



28 marzo 2025



Roberto Tafuri
Microsoft Solution Team Leader



Luigi Pandolfino
Azure Meetup Veneto



Andrea Marchi
Azure Meetup Veneto

Protezione avanzata dei server con Microsoft Defender for Cloud



veneto.globalazure.it

Il gruppo nasce con l'obiettivo di creare una community per la condivisione di informazioni ed esperienze su **Microsoft Azure** e **365**.

Si rivolge a professionisti del settore IT ma anche ad appassionati di tecnologia, studenti e imprenditori interessati ad approfondire le **soluzioni cloud** e **ibride messe** a disposizione da **Microsoft**.



veneto.globalazure.it



Sessioni tecniche in
presenza ed eventi dedicati
al mondo **Microsoft**



Webinar con esperti di
tecnologie **Microsoft**



| Cosa facciamo |



VICENZA

9 Maggio 2025

TORINO

10 Maggio 2025

PORDENONE

10 Maggio 2025

CATANIA

10 Maggio 2025

MILANO

12 Maggio 2025



Lista di attesa



@azuremeetupveneto



VICENZA

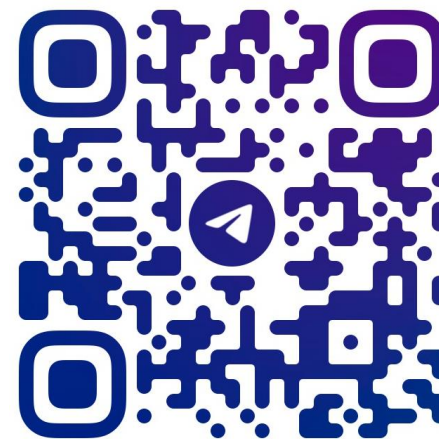
9 Maggio 2025 | 8:30–18:00

Elevator Innovation Hub
Viale A. Fusinato 8

In collaborazione con:



Riserva un posto



@azuremeetupveneto



Microsoft Defender for Cloud Defender for Servers

Protect your servers from threats

Roberto Tafuri – Microsoft Solution Team Leader - WeAreProject

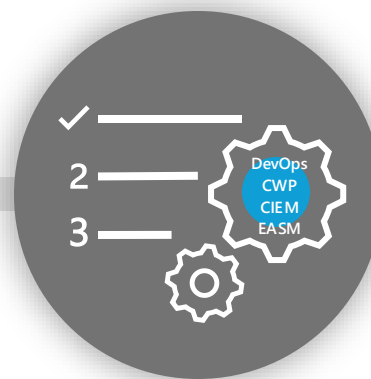


Microsoft Defender for Cloud

Unify your DevOps
Security Management



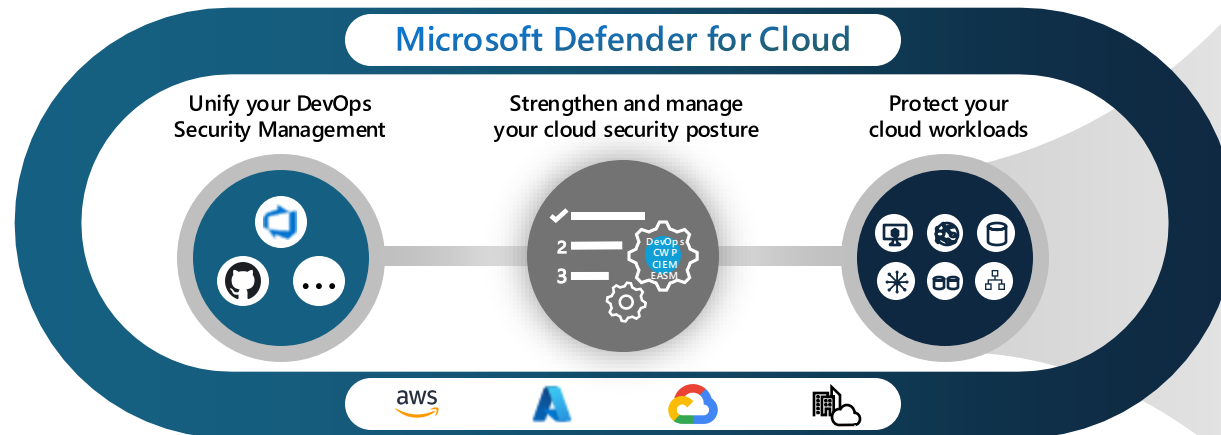
Strengthen and manage your
cloud security posture



Protect your cloud
workloads



Cloud Workload Protection



Compute:

Any server Azure VMSS Azure K8s App Services Unmanaged K8s

Service layer:

Azure DNS Key Vault Network Layer V1 Resource Management

Databases and storage:

Blob storage File storage Maria DB Cosmos DB Azure SQL MySQL Postgres SQL Unmanaged SQL

AWS workloads:

Amazon EKS Amazon EC2 Unmanaged SQL Unmanaged Kubernetes

GCP workloads:

GKE clusters Google Compute Unmanaged SQL Unmanaged Kubernetes

On-premises workloads:

Kubernetes SQL Servers Servers

Server security in the cloud is different

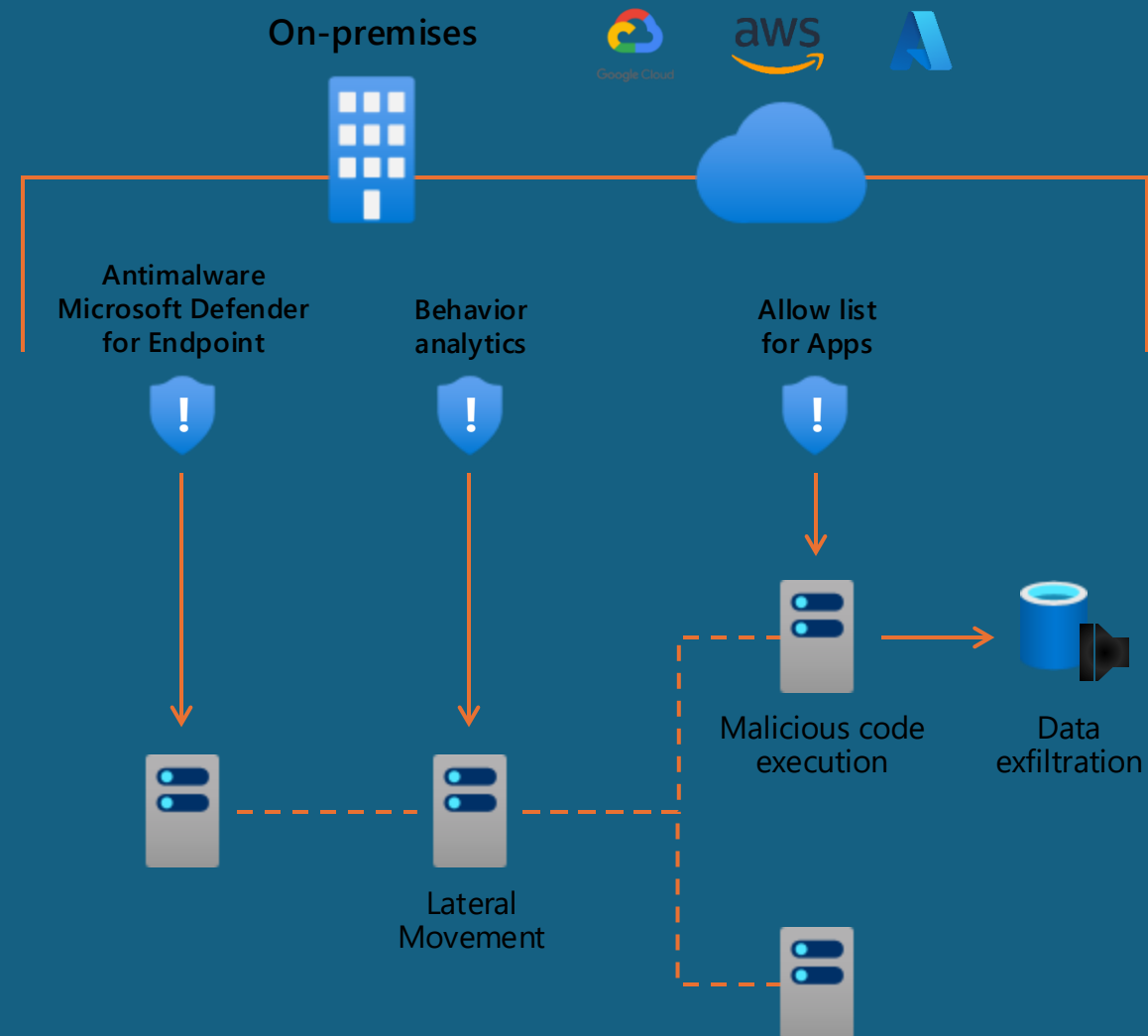
- Running VMs in the cloud requires an additional layer of security to protect the control plane surrounding your servers
- Threat detections need to extend to connected, cloud-native components including network, storage, and the control plane to fully assess and protect the security state of your servers
- To be effective, modern workload protection solutions need to provide traditional VM security and provide optimized detections and mechanisms for cloud-based resources



Microsoft Defender for Servers

Protect your servers from threats

- Central VM security view
- Simple onboarding experience with frictionless auto-provisioning
- Discovery of unmonitored machines



Microsoft Defender for Servers

Protect machines in hybrid and multi-cloud environments



Multicloud support

- Support any Windows and Linux servers
- Coverage for managed services incl. Amazon EC2 and Google Compute Engine



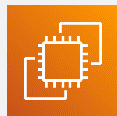
Leading EDR solution

- Integrated with Defender for Endpoint
- Next generation antivirus protection
- Endpoint detection and response
- Automated self-healing
- Vulnerability Assessment



Optimized for Cloud environments

- Adaptive Application Control
- Just in time VM access
- File integrity monitoring
- Adaptive network hardening

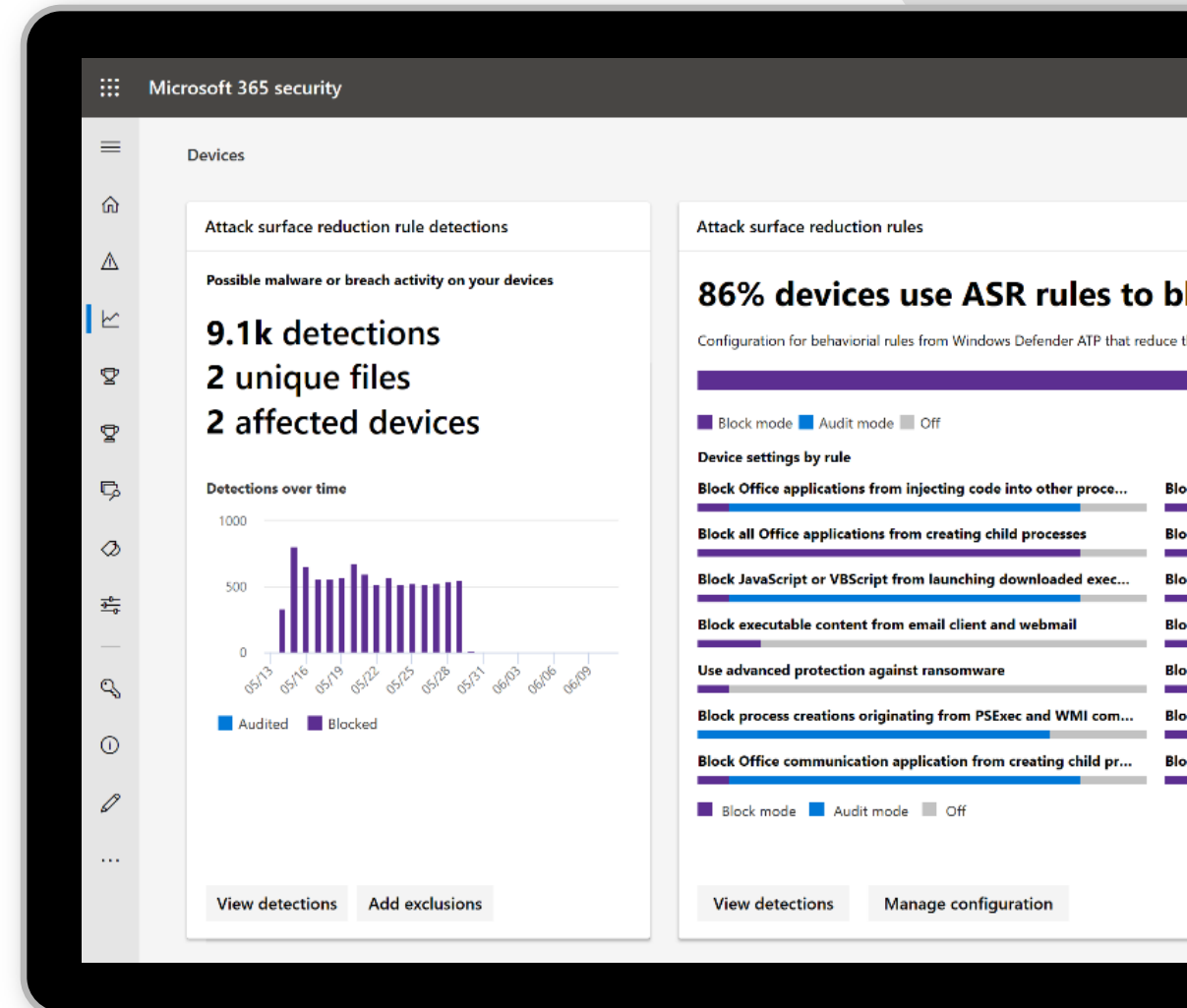


Attack surface reduction

Powered by Microsoft Defender for Endpoint

Eliminate risks by reducing the surface area of attack

- System hardening without disruption
- Customization that fits your organization
- Visualize the impact and simply turn it on

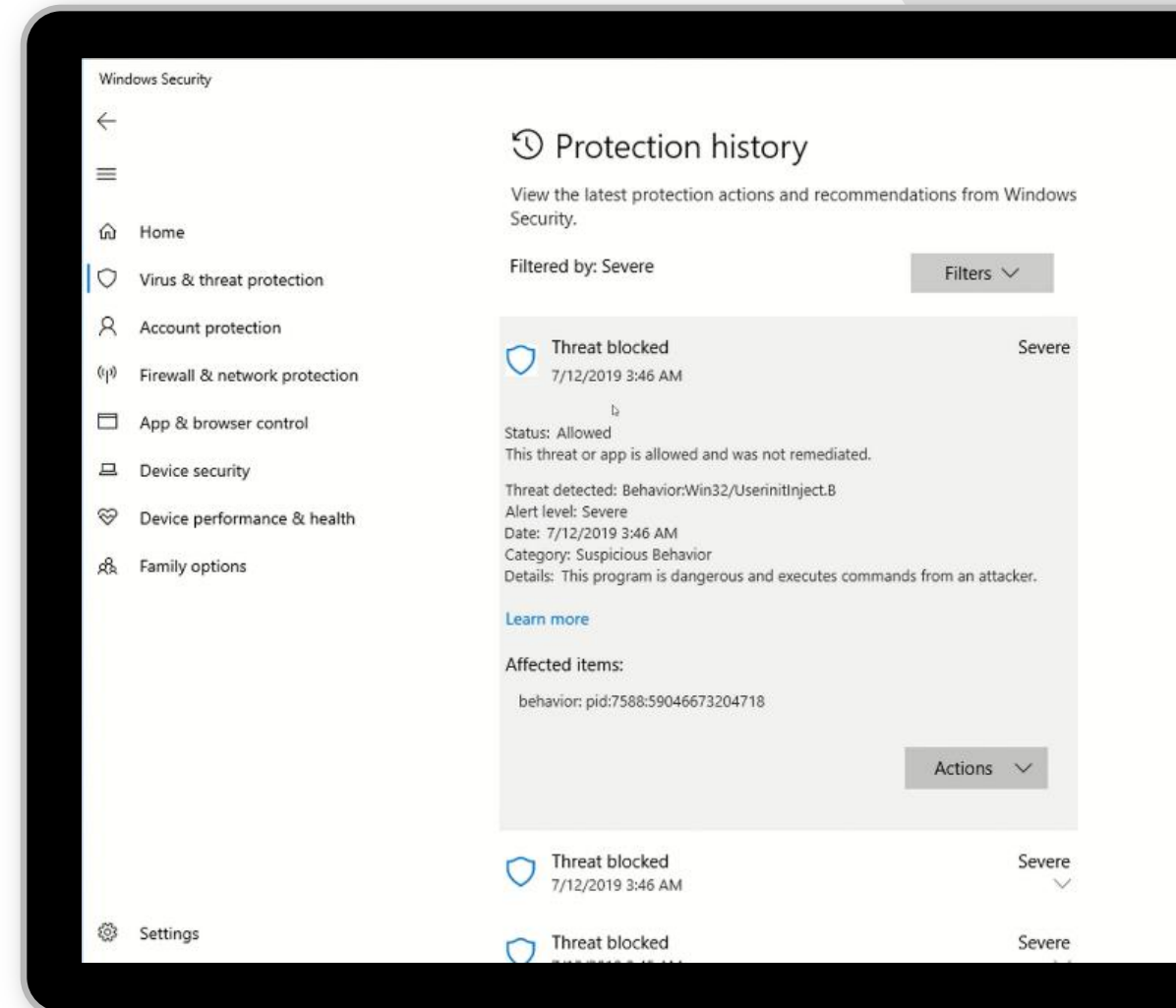


Next generation antivirus protection

Powered by Microsoft Defender for Endpoint

Blocks and tackles sophisticated threats and malware

- Behavioral based real-time protection
- Blocks file-based and fileless malware
- Stops malicious activity from trusted and untrusted applications



Endpoint detection & response

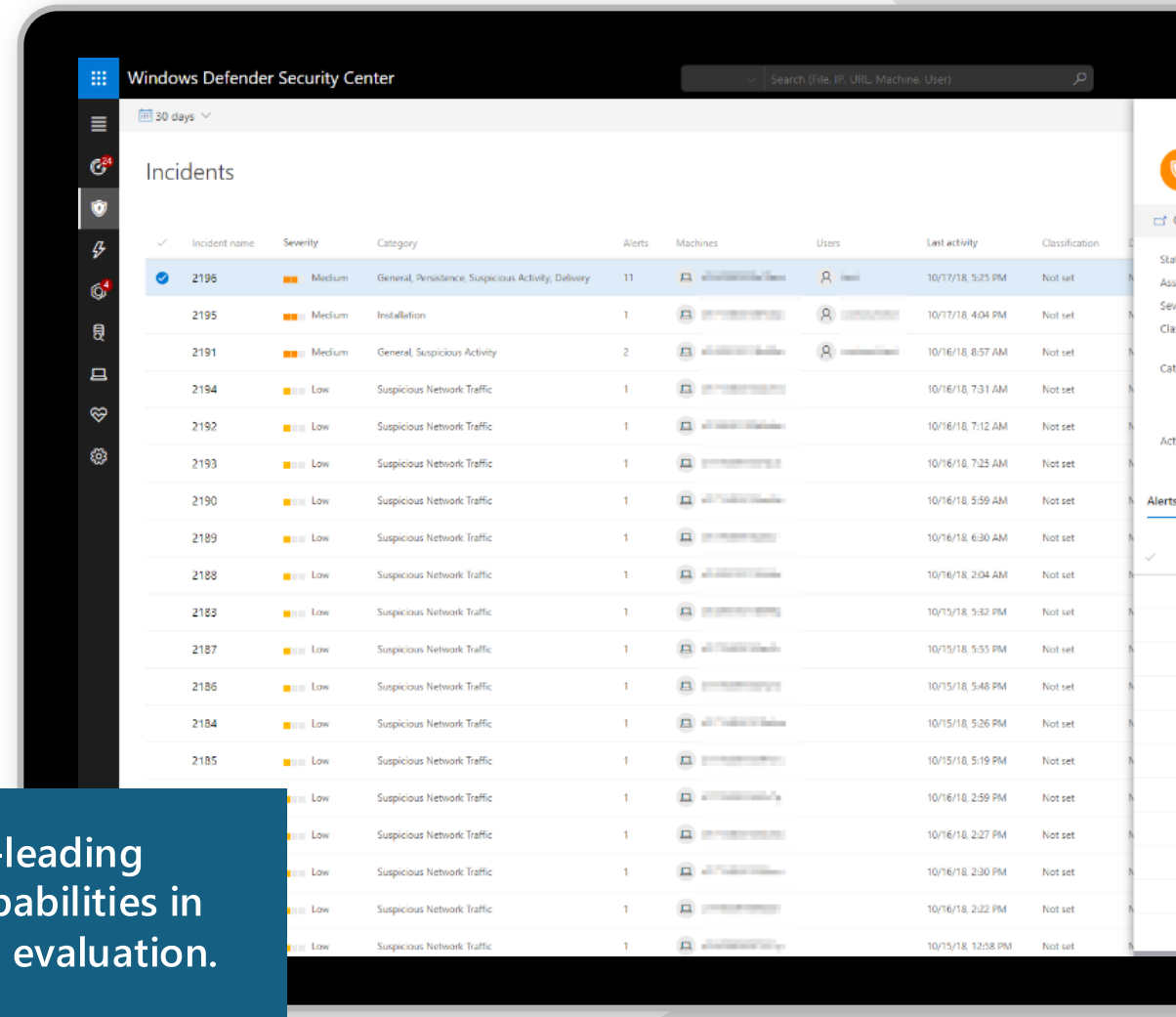
Powered by Microsoft Defender for Endpoint

Detect and investigate advanced persistent attacks

- Correlated behavioral alerts
- Investigation & hunting over six months of data
- Rich set of response actions

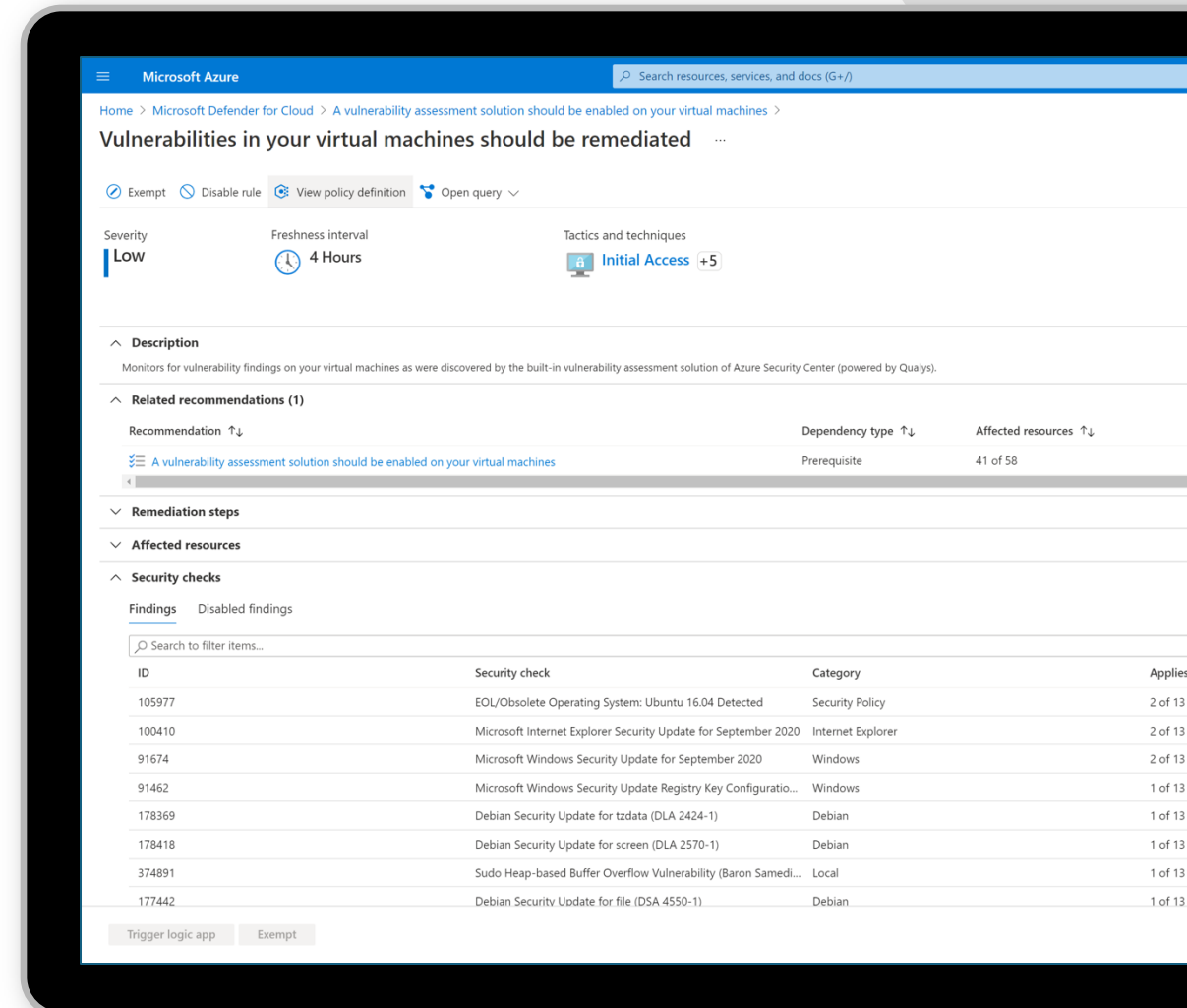


Demonstrated industry-leading optics and detection capabilities in MITRE ATT&CK®-based evaluation.



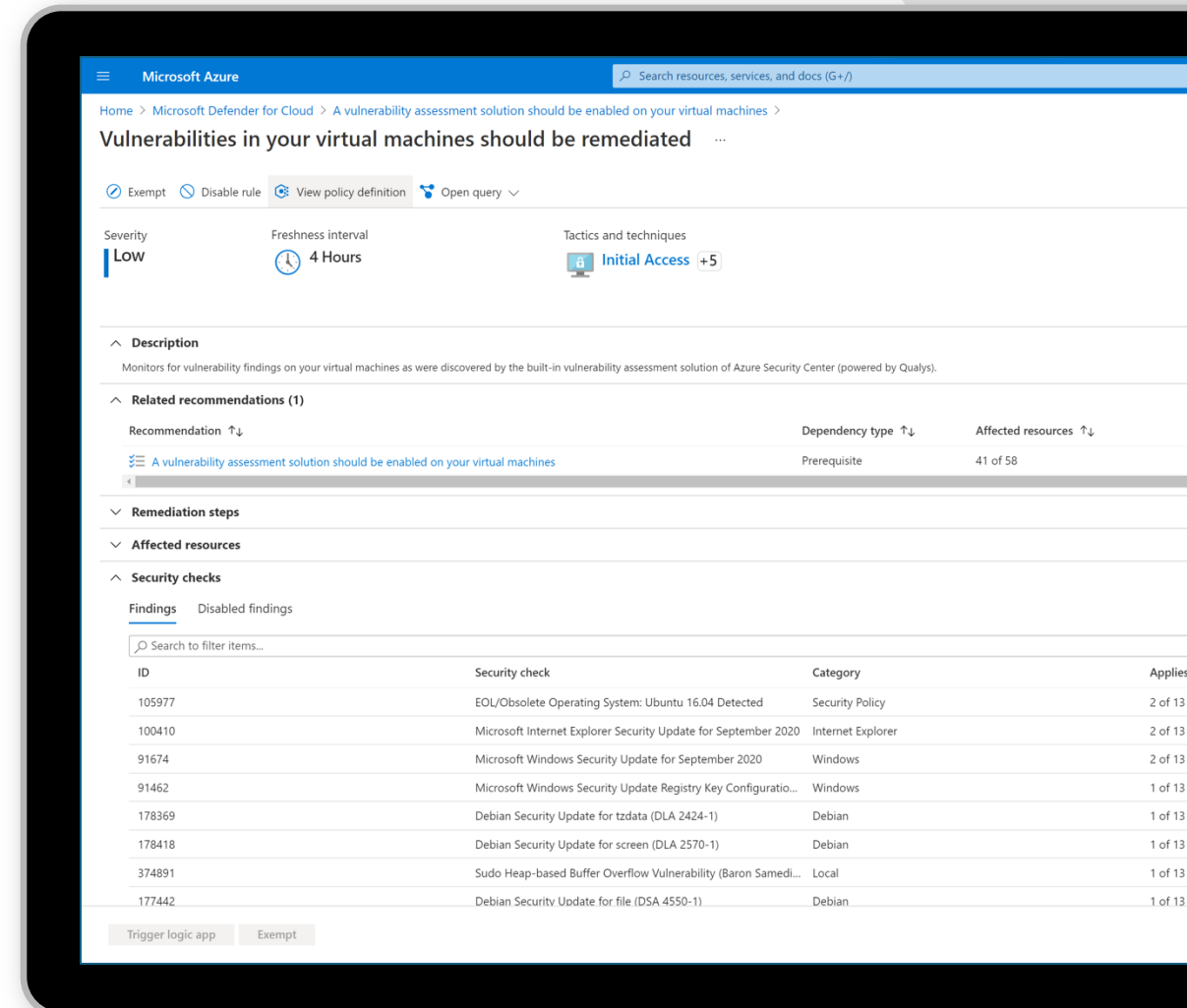
Assess your VMs and containers for vulnerabilities

- Automated deployment of the vulnerability scanner
- Continuously scans installed applications to find vulnerabilities for Linux & Windows VMs
- Visibility to the vulnerability findings in Security Center portal and APIs
- Choose between Qualys and Microsoft's threat and vulnerability management capabilities



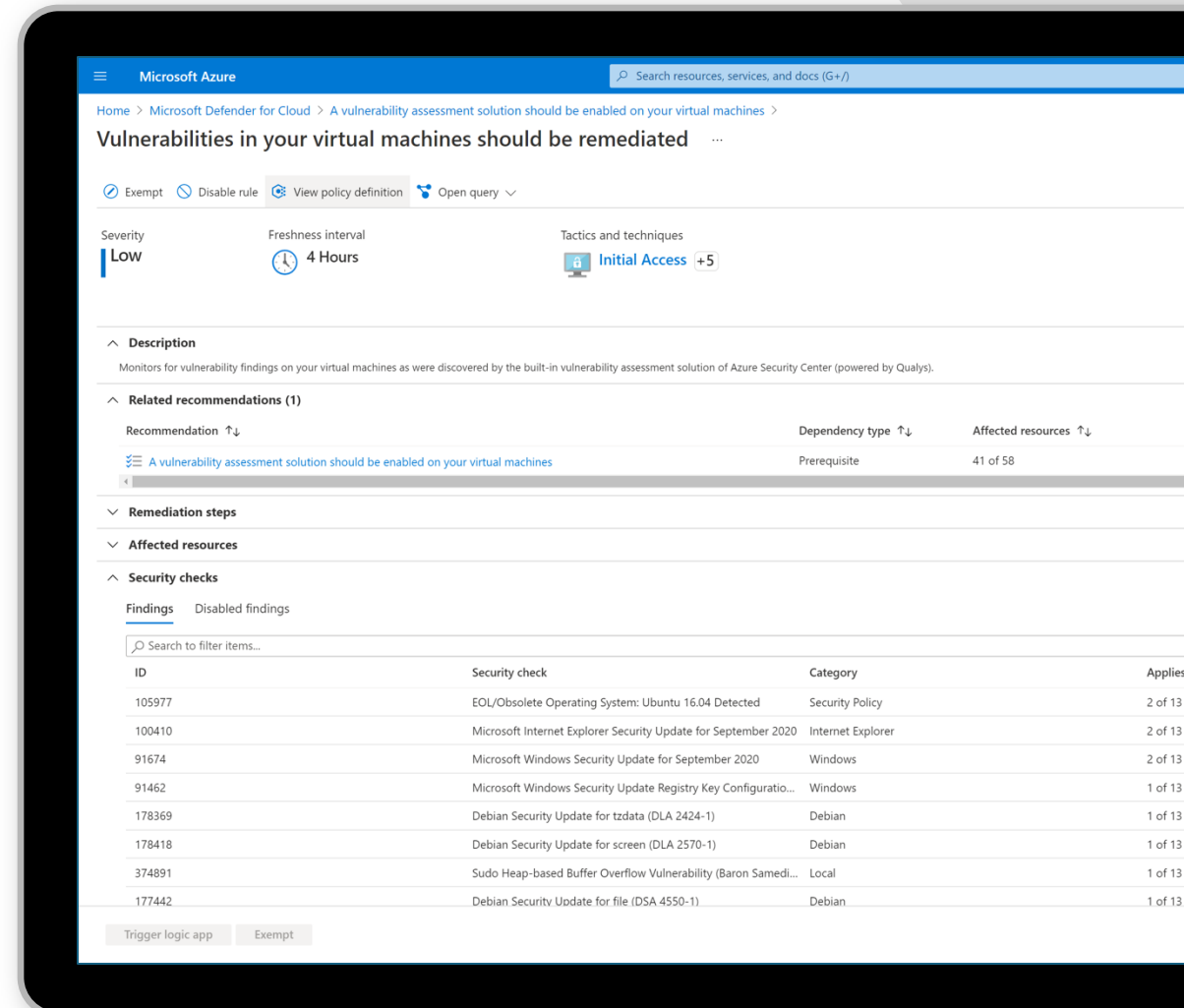
Just-in-time VM access

- Lock down the inbound traffic to your VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed



File integrity monitoring

- Examine OS files, Windows registries, application software, Linux system files, and more, for changes that might indicate an attack
- Select the files that you want to be monitored using suggestions or your own logic



Supported operating systems



Windows Server 2012 R2

Windows Server 2016

Windows Server, version 1803 or later

Windows Server 2019

Windows Server 2022



Red Hat Enterprise Linux 7.2+

Red Hat Enterprise Linux 8.x

CentOS 7.2+, 8

Ubuntu 16.04, 18.04, 20.04

SUSE Linux Enterprise Server 12, 15

Oracle Linux 7.2 or higher

Oracle Linux 8.x

Amazon Linux 2

Onboarding

- Enable Defender for Servers P1 or P2 in the Azure Portal (one-click)
- Install the Azure Arc agent to on-prem and non-Azure cloud servers
- MDE will be automatically provisioned- via the MDE.Windows & MDE.Linux extensions
- On-premise servers are now onboarded to Defender for Cloud and Defender for Endpoint

1. Server onboards to Azure Arc (the server is then discoverable by Defender for Servers)
2. Then Defender for Servers automatically provisions MDE to this server as an extension
3. Defender for Endpoint capabilities are now available on the server



Feature comparison

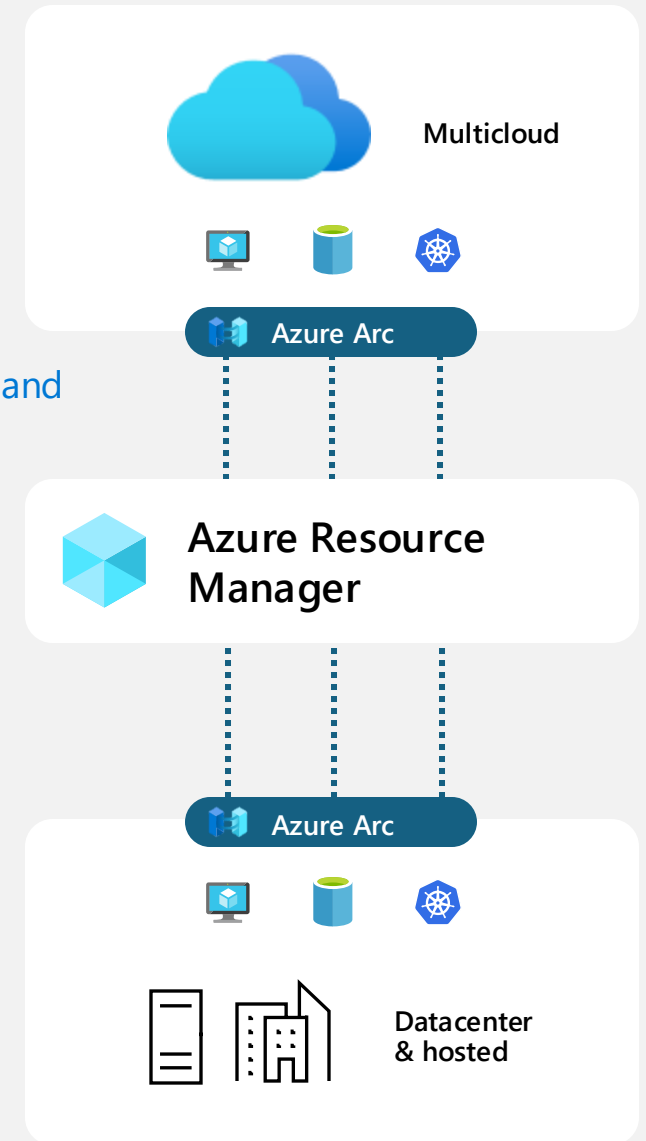
Feature	Defender for Servers P1 (\$5)*	Defender for Servers P2 (\$15)*
Defender for Endpoint integration	✓	✓
Licensing	✓	✓
Defender for Endpoint provisioning	✓	✓
Unified view	✓	✓
Threat detection for OS-level (agent-based)	✓	✓
Threat detection for network-level (agentless)		✓
Microsoft Defender Vulnerability Management Add-on		✓
Security Policy and Regulatory Compliance		✓
Free data ingestion (500 MB) in workspaces		✓
<u>Just-in-time virtual machine access</u>		✓
<u>File integrity monitoring</u>		✓
<u>Docker host hardening</u>		✓
<u>System updates and patches</u>		✓
Agentless scanning		✓

Use Azure Arc to connect workloads anywhere to Microsoft Defender for Cloud

- Azure Arc unlocks hybrid and multicloud scenarios so you can manage security for all your resources in a consistent way
- Enforce compliance and simplify audit reporting
- Asset organization and inventory with a unified view in the Azure Portal—Azure Tags
- Server owners can view and remediate to meet their compliance—RBAC in Azure

Azure Arc enables cloud management and security protections

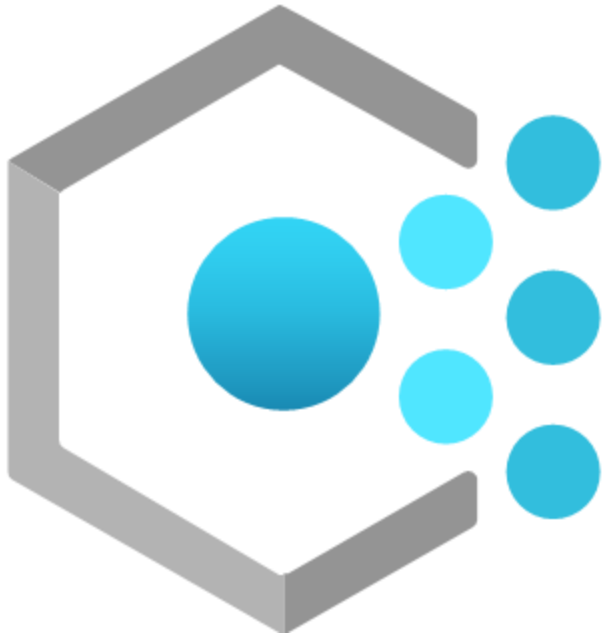
Single control plane for any resource, anywhere



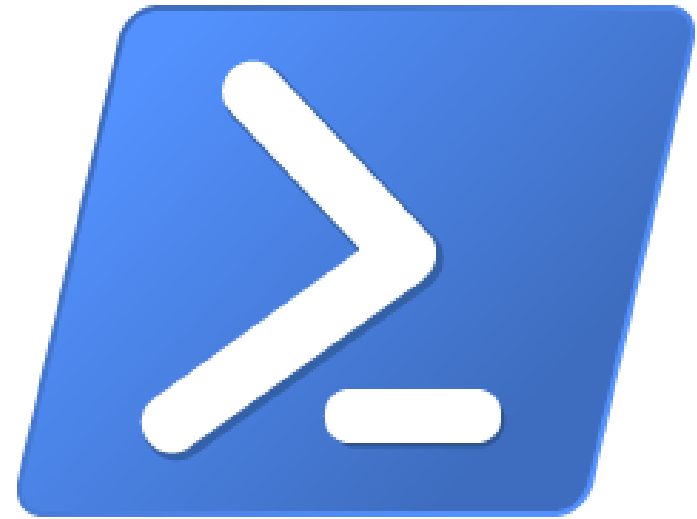
Demo



Manage Microsoft Defender for Servers plans



Azure Policy



Powershell Script

Microsoft Defender for Cloud

- Secure and protect resources across the three major cloud providers and hybrid environments in one place

- Ensure secure and compliant configuration of cloud resources

- Detect vulnerabilities and threats to protect against malicious attacks




SIEM

Microsoft Sentinel

Visibility across your entire organization


Existing security
portfolio


Microsoft
ecosystem

 Windows



macOS



iOS

aws



Microsoft 365 Defender

Secure your end users

Microsoft Defender for Cloud

Secure your infrastructure

XDR



Grazie!