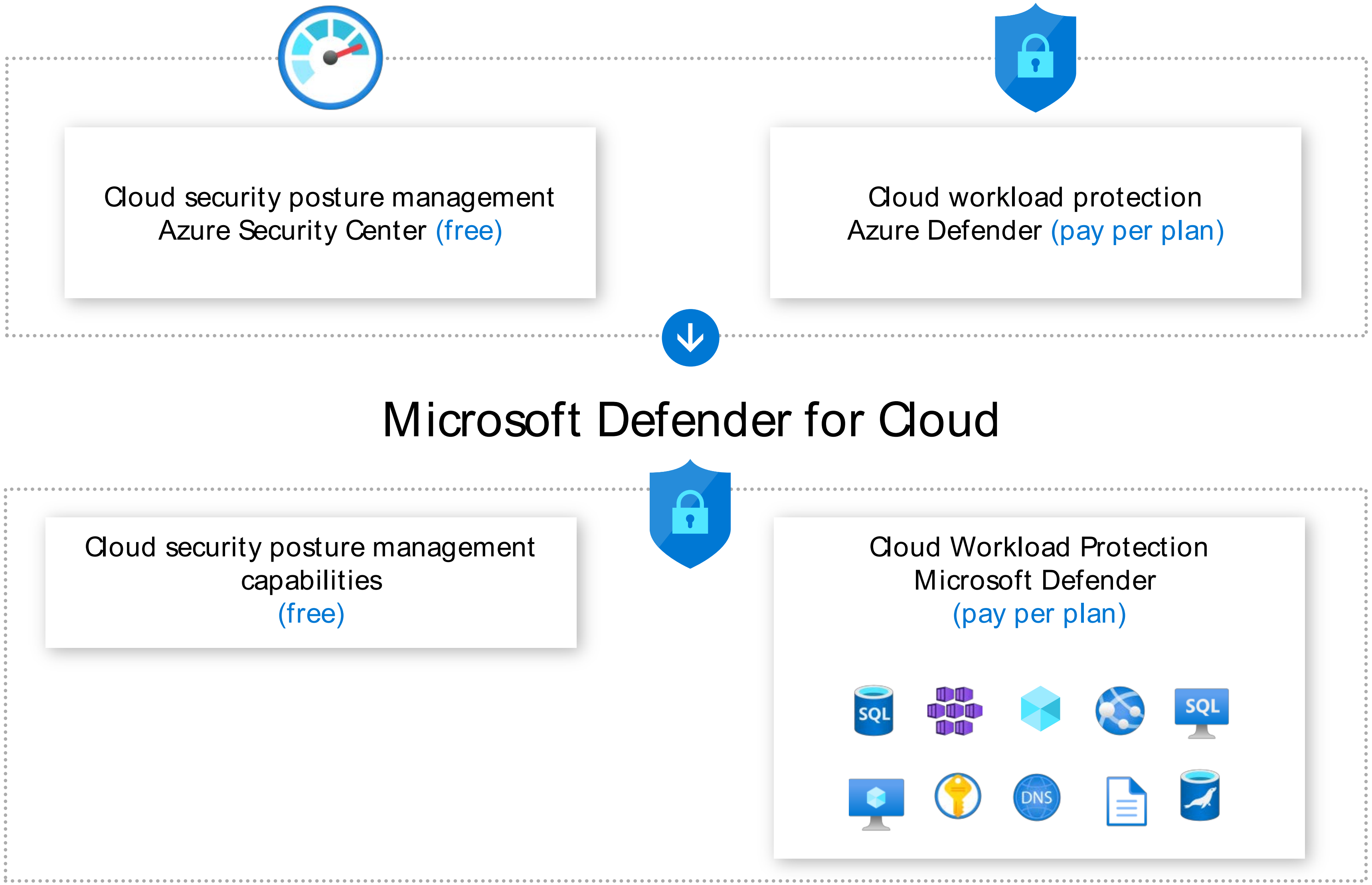
Tom Janetscheck, Senior Program Manager

Microsoft Security

Breaking news

Azure Security Center and Azure Defender are now Microsoft Defender for Cloud!

A new name for multi-cloud security: Microsoft Defender for Cloud



Cloud security posture management
Azure Security Center (free)

Cloud workload protection
Azure Defender (pay per plan)

Microsoft Defender for Cloud

Cloud security posture management capabilities
(free)

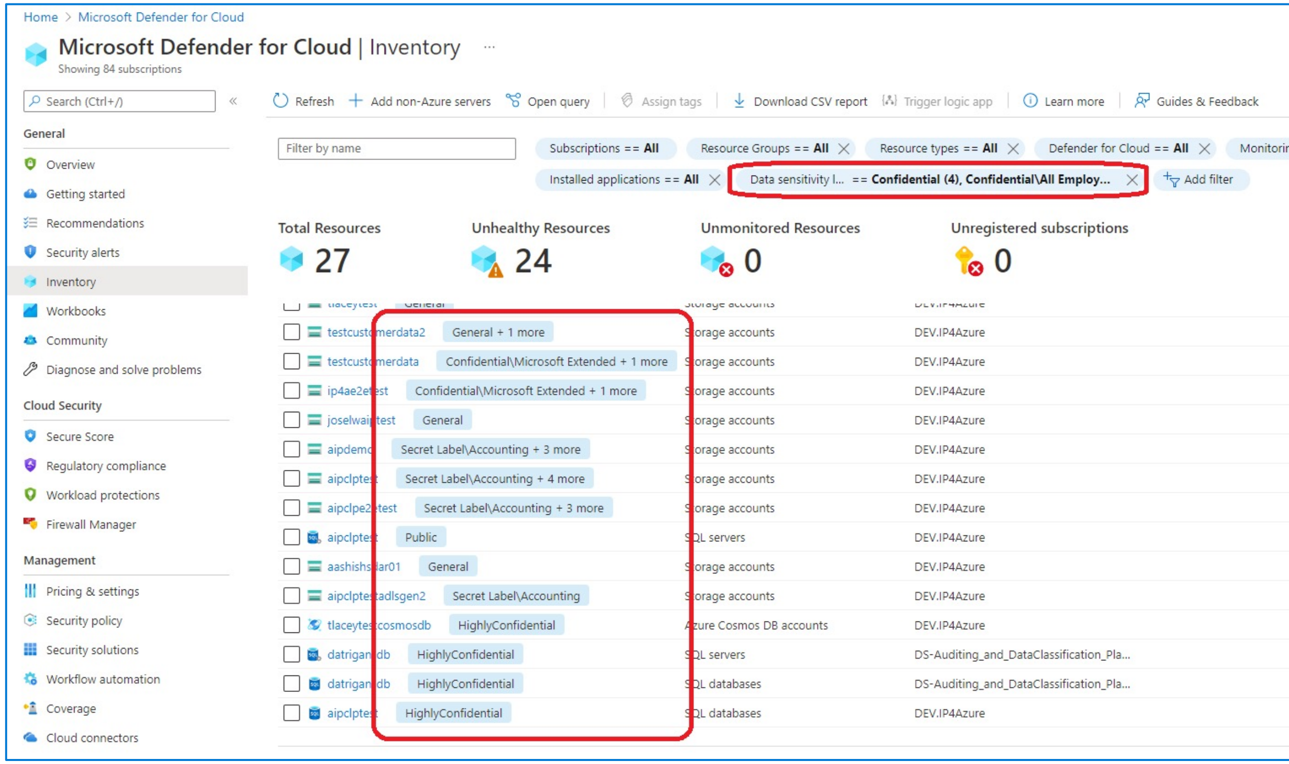
Cloud Workload Protection
Microsoft Defender
(pay per plan)

Ignite 2021 news

Identify sensitive data in cloud resources

Integrated with Azure Purview

- Extend visibility from cloud infrastructure resources into the data layer
- Leverage an entirely new way to prioritize security policies and the investigation of alerts
- Filter recommendations and resources by data sensitivity
- Easily view the number of assets that contain sensitive information across your environment



Microsoft Defender for Cloud | Inventory

Showing 84 subscriptions

Subscriptions == **All**

Resource Groups == **All**

Resource types == **All**

Defender for Cloud == **All**

Installed applications == **All**

Data sensitivity l... == **Confidential (4), Confidential\All Employ...**

Total Resources 27

Unhealthy Resources 24

Unmonitored Resources 0

Unregistered subscriptions 0

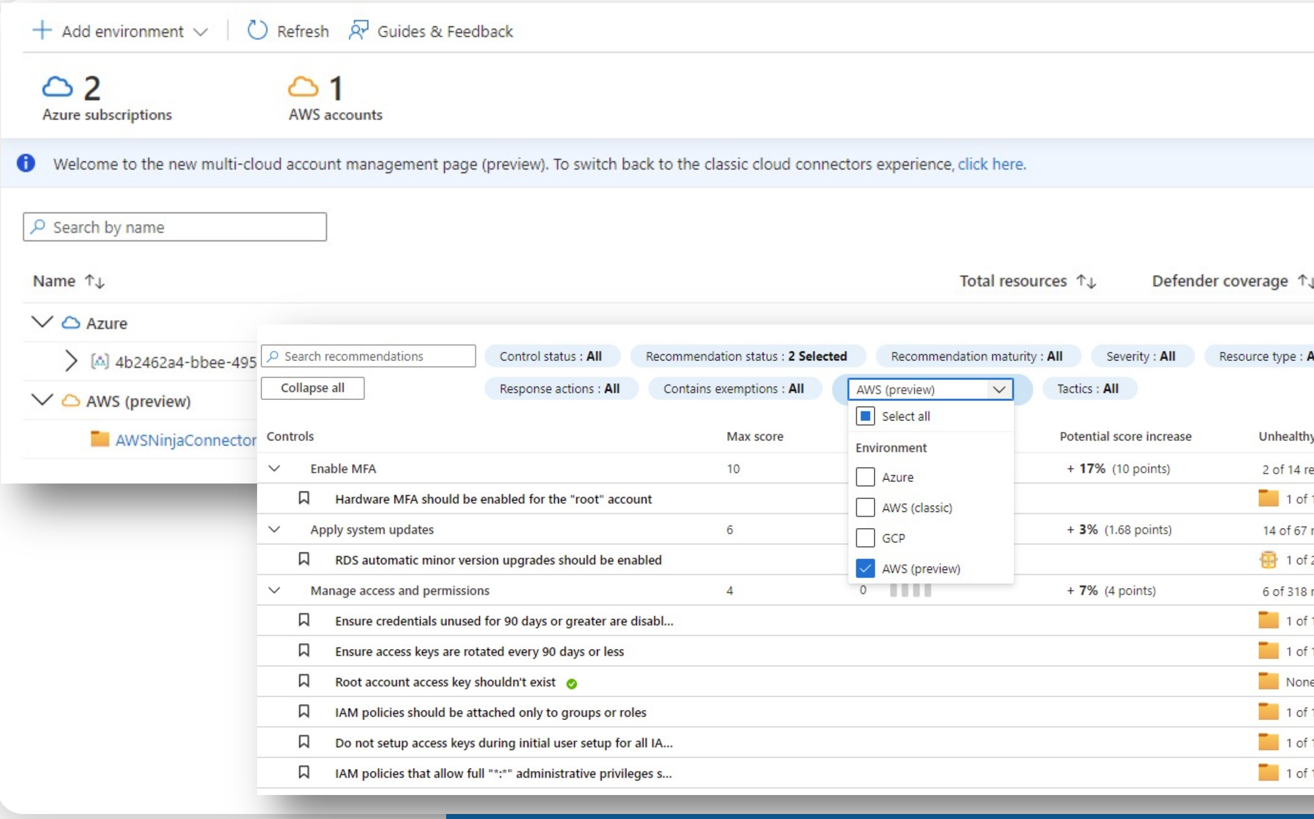
□	tlaceytest	General	Storage accounts	DEV.IP4Azure
□	testcust merdata2	General + 1 more	S orage accounts	DEV.IP4Azure
□	testcust merdata	Confidential\Microsoft Extended + 1 more	S orage accounts	DEV.IP4Azure
□	ip4ae2e est	Confidential\Microsoft Extended + 1 more	S orage accounts	DEV.IP4Azure
□	joselwai test	General	S orage accounts	DEV.IP4Azure
□	aipdemo	Secret Label\Accounting + 3 more	S orage accounts	DEV.IP4Azure
□	aipclpte	Secret Label\Accounting + 4 more	S orage accounts	DEV.IP4Azure
□	aipclpe2 test	Secret Label\Accounting + 3 more	S orage accounts	DEV.IP4Azure
□	aipclpte	Public	S L servers	DEV.IP4Azure
□	aashishs ar01	General	S orage accounts	DEV.IP4Azure
□	aipclpte adlsgen2	Secret Label\Accounting	S orage accounts	DEV.IP4Azure
□	tlaceyte cosmosdb	HighlyConfidential	A ure Cosmos DB accounts	DEV.IP4Azure
□	datrigan db	HighlyConfidential	S L servers	DS-Auditing_and_DataClassification_Pla...
□	datrigan db	HighlyConfidential	S L databases	DS-Auditing_and_DataClassification_Pla...
□	aipclpte	HighlyConfidential	S L databases	DEV.IP4Azure

Ignite 2021 news

New approach to multi-cloud scenarios

New AWS Connector

- Seamless onboarding using AWS API
- 160+ out of the box recommendations, CIS, PCI & AWS Foundational Security Best Practices support, multi-cloud view in Secure Score
- EKS support, easier onboarding for workloads



2 Azure subscriptions

1 AWS accounts

Welcome to the new multi-cloud account management page (preview). To switch back to the classic cloud connectors experience, click here.

Control status : **All**

Recommendation status : **2 Selected**

Recommendation maturity : **All**

Severity : **All**

Resource type : **A**

Response actions : **All**

Contains exemptions : **All**

AWS (preview)

Tactics : **All**

■ Select all

Environment

□ Azure

□ AWS (classic)

□ GCP

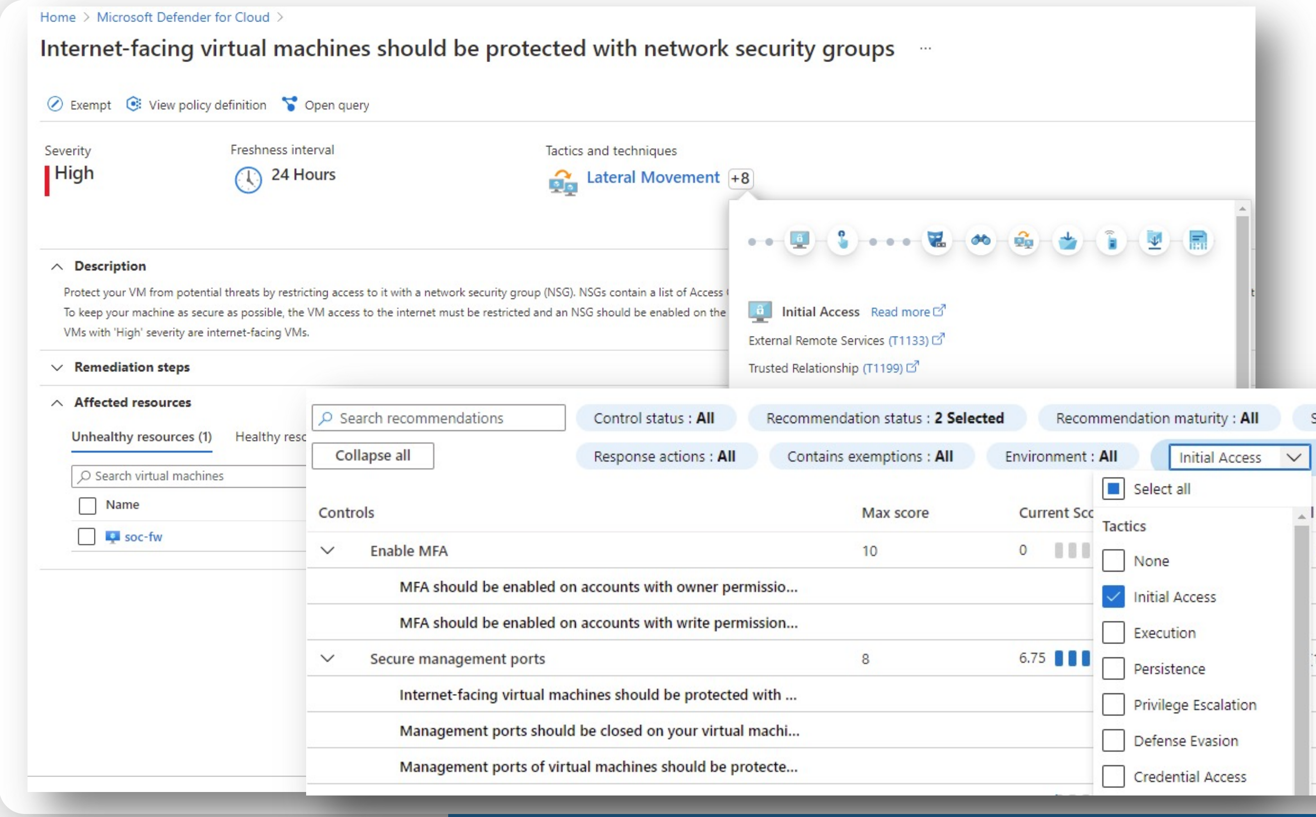
☑ AWS (preview)

Controls	Max score		Potential score increase	Unhealthy
Enable MFA	10		+ **17%** (10 points)	2 of 14 re
Hardware MFA should be enabled for the "root" account				1 of 1
Apply system updates	6		+ **3%** (1.68 points)	14 of 67 r
RDS automatic minor version upgrades should be enabled				1 of 2
Manage access and permissions	4	0	+ **7%** (4 points)	6 of 318 r
Ensure credentials unused for 90 days or greater are disabl...				1 of 1
Ensure access keys are rotated every 90 days or less				1 of 1
Root account access key shouldn't exist ✓				None
IAM policies should be attached only to groups or roles				1 of 1
Do not setup access keys during initial user setup for all IA...				1 of 1
IAM policies that allow full "*:*" administrative privileges s...				1 of 1

Ignite 2021 news

Security recommendations now map to the MITRE ATT&CK® framework

- Globally accessible knowledge base of threat actors’ tactics and techniques
- Recommendations details pages show the mapping for all relevant recommendations
- New Tactics filter in recommendations page
- Azure Resource Graph queries include the MITRE ATT&ACK® tactics and techniques



Home > Microsoft Defender for Cloud >

Internet-facing virtual machines should be protected with network security groups ...

Severity: High

Freshness interval: 24 Hours

Tactics and techniques: Lateral Movement +8

Initial Access Read more

External Remote Services (T1133)

Trusted Relationship (T1199)

Description

Protect your VM from potential threats by restricting access to it with a network security group (NSG). NSGs contain a list of Access
To keep your machine as secure as possible, the VM access to the internet must be restricted and an NSG should be enabled on the
VMs with 'High' severity are internet-facing VMs.

Remediation steps

Affected resources

Unhealthy resources (1) Healthy reso

Search virtual machines

□ Name

□ soc-fw

Search recommendations

Control status : All
Recommendation status : 2 Selected
Recommendation maturity : All
Response actions : All
Contains exemptions : All
Environment : All
Initial Access

Collapse all

Controls	Max score	Current Sco
Enable MFA	10	0
MFA should be enabled on accounts with owner permissio...		
MFA should be enabled on accounts with write permission...		
Secure management ports	8	6.75
Internet-facing virtual machines should be protected with ...		
Management ports should be closed on your virtual machi...		
Management ports of virtual machines should be protecte...		

■ Select all

Tactics

□ None
☑ Initial Access
□ Execution
□ Persistence
□ Privilege Escalation
□ Defense Evasion
□ Credential Access

Security Alerts Workbook

Ignite 2021 news

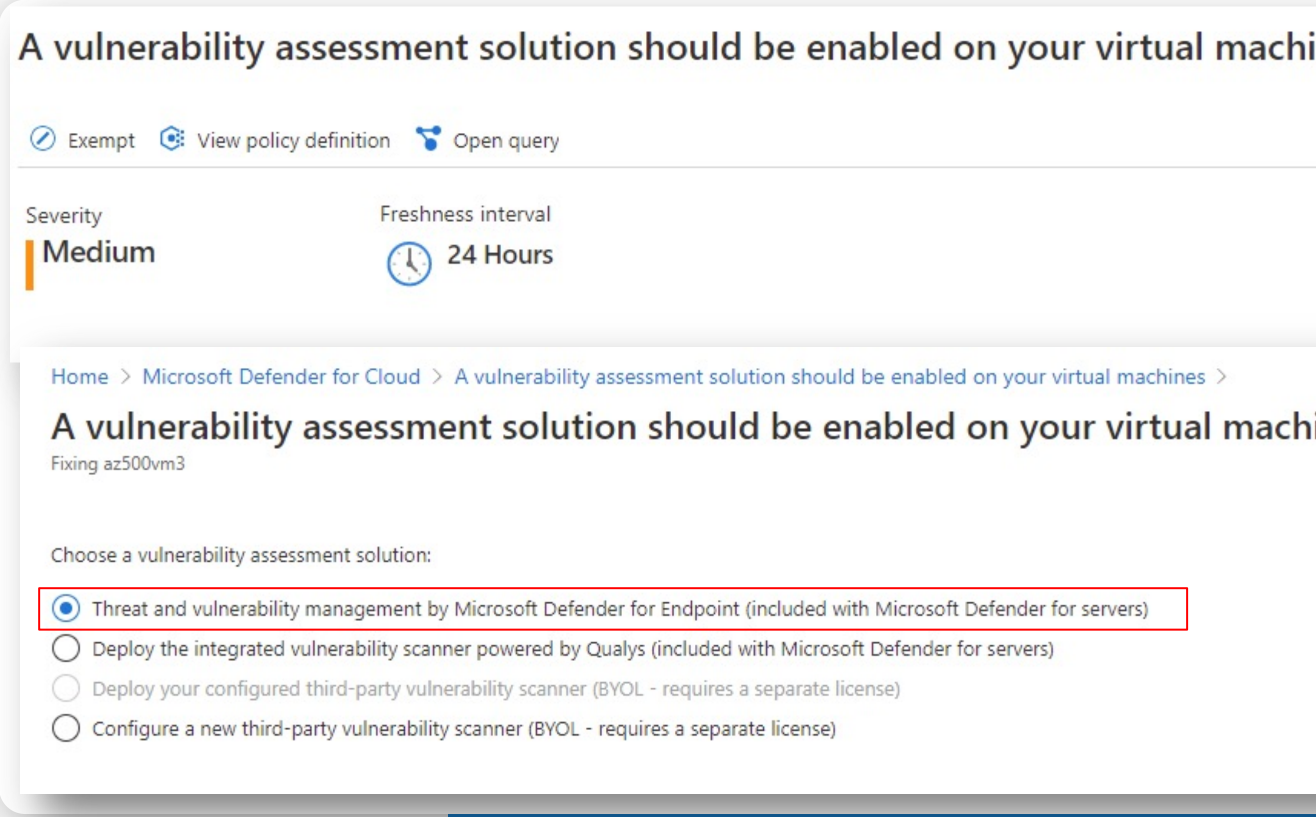
Microsoft Defender for Server

Integration with TVM is now GA

- Use threat and vulnerability management to discover vulnerabilities and misconfigurations in near real time with the integration with Microsoft Defender for Endpoint

- No need for additional agents or periodic scans.

- Threat and vulnerability management prioritizes vulnerabilities based on the threat landscape and detections in your organization.



A vulnerability assessment solution should be enabled on your virtual machi

Severity
Medium

Freshness interval
24 Hours

Home > Microsoft Defender for Cloud > A vulnerability assessment solution should be enabled on your virtual machines >

A vulnerability assessment solution should be enabled on your virtual machi

Fixing az500vm3

Choose a vulnerability assessment solution:

● Threat and vulnerability management by Microsoft Defender for Endpoint (included with Microsoft Defender for servers)

○ Deploy the integrated vulnerability scanner powered by Qualys (included with Microsoft Defender for servers)

○ Deploy your configured third-party vulnerability scanner (BYOL - requires a separate license)

○ Configure a new third-party vulnerability scanner (BYOL - requires a separate license)

Ignite 2021 news

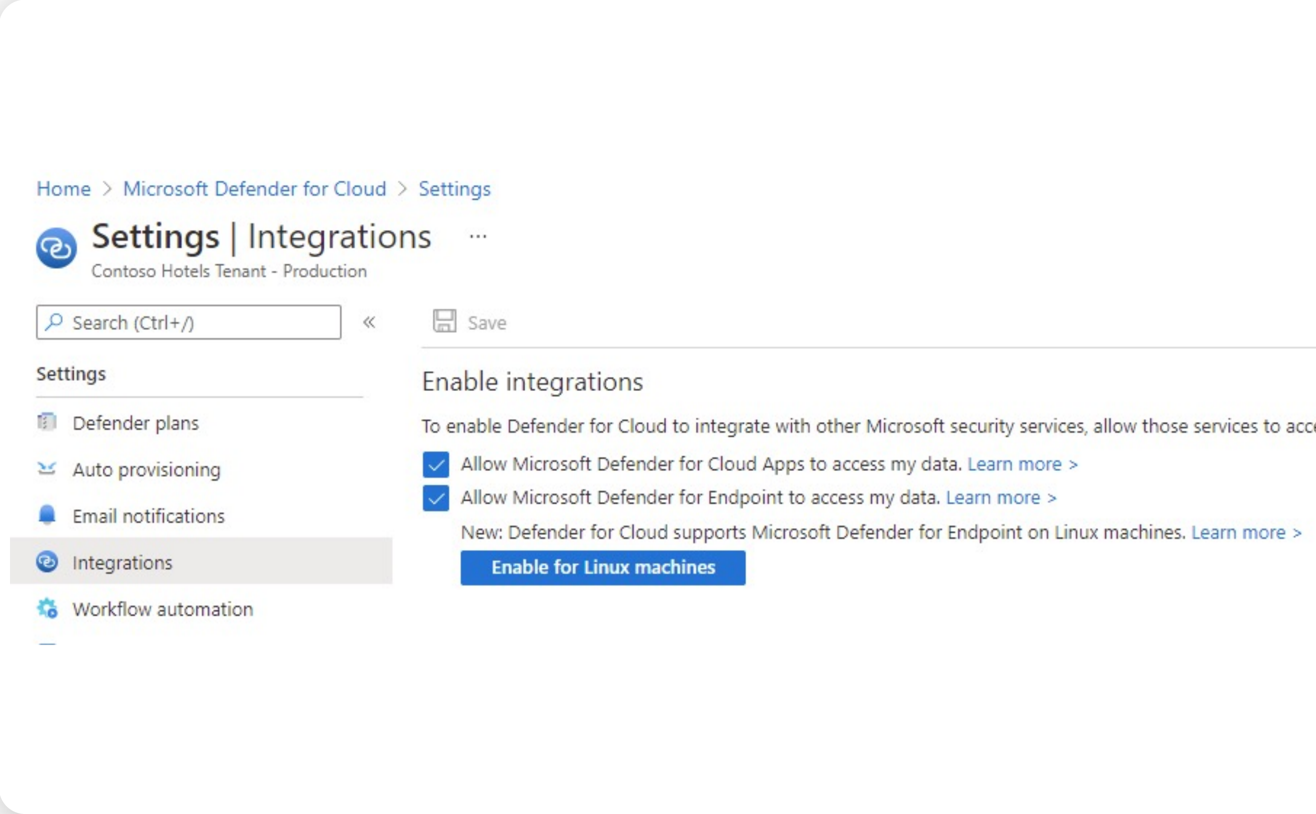
Microsoft Defender for Server

Integration with MDE for Linux is now GA

- In August, we announced preview support for deploying the Defender for Endpoint for Linux sensor to supported Linux machines. This feature is now released for general availability (GA).

- Microsoft Defender for servers includes an integrated license for MDE. Together, they provide comprehensive endpoint detection and response (EDR) capabilities.

- When Defender for Endpoint detects a threat, it triggers an alert. The alert is shown in Defender for Cloud.



Home > Microsoft Defender for Cloud > Settings

Settings | Integrations ...

Contoso Hotels Tenant - Production

Search (Ctrl+/) «

Save

Settings

- Defender plans
- Auto provisioning
- Email notifications
- Integrations
- Workflow automation

Enable integrations

To enable Defender for Cloud to integrate with other Microsoft security services, allow those services to acc

☑ Allow Microsoft Defender for Cloud Apps to access my data. Learn more >

☑ Allow Microsoft Defender for Endpoint to access my data. Learn more >

New: Defender for Cloud supports Microsoft Defender for Endpoint on Linux machines. Learn more >

Enable for Linux machines

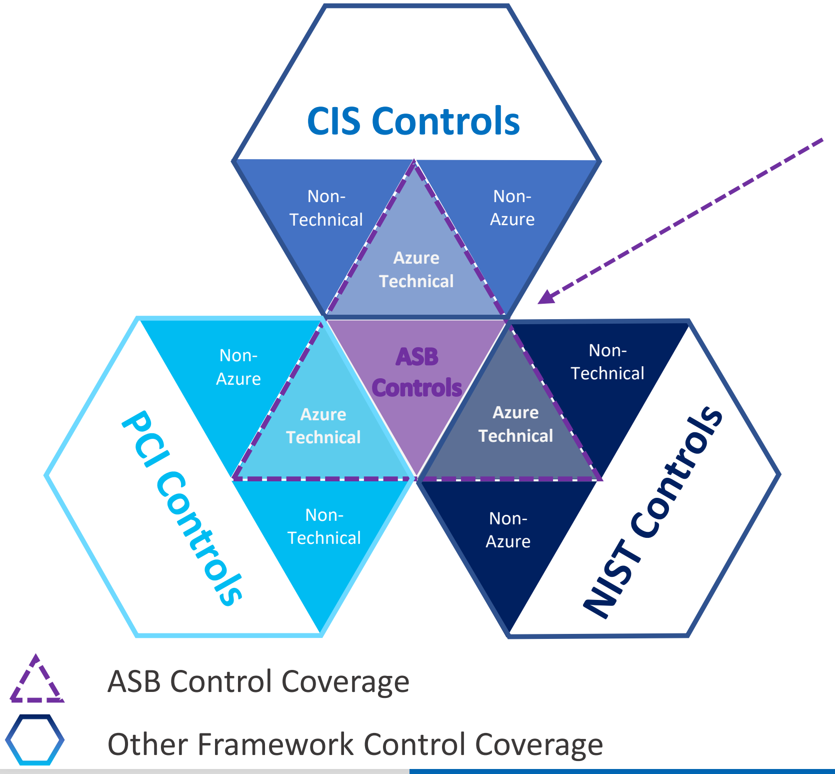
Server Monitoring Dashboard Workbook

Ignite 2021 news

Azure Security Benchmark v3

Azure's own security control framework based on industry standards

- Additional control mappings for PCI-DSS v3.2.1
- Collaborated with Center for Internet Security (CIS) to map ASB v3 controls with CIS Controls v8
- New controls for DevOps Security and Key and Certificate management
- Restructured control guidance for more granular and actionable insights
- ASB v3 is the new default in the Regulatory Compliance Dashboard in Microsoft Defender for Cloud



ASB provides a canonical set of **Azure-centric technical security controls** based on widely used security/compliance control frameworks such as CIS, NIST and PCI.

Demo

Strengthen you cloud security posture today

Enable Defender for Cloud to assess your secure score

Fix your top 5 secure score recommendations today

Start a free trial to protect your multicloud workloads

Onboard on-premises workloads

To learn more, visit: aka.ms/DefenderForCloud ›

Q&A

Thank you