Microsoft Security

Azure DCS (aka MPC) Session #5

Defender for Cloud Workloads – August 2023

Jeff Beckitt
Technical Specialist - Security

Azure DCS (aka MPC) Session #5 | Agenda

Times are approximate and best guess only 😄.

Workshop: 2 hours	
Duration	Content
45 mins	Microsoft Defender for Cloud Overview
20 mins	• Defender for Server Plan 1 & Plan 2
40 mins	Defender for ….
15 minutes	Q&A and discussion

Cloud security is more important than ever

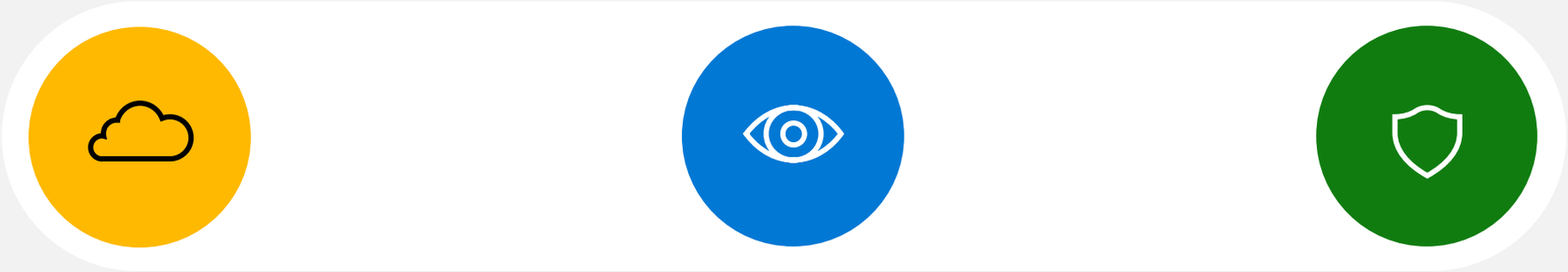
Cloud migration involves ongoing on-prem (hybrid) and multicloud resources, expanding the attack surface

Increasing complexity of in the development and deployment of cloud applications

Complex and dynamic regulatory landscape

Securing multicloud environments

Top-of-mind



Develop and operate secure apps in the cloud

>54%

of enterprises do not integrate security into DevOps pipelines.[1]

Visibility into security and compliance

86%

of surveyed security decision makers believe their cybersecurity strategy doesn't keep up with their multicloud environments.[2]

Protect against increasing, sophisticated attacks

$4.24M

is the average cost of a breach, 2021.[3]

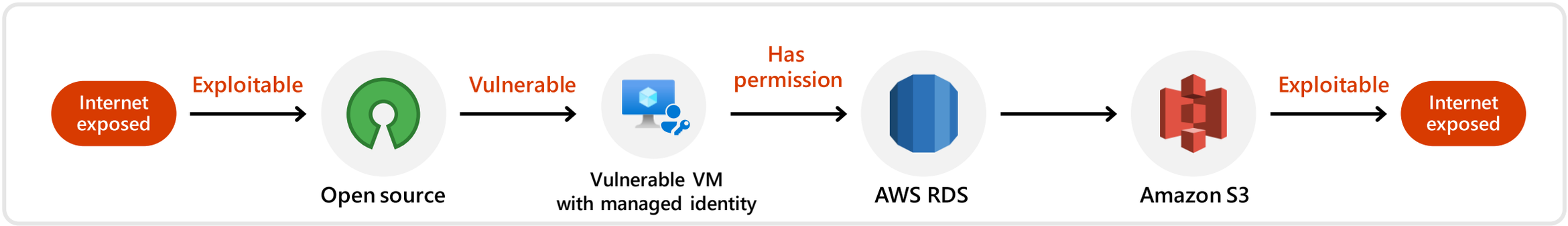
1. Microsoft Enterprise DevOps Report
2. Microsoft Cloud Security Priorities and Practices Research
3. Ponemon Institute, Cost of a Breach Report

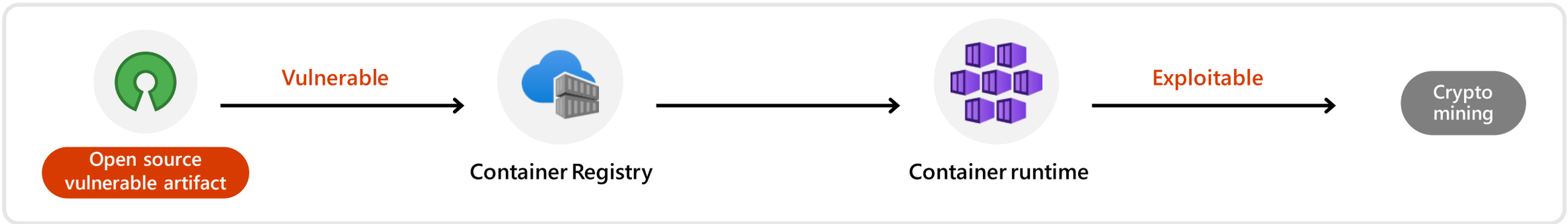
Attacker point of view of potential kill chains

Do you have an effective detection and response tool in the cloud?

Do you know where is your data and is it sensitive?

Can you describe how effective your guardrail and governance policy?





Cloud security and protection needs

DevSecOps

(including development artifact scanning and Infrastructure-as-Code scanning)

Cloud security posture management

Cloud workload protection

Cloud infrastructure entitlement management

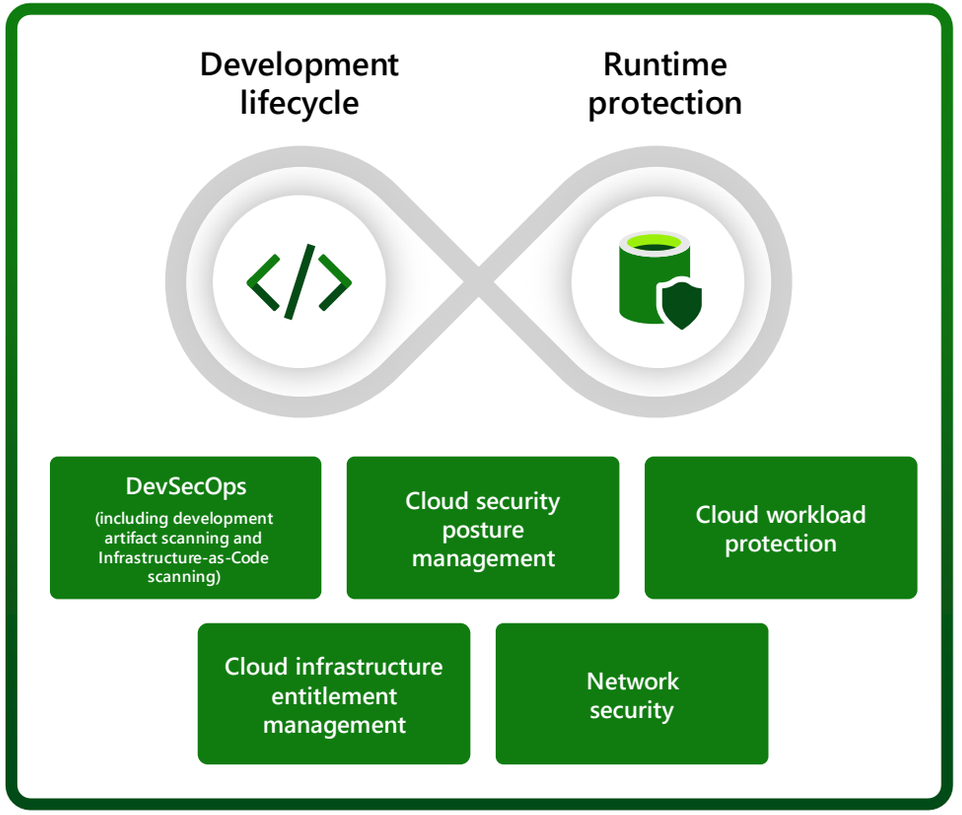
Network security

Microsoft's cloud-native application protection platform (CNAPP)

Get integrated protection for your multicloud resources, app, and data.
Named by Gartner as a representative CNAPP provider.

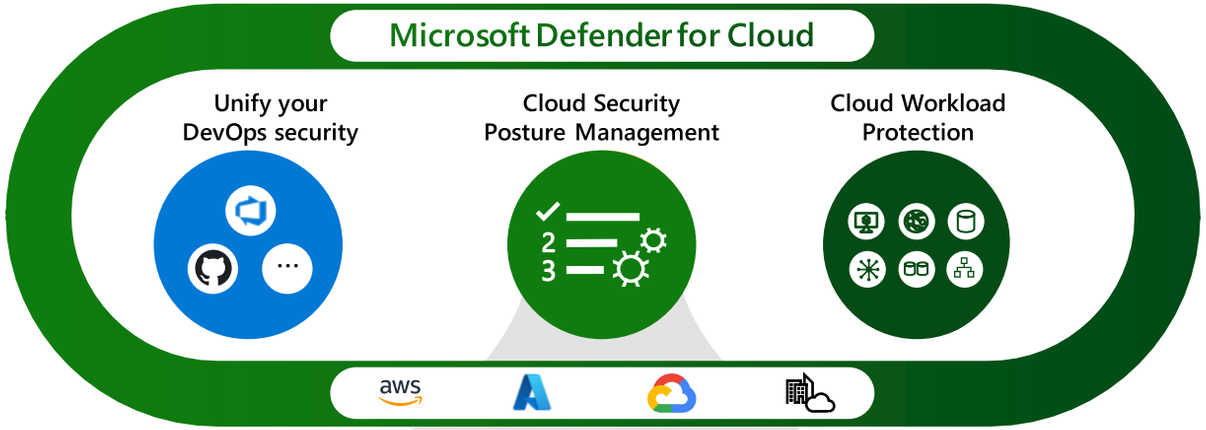
Hybrid and multicloud

- Code
- Compute
- Identity
- Data
- Storage



Unified security and compliance capabilities to prevent, detect, and respond to modern cloud security threats across the entire cloud app lifecycle

Access CNAPP capabilities in Microsoft Defender for Cloud



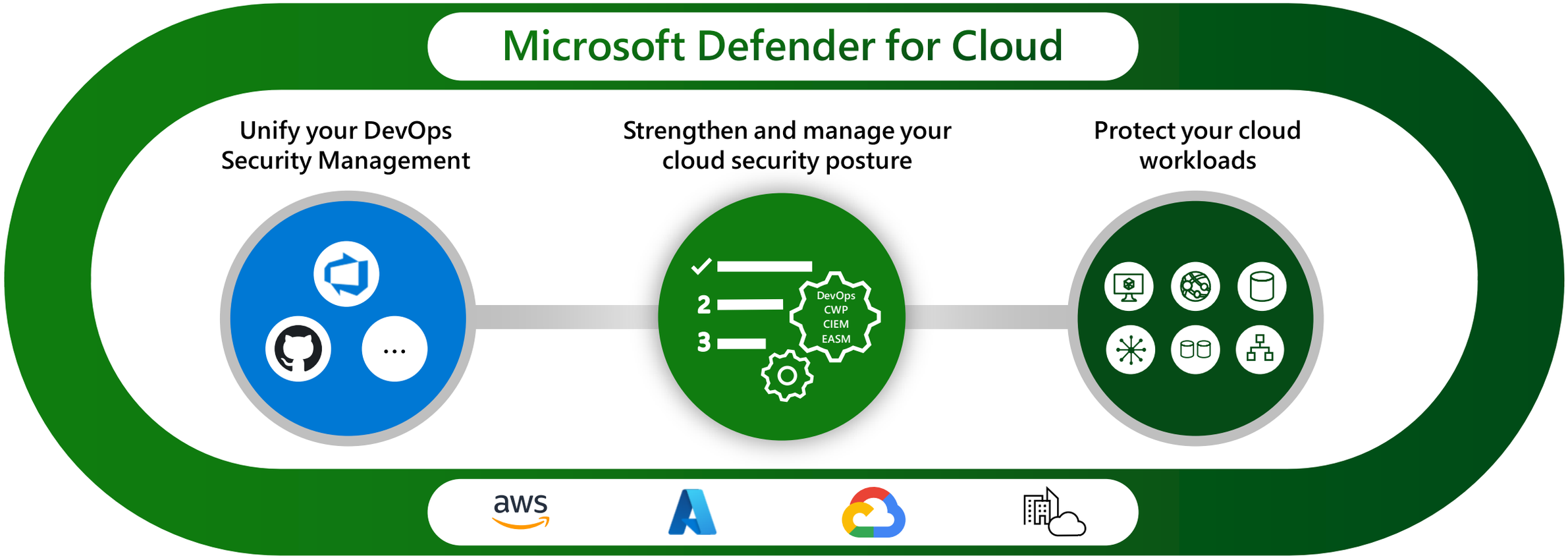
Microsoft Purview
(Data security)

Microsoft Defender External Attack Surface Management
(EASM)

Microsoft Entra Permissions Management
(CIEM)

Azure Network Security

Microsoft Sentinel
(SIEM)


Microsoft Defender for Cloud
Unify your DevOps Security Management
Strengthen and manage your cloud security posture
Protect your cloud workloads
2
3
DevOps
CWP
CIEM
EASM
aws

How we're different

Multi-cloud and hybrid support

- Streamlined auto-provisioning for new resources
- Multicloud security benchmark for compliance
- Multicloud agentless vulnerability scanning
- Built in with Azure with no deployment required and the broadest protection coverage

Contextual code to cloud security

- Integrated view across clouds to manage security posture, assess risk, and take required actions
- Prioritized recommendations with attack path, reducing noise by up to 99%
- Track and manage your security posture state over time

Full-lifecycle protection

- Manage security of cloud-native applications with a single platform
- Minimize vulnerabilities from making it to production with code scanning and IaC scanning
- Reduce time to remediate with integrated workflows into developer environments

Advanced Threat Protection

- Workload-specific signals and threat alerts
- CWPP with dedicated workload protection for Azure storage and databases
- Deterministic, AI, and anomaly-based detection mechanisms
- Leverages the power of Microsoft Threat Intelligence with 43 trillion signals daily

Unify DevOps Security Management

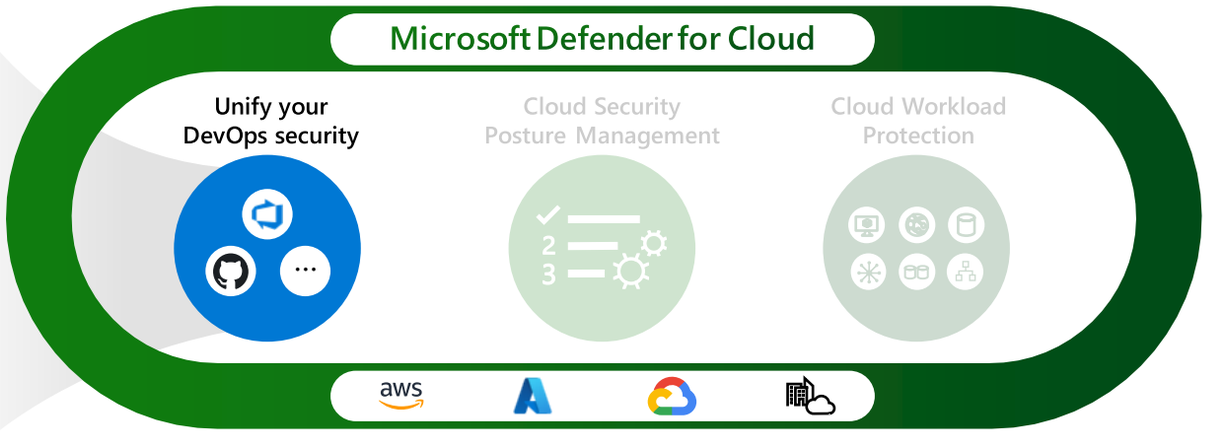
Unify your DevOps security

DevOps posture visibility
Code | Dependencies | Secrets | Container images | Infrastructure-as-Code security insights

Infrastructure-as-Code security
ARM | Bicep | Terraform | CloudFormation | Many more

Code-to-cloud contextualization
Across multipipeline and multicloud environments

Integrated workflows
Pull request annotations | Developer ownership assignments

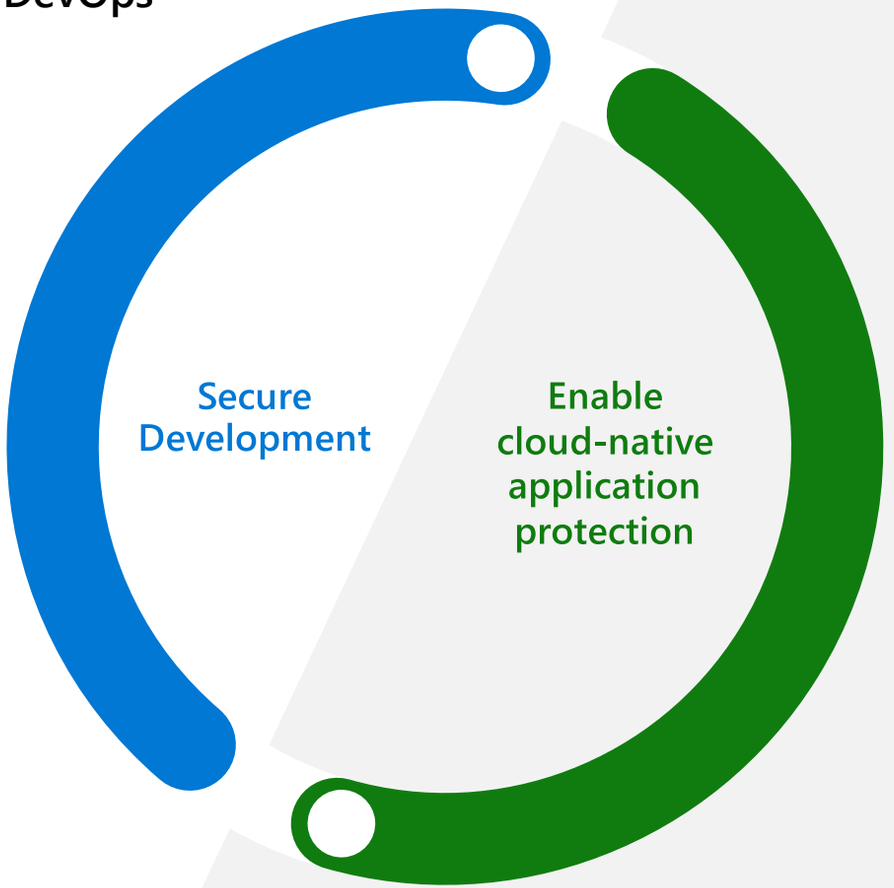


Better together

GitHub Advanced Security
GitHub Advanced Security for Azure DevOps

Developer first. Community driven.

- Code security
- Dependencies security
- Embedded secrets protection
- Developer remediation



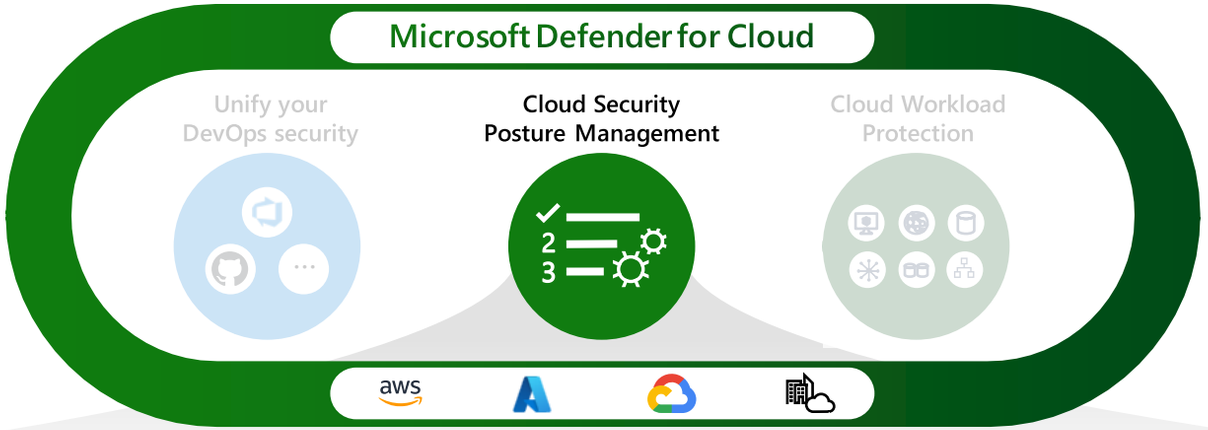
Defender for DevOps

Unify multi-pipeline DevOps security

- Multi-pipeline DevOps security management
- Infrastructure-as-code security
- Code to cloud contextualization
- Automated workflows

Strengthen and manage your Security Posture with Microsoft Defender for Cloud

Cloud security posture management



Foundational CSPM (free)

Asset inventory and secure score analysis
Frictionless onboarding | +450 built-in assessments | Custom capabilities | Policy management

Advanced remediation
Quick-fix remediation | Automated remediation using Logic Apps | Enforcement policies

Data export and out-of-the-box reporting
Built in Azure Workbooks | At-scale data streaming and export | Integration with SIEM/SOAR solutions

Integrated workflows and automation
Out-of-the-box and custom automations triggered by security events

Defender CSPM

Agentless vulnerability scanning
Visibility on software and CVEs | Disc snapshots | Insecure secrets and keys

Integrated data and insights
Defender for DevOps | Defender External Attack Surface Management |

Contextual cloud security and risk prioritization
Attack path analysis | Intelligent cloud security graph | Custom path queries on cloud security explorer | Risk-based prioritization

Regulatory compliance and industry benchmarks
Over 50 standards | Multicloud Microsoft security benchmark | Compliance dashboard and reporting | Integration with Microsoft Purview compliance manager

Governance management
Assign owners automatically | Drive accountability in the organization | Grace period | Reduce time to remediate

Data-aware security posture
Multicloud data estate discovery | Identify data flows and resources containing sensitive and shadow data | Uncover potential sensitive data exposure and data breaches

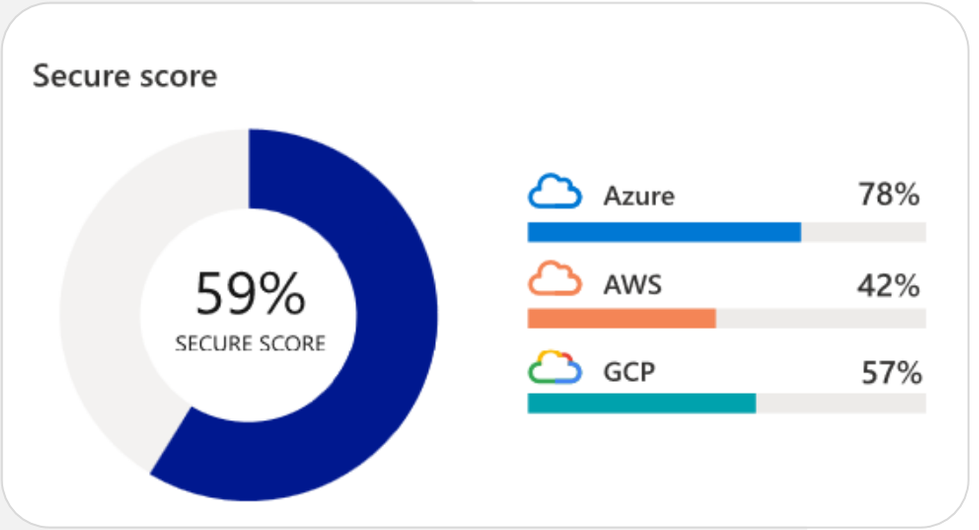
Free foundational CSPM

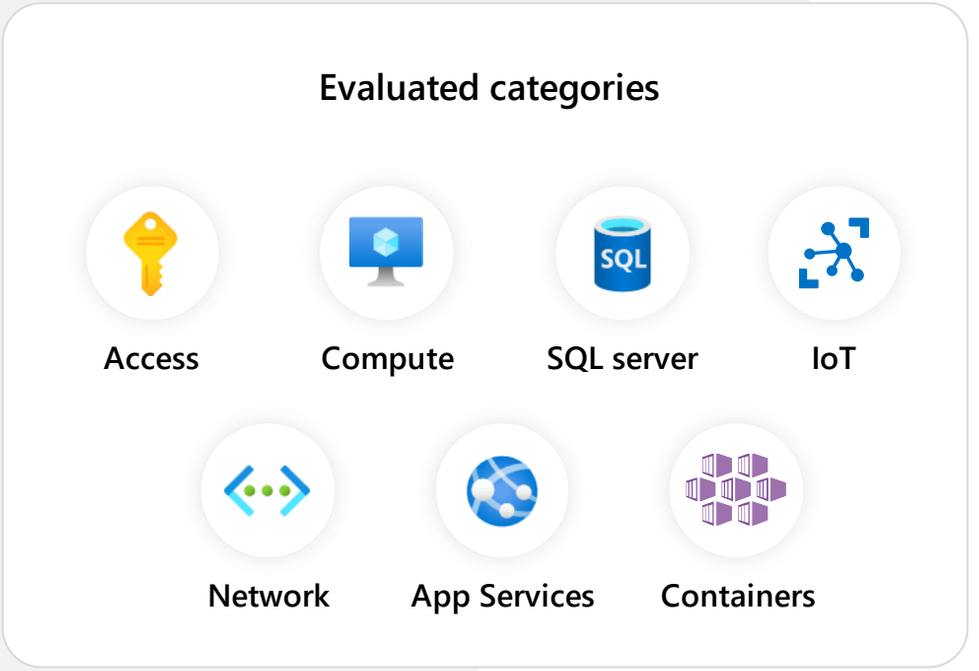
Secure Score

- Strengthen security posture across all critical cloud resources including network, access, compute, databases, your service layer, and more
- 450+ out-of-the-box recommendations
- Create custom recommendations to meet organizational requirements

Multicloud security benchmark for security compliance

- Manage cloud security compliance with continuous assessment of cloud resources across Amazon Web Services, Microsoft Azure, and Google Cloud Platform in a single, integrated dashboard
- Use industry standards, regulatory compliance frameworks, and cloud-specific benchmarks to implement best practices (CIS, PCI, NIST, SOC, ISO HIPAA, etc.)
- Create custom recommendations to meet unique organizational needs





Microsoft Defender CSPM

Cut through the noise and get in front of your most critical risks across your multicloud and hybrid environments with contextual security posture management.

Continuous monitoring and intelligent prioritization from attack path analysis

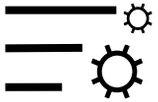
Agentless vulnerability scanning provides visibility across your environment. And attack path analysis uses integrated insights to prioritize potential lateral movement paths.

Prevent data breaches and sensitive data exposure

Data-aware security posture management helps teams continuously discover their cloud data estate, automatically identify and assess risks, and prioritize remediation of sensitive data exposure.

Centralized visibility with integrated CNAPP insights

The cloud security graph integrates insights across CWP, DevOps, Microsoft Entra (CIEM), Defender EASM, Microsoft Sentinel (SIEM), Microsoft 365 Defender, and Azure Network Security.



Remediate vulnerabilities and misconfigurations with governance rules and remediation at scale

Easily reach resource owners of identified risks and automatically assign ownership across the organization to drive remediation at scale and reduce time to mitigate

Foundational CSPM vs Defender CSPM

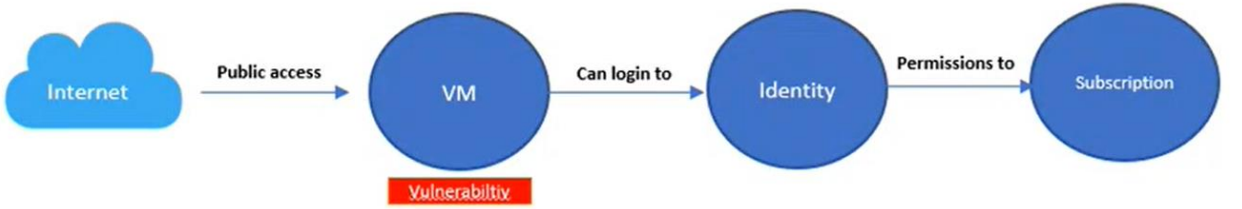
Feature	Foundational CSPM (free)	Defender CSPM (billing applies)
Security recommendations (recommendations across infrastructure, i.e. Network, CIEM, etc.)	●	●
Asset inventory	●	●
Secure score	●	●
Data visualization and reporting with Azure Workbooks	●	●
Data exporting	●	●
Workflow automation	●	●
Remediation Tracking	●	●
Microsoft Cloud Security Benchmark	●	●
'Azure Policy' based recommendation customization	●	●
Integration with Entra Permissions Managements	●	●
KQL based recommendation customization		●
Regulatory compliance assessments		●
Governance		●
Attack path analysis		●
Cloud security explorer		●
EASM insights in network exposure		●
Agentless vulnerability assessments for compute (using Microsoft Defender Vulnerability Management)		●
Agentless discovery for Kubernetes *(public preview on April 15)*		●
Agentless vulnerability assessments for container images, including registry scanning *(public preview on April 15)*		●
Sensitive data discovery *(generally available for Storage in May)*		●
Data flows discovery (*generally available in May*)		●

Foundational CSPM vs Defender CSPM (Cloud coverage)

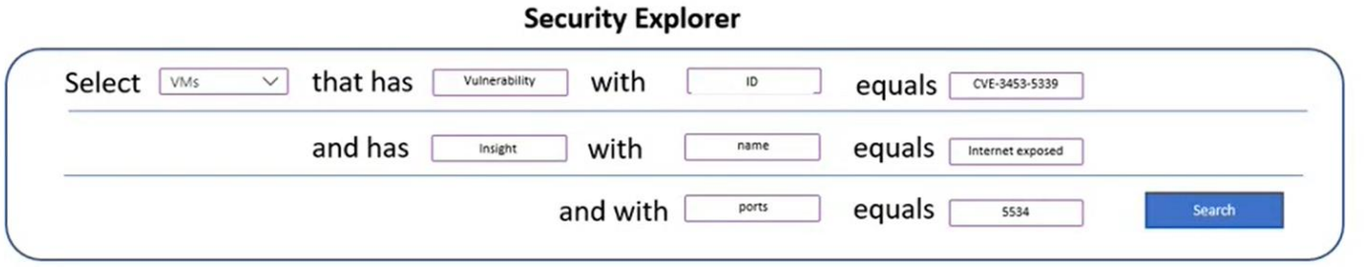
Feature	Foundational CSPM (free)	Defender CSPM (billing applies)	Cloud coverage		
			Azure	AWS	GCP
Security recommendations (recommendations across infrastructure, i.e. Network, CIEM, etc.)	●	●	●	●	●
Asset inventory	●	●	●	●	●
Secure score	●	●	●	●	●
Data visualization and reporting with Azure Workbooks	●	●	●	●	●
Data exporting	●	●	●	●	●
Workflow automation	●	●	●	●	●
Remediation Tracking	●	●	●	●	●
Microsoft Cloud Security Benchmark	●	●	●	●	
'Azure Policy' based recommendation customization	●	●	●	●	
Integration with Entra Permissions Managements	●	●	●	●	●
KQL based recommendation customization		●		●	●
Regulatory compliance assessments		●	●	●	●
Governance		●	●	●	●
Attack path analysis		●	●	●	
Cloud security explorer		●	●	●	
EASM insights in network exposure		●	●	●	
Agentless vulnerability assessments for compute (using Microsoft Defender Vulnerability Management)		●	●	●	
Agentless discovery for Kubernetes *(preview)*		●	●		
Agentless vulnerability assessments for container images, including registry scanning *(preview)*		●	●		
Sensitive data discovery *(generally available for Storage in May)*		●	●	●	
Data flows discovery (*generally available in May*)		●	●	●	

Contextual Security

Attack path Analysis

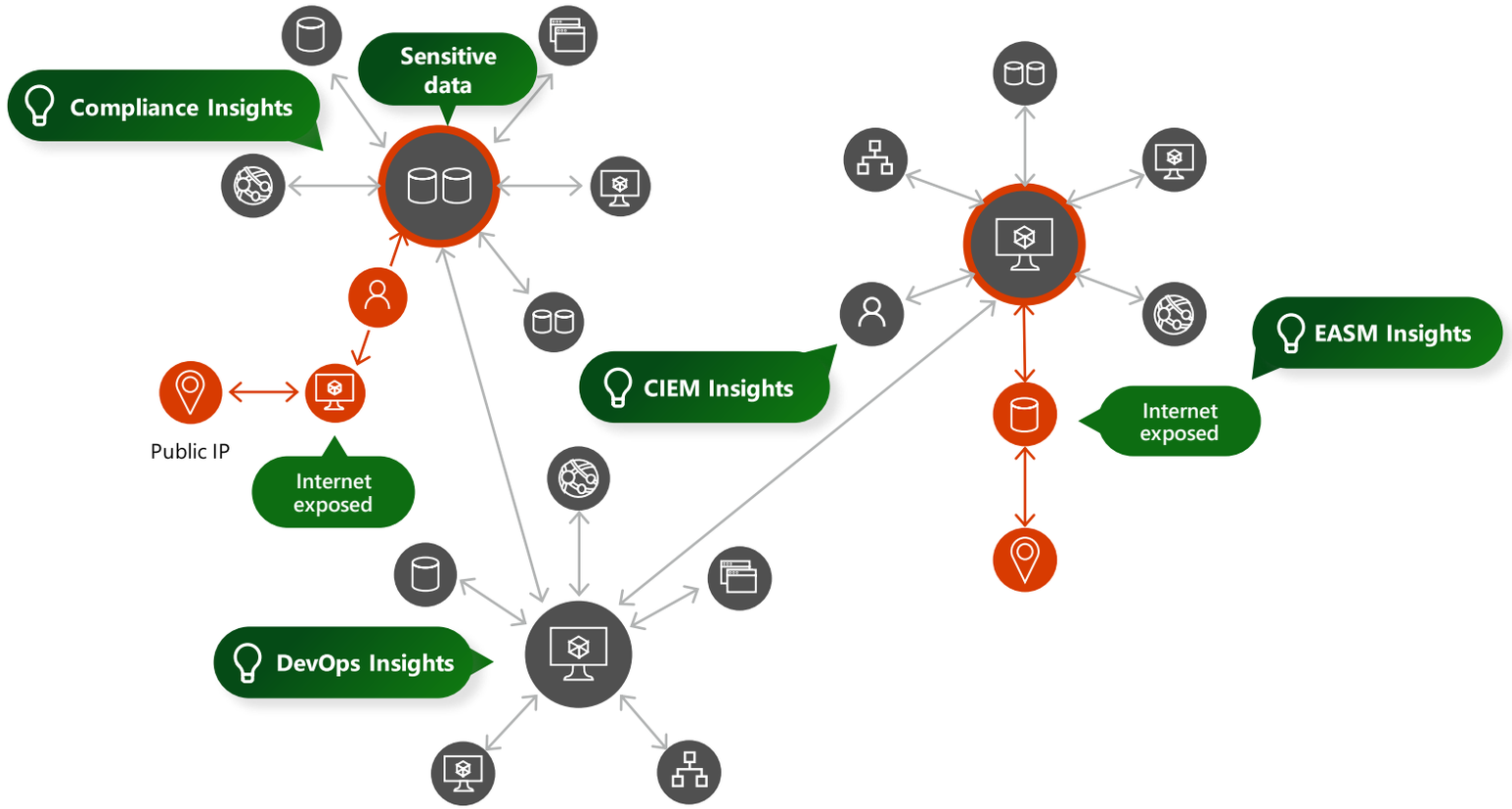


Cloud Security Map Explorer

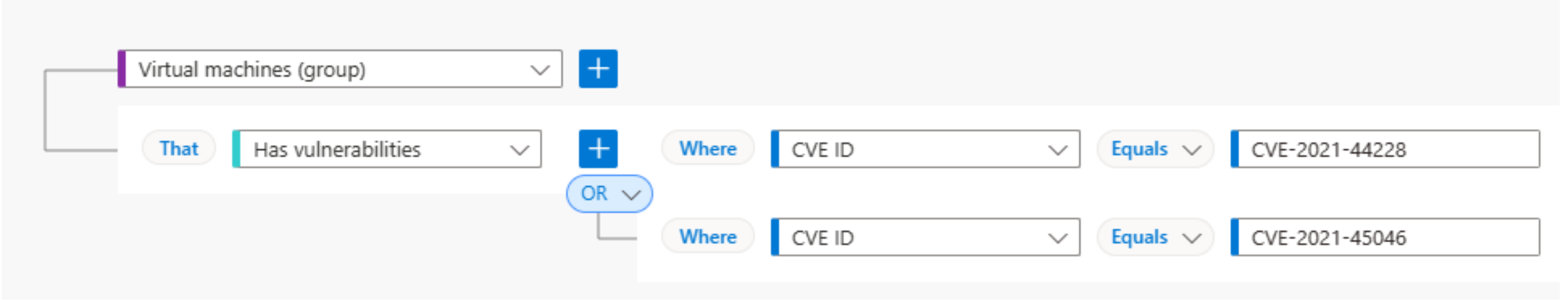


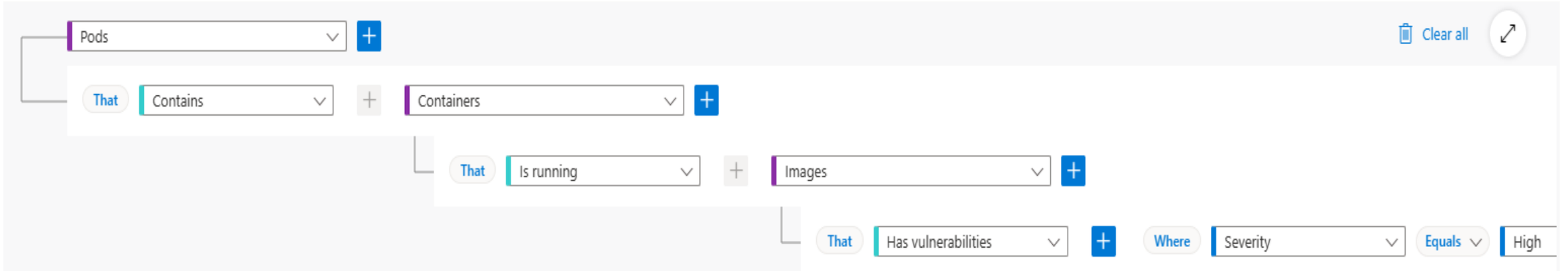
New cloud security graph to analyze blast radius

- **Agentless scanning for full visibility** across your multicloud environment and inter-connected assets.
- **Identify and prioritize lateral movement pathways** using contextual security insights.
- Use **graph-based queries to proactively find and evaluate security risks** in the right contexts to prioritize remediation actions.
- Use contextual data with integrations across **DevOps, EASM, CIEM, Compliance,** and now **data-aware posture.**



Cloud Security Explorer





Attack Path Analysis

Home > Microsoft Defender for Cloud | Recommendations >

Microsoft Defender for Cloud | Attack paths ...

Attack paths ...

Here you can see the open attack paths on the selected subscriptions.

1516 Total attack paths

547 Affected resources

19 Active recommendations

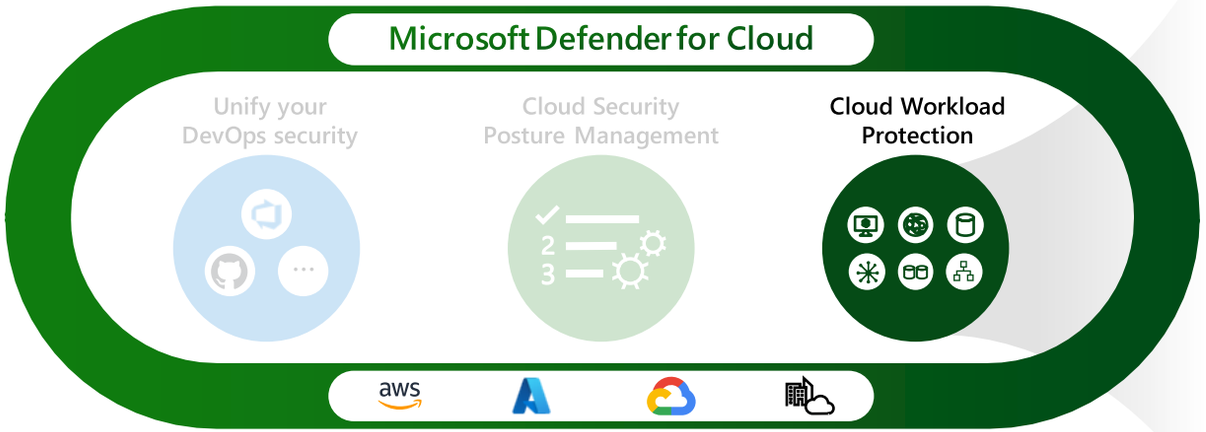
Attack path ↑↓	Environment ↑↓	Paths count ↑↓	Risk categories	Affected resources
VM with high severity vulnerabilities has read permission to a Key Vault	Azure	1	Credentials exposure, Compute abuse	
Internet exposed VM with high severity vulnerabilities has read permission to a Key Vault	Azure	1	Credentials exposure, Compute abuse	
Internet exposed VM has high severity vulnerabilities	Azure	6	Compute abuse	
Internet exposed Kubernetes pod is running a container with RCE vulnerabilities	Azure	105	Compute abuse	+
AAD User account with no MFA has read permissions on a Key Vault	Azure	88	Credentials exposure	
AAD User account with no MFA has read permissions on a data store	Azure	1291	Data exposure	+
AAD User account with no MFA has high-privileged permissions to a subscription	Azure	22	Subscription/account takeover	

< Previous Page 1 of 1 Next >

[Cloud security explorer and attack path analysis - Microsoft Defender for Cloud | Microsoft Learn]

Detect threats and protect your 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, SQL on VM

AWS workloads: Amazon EKS, Amazon EC2, SQL on VM, Unmanaged Kubernetes

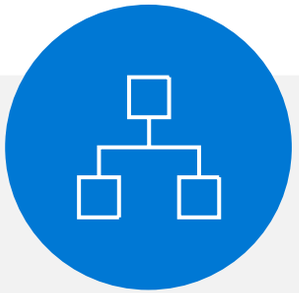
GCP workloads: GKE clusters, Google Compute, SQL on VM, Unmanaged Kubernetes

On-premises workloads: Kubernetes, SQL on VM, Servers

Threat protection for all layers of the cloud and on-premises

Threat detection

Prioritized alerts across compute, databases, the cloud service layer, and more



MITRE ATT&CK® framework mapping

Understand the effect across the adversary's attack lifecycle

Leading threat intelligence

Rely on highly sophisticated and resource-specific alerts based on Microsoft's global threat intelligence

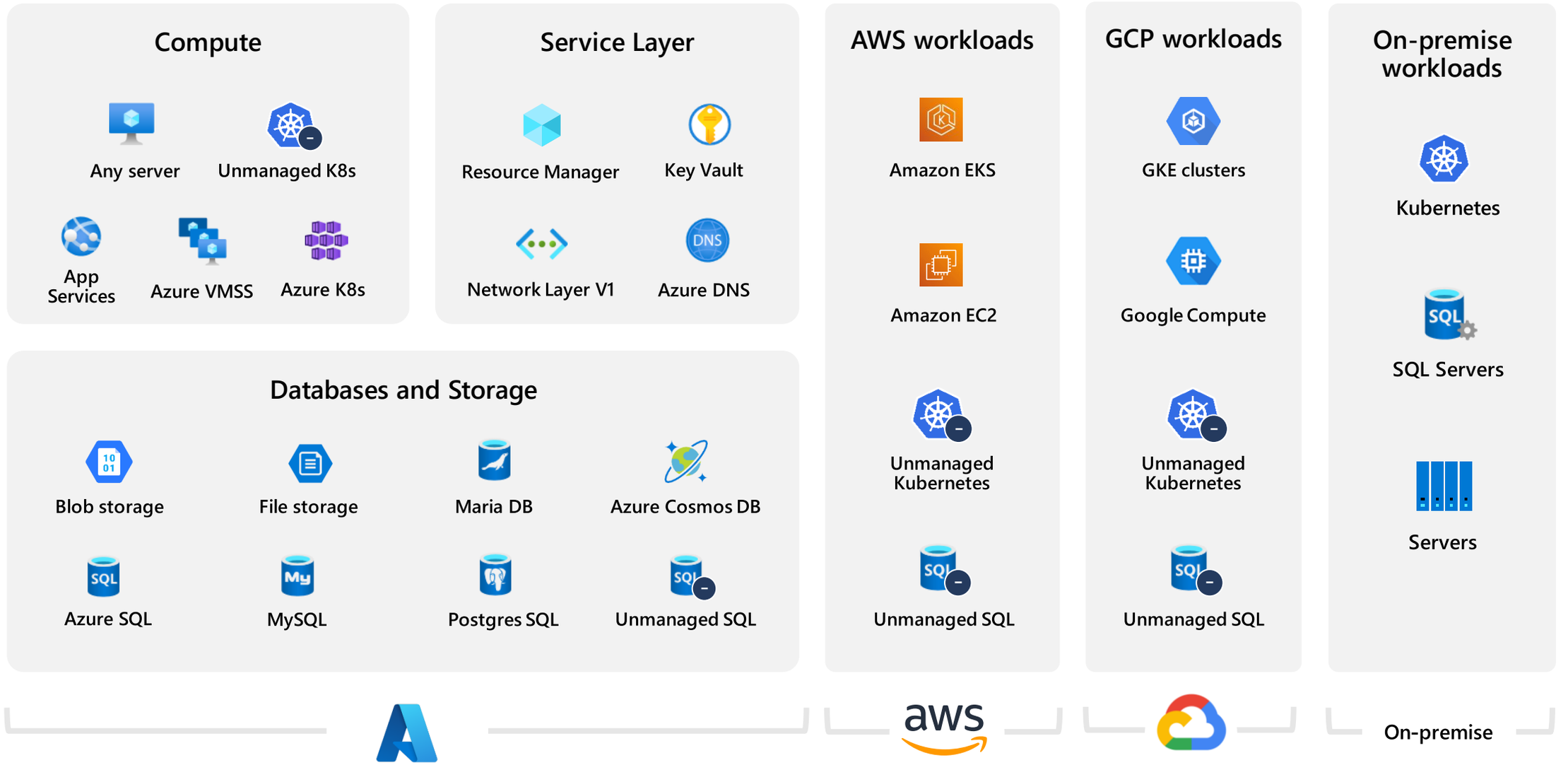
Agentless vulnerability assessment & management

Identify and remediate vulnerabilities before they are exploited

Alert correlation

Prioritize more easily with connected alerts that are grouped into incidents

Full-stack coverage with dedicated detections

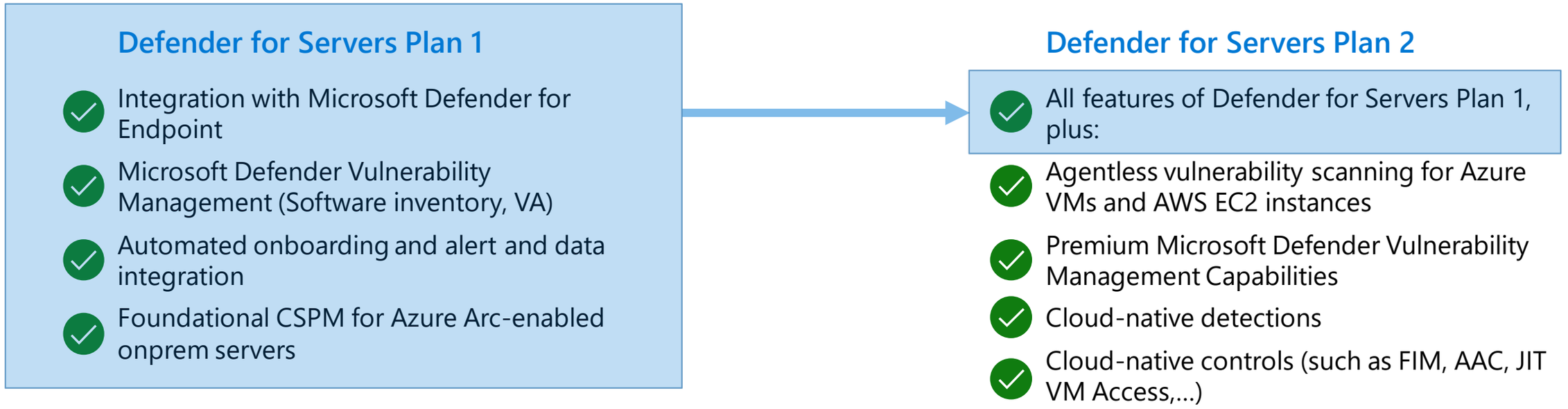


Server security in the cloud is different

- 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

Features of Defender for Servers plans

Protecting Servers using Defender for Cloud



Features of Defender for Servers plans

Annual M365 license AND Azure consumption based options

M365

Azure

Select a Defender for Servers plan in Microsoft Defender for Cloud | Microsoft Learn

Defender for Servers Plan 2

All the features of Defender for Servers Plan 1 and;

* Network Layer Threat Detection*
* Security Policy and Regulatory Compliance
* Premium Vulnerability Management functions
* Adaptive App Control
* 500MB no-cost select data ingest
* Just-in-Time virtual machine access**
* Adaptive network hardening *
* File integrity monitoring
* Docker host hardening
* Network map*
* Agentless vulnerability scanning**

* Currently Azure Only

**Azure and AWS

Defender for Servers Plan 1

Defender for Endpoint for Servers

All the features of P1 and;

* Device discovery
* Device inventory
* Core Vuln Mgmt.
* Threat Analytics
* AIRs
* Advanced Hunting
* EDR
* Endpoint Attack Notify

Defender for Endpoint P1

**endpoints only

* Next-generation protection
* Attack surface reduction
* Manual response Actions
* Centralized management
* Security reports
* APIs

Feature comparison

Feature	Defender for Endpoint for Servers ($5)	Defender for Servers P1 ($5)	Defender for Servers P2 ($15)
Hardening recommendations			
Asset discovery			
Vulnerability assessment using Microsoft Defender Vulnerability Management			
Attack surface reduction			
Next generation antivirus protection			
Endpoint detection & response			
Automated self-healing			
Hourly billing optimized for dynamic cloud resources			
Automatic agent onboarding for resources in Azure, AWS, GCP			
Management optimized for cloud environments			
Support for AWS and GCP-native compute (EC2 + Google Compute Engine)			
Unified experience for all workload types (Servers, containers, databases, and more)			
All Defender Vulnerability Management Premium capabilities: Security Baselines, Firmware & Hardware assessment, Digital Certificates, Network share analysis, Blocking Vulnerable Applications	$2/month	Not Available	
Log-analytics (500MB free)			
Regulatory compliance assessment			
Vulnerability assessments and security benchmarks			
Network layer threat detection *			
Adaptive application controls			
File integrity monitoring			
Just-in-time VM access for management ports			
Adaptive network hardening *			

* Currently Azure-only

Microsoft Defender Vulnerability Management

Advanced vulnerability management capabilities for endpoints

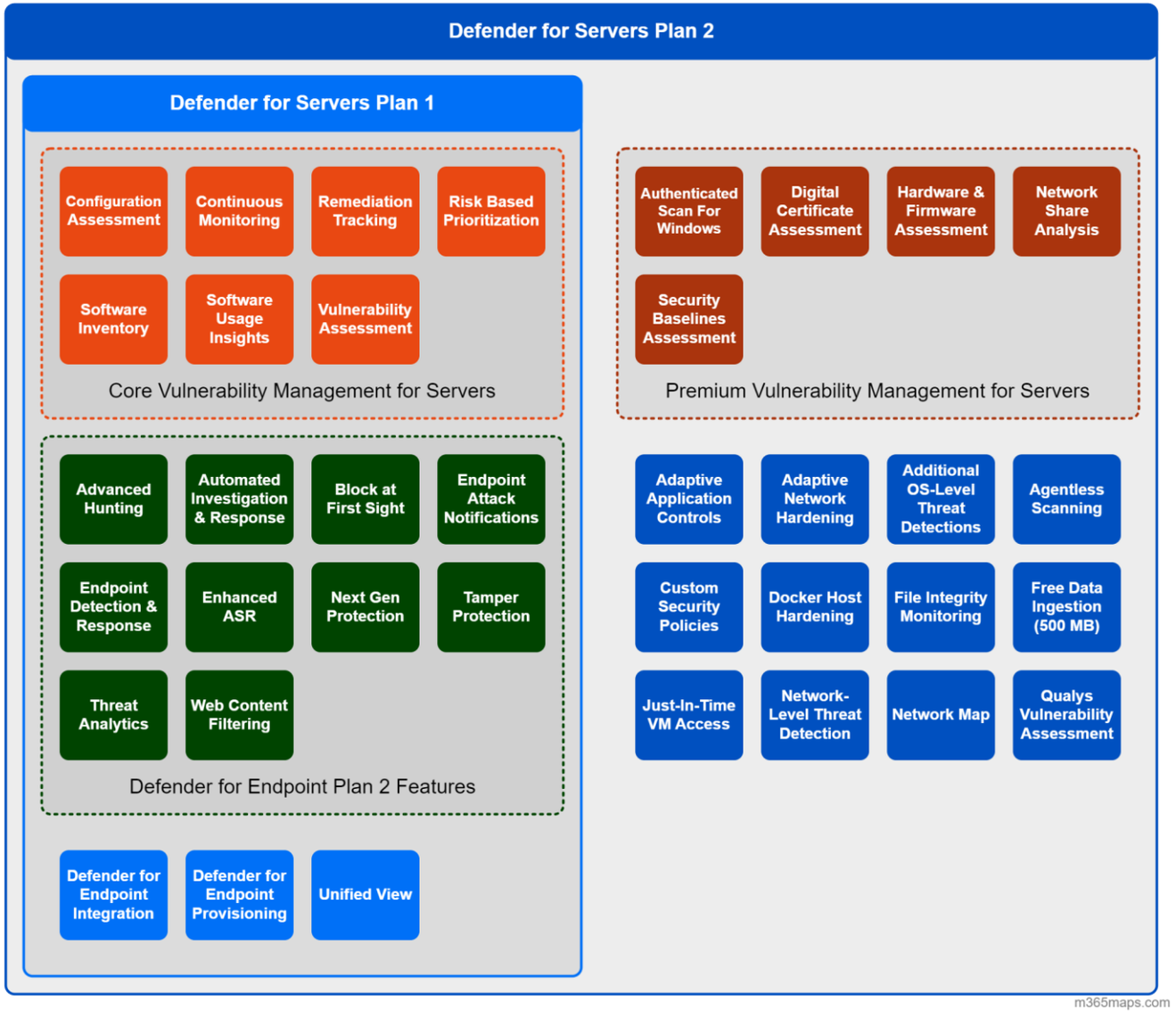
Key capabilities	MDVM capabilities included in foundational server protection (Defender for Servers P1 & Defender for Endpoint for servers)	MDVM add-on ($2) available to Defender for Endpoint for servers	MDVM capabilities included in Defender for Servers P2
Vulnerability assessment			
Configuration assessment			
Continuous monitoring			
Threat analytics and threat intelligence			
Risk-based prioritization			
Remediation tracking			
Consolidated asset inventories			
Discovery of unmanaged and managed devices			
Security baseline assessment			
Authenticated scans for vulnerability assessments			
Hardware and firmware assessment			
Digital certificates assessment			
Network shares analysis			
Block vulnerable applications			

Defender Vulnerability Management add-on SKU for Defender for Endpoint for Servers

Additional Resources

- Defender for Servers onboarding option without using Azure Arc (Note: Direct onboarding provides access to all Defender for Servers Plan 1 features. For Defender for Servers Plan 2, certain features still require the deployment of the Azure Monitor Agent with Azure Arc on non-Azure machines.)
  - **Current Limitations**
- Credit for purchased Defender for Endpoint for Servers licenses when moving to Defender for Servers
  - If you already have a license for Microsoft Defender for Endpoint for Servers, you won't have to pay for that part of your Microsoft Defender for Servers Plan 1 or 2 license.
- Cloud Optimisation
  - Usage based billing for Defender for Servers Plan 1, measured by hour, paid by the month ~ suited to dynamic workloads
  - Defender for Endpoint for Servers = annual billing

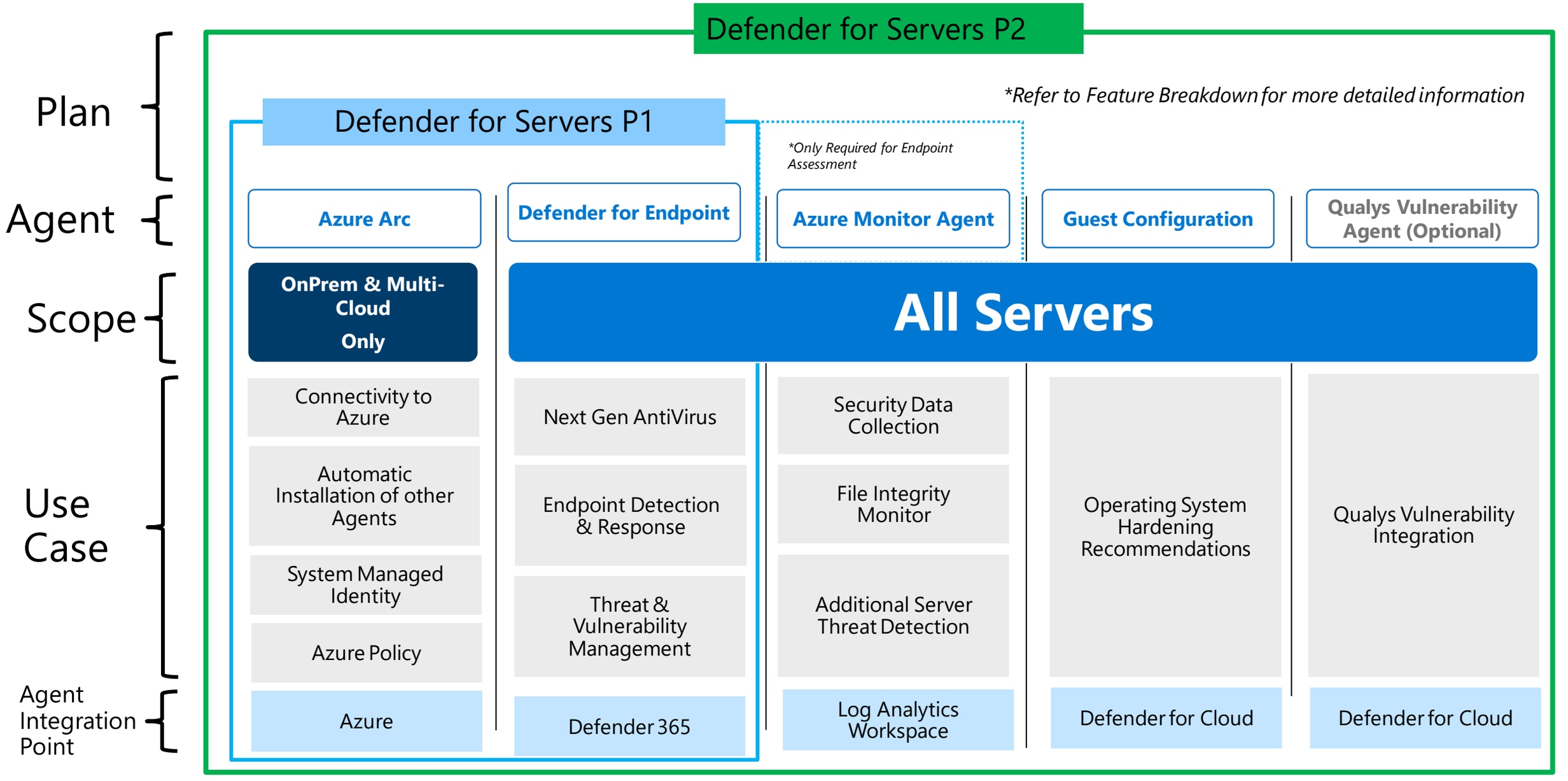
Another view – from m365maps.com



[Microsoft Defender for Servers | M365 Maps]

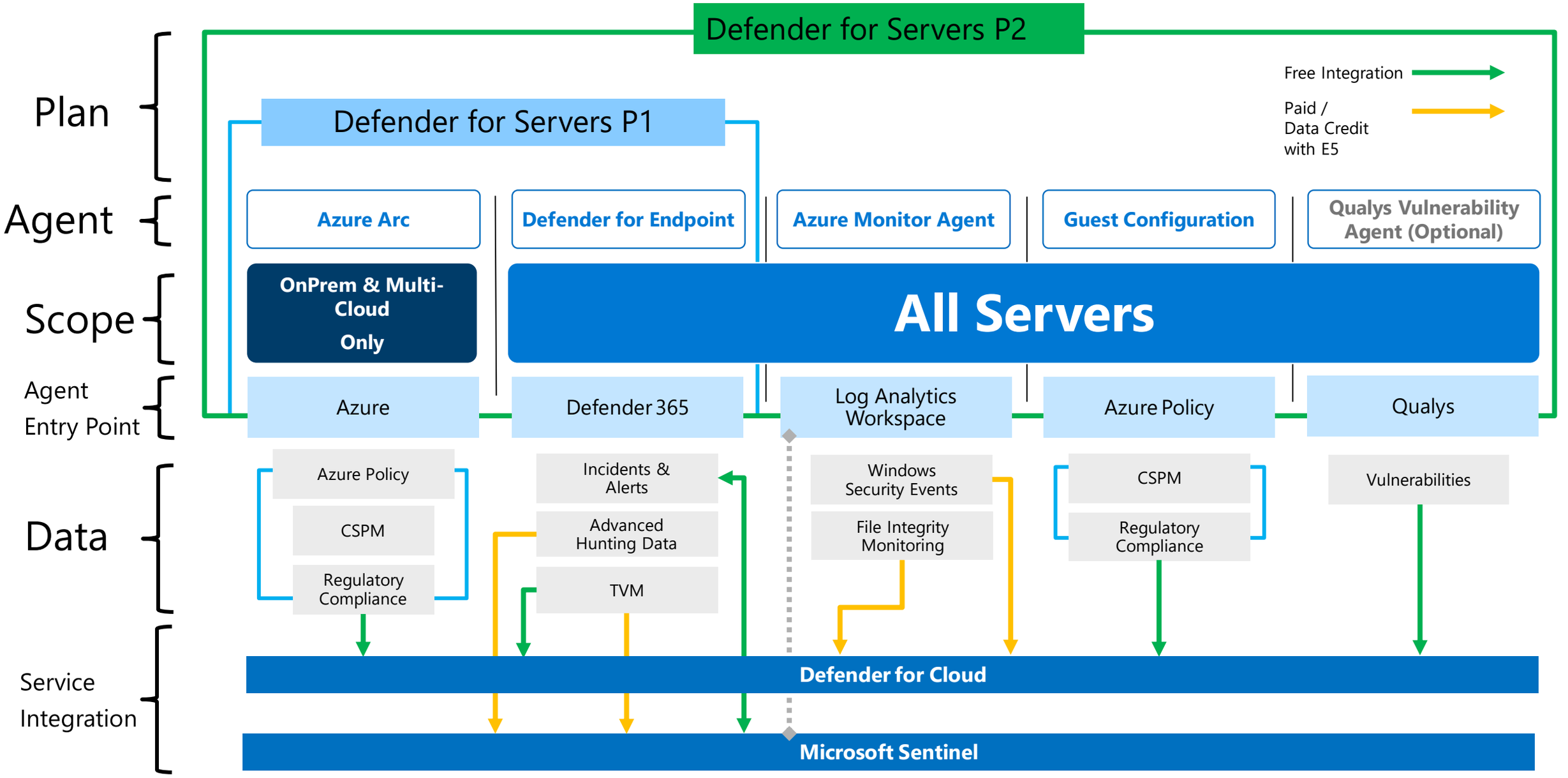
Defender for Servers Agents

High Level Breakdown



Defender for Servers Agents

Data Integration with Microsoft Security



Defender for Servers

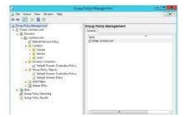
Management

Third Party System Management

puppet

Microsoft Intune

Group Policy Management



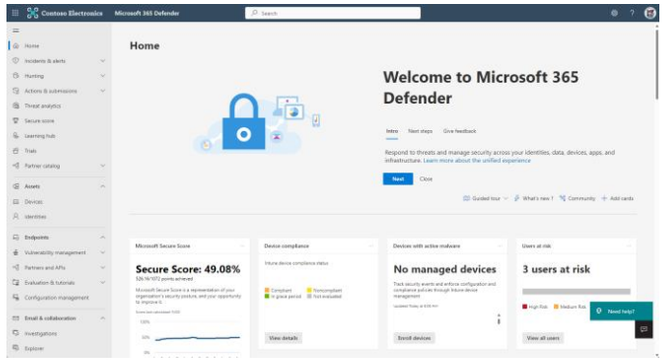
ANSIBLE

Microsoft System Center Configuration Manager

CHEF

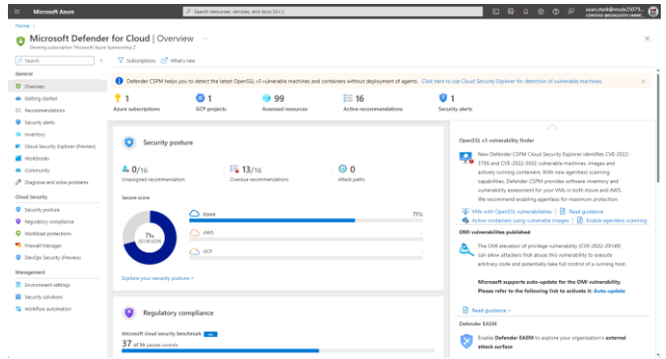
- Antivirus Exclusions
- Defender for Endpoint Settings
- Defender for Endpoint Updates

Defender 365 Portal
security.microsoft.com



- Incidents and Alerts
- Threat & Vulnerability Management
- Endpoint Detection & Response
- Deeper Investigation
- Advanced Hunting
- Threat Analytics
- Microsoft Secure Score

Defender for Cloud Portal
portal.azure.com



- File Integrity Monitoring
- Regulatory Compliance
- Microsoft Cloud Secure Score
- Security Recommendations
- Security Policy Enforcement

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



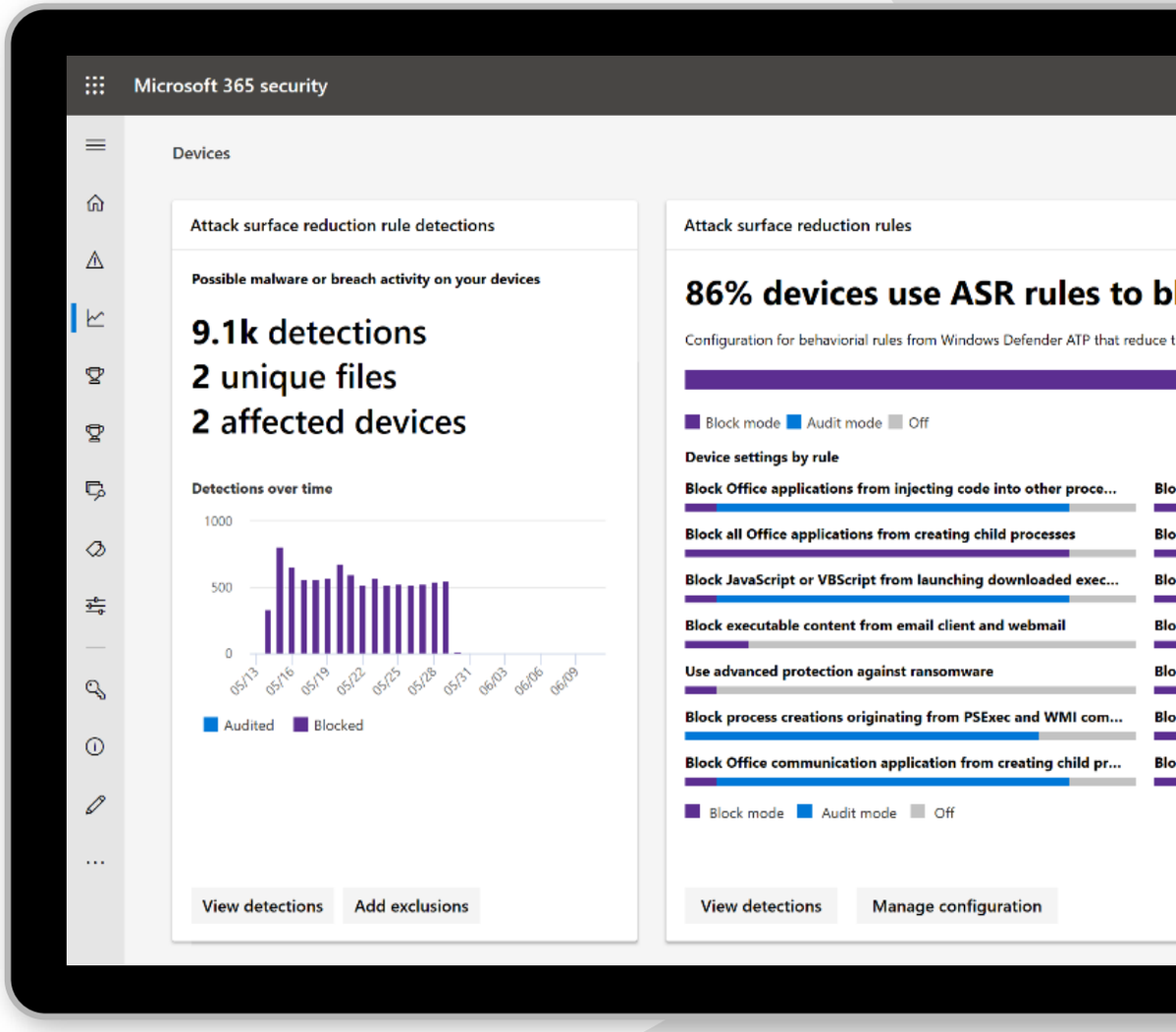


Attack surface reduction

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

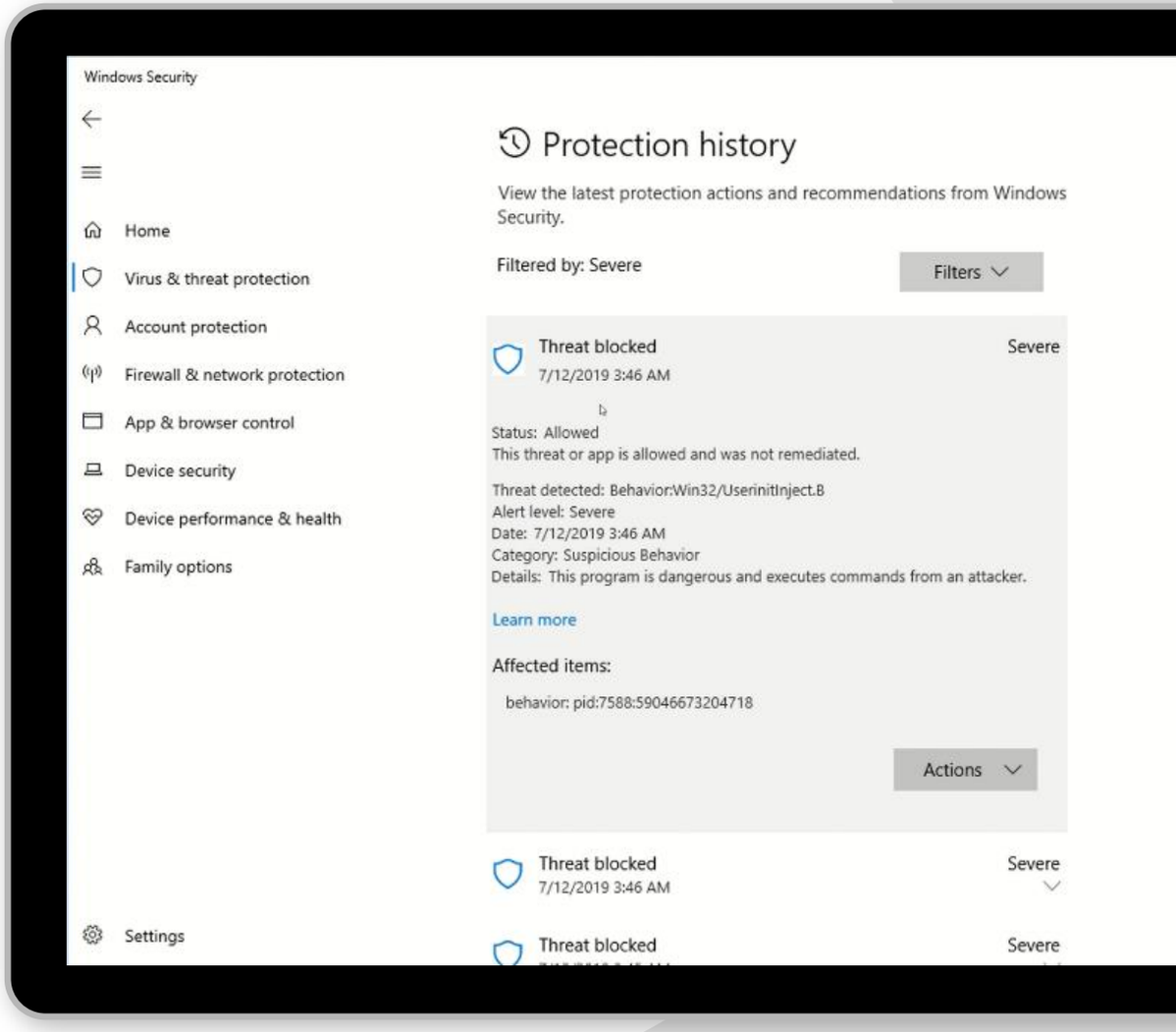


Next generation antivirus protection

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

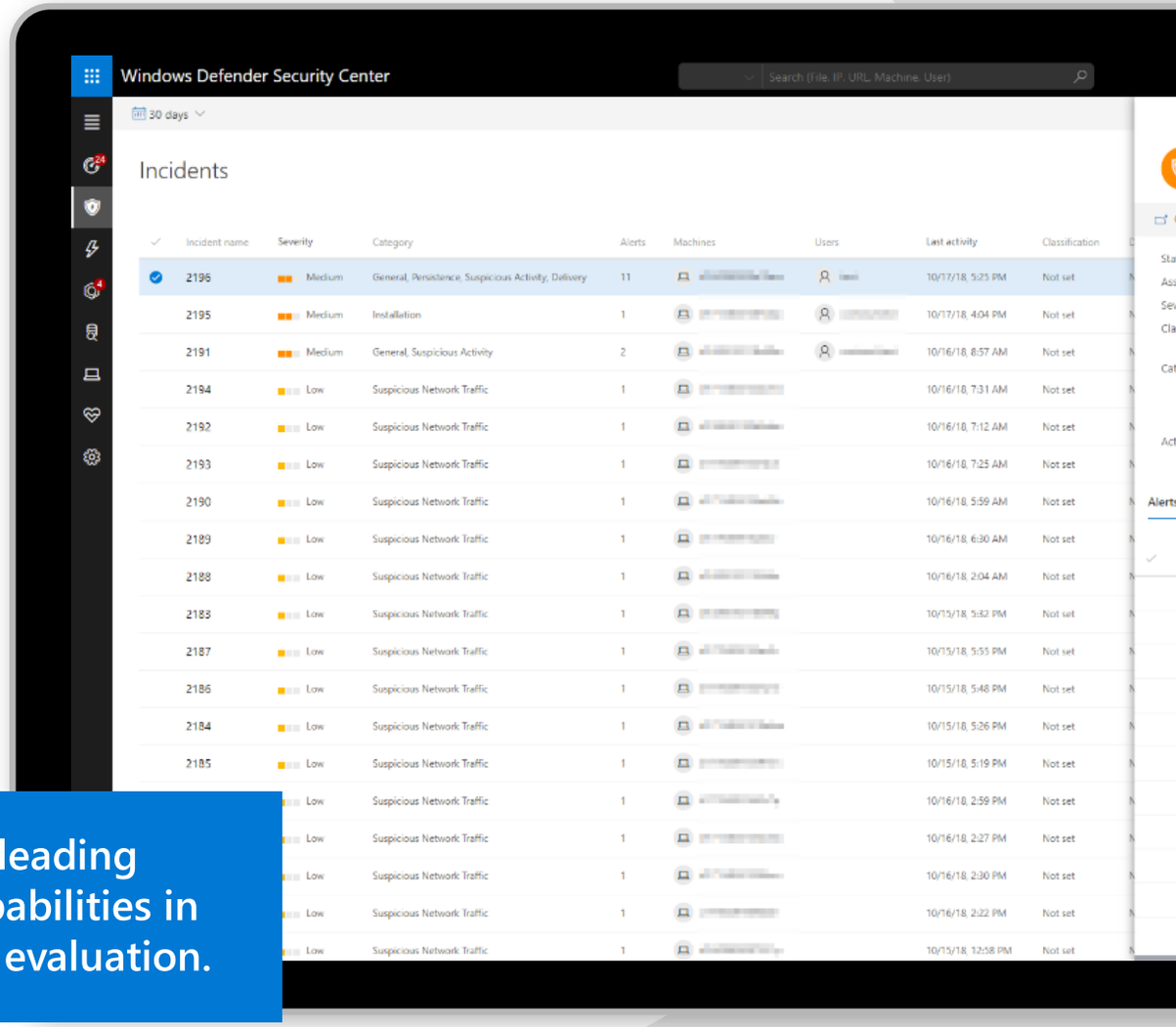


Endpoint detection & response

Powered by Microsoft Defender for Endpoint

Detect and investigate advanced persistent attacks

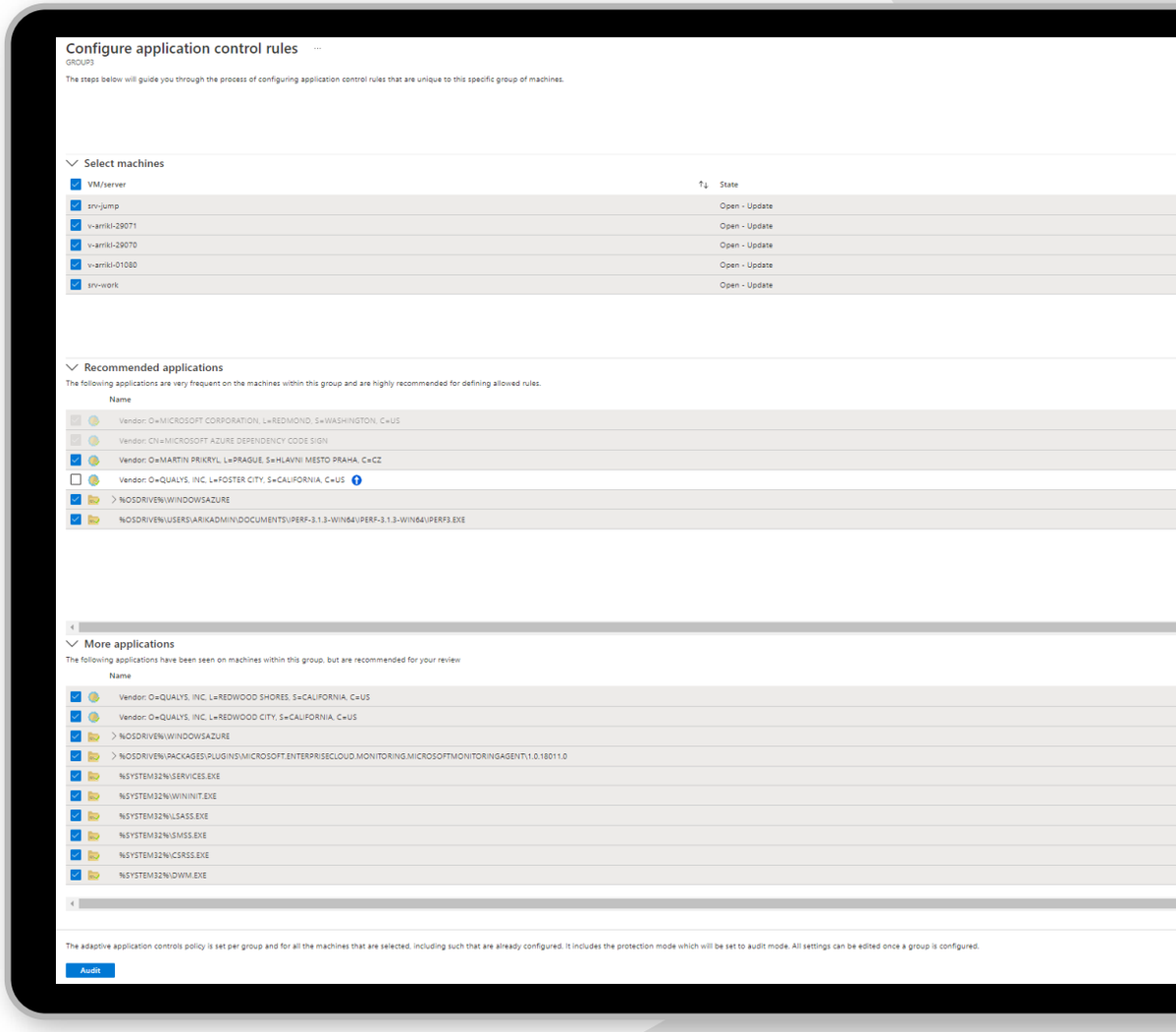
- Correlated behavioral alerts
- Investigation & hunting over six months of data
- Rich set of response actions



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

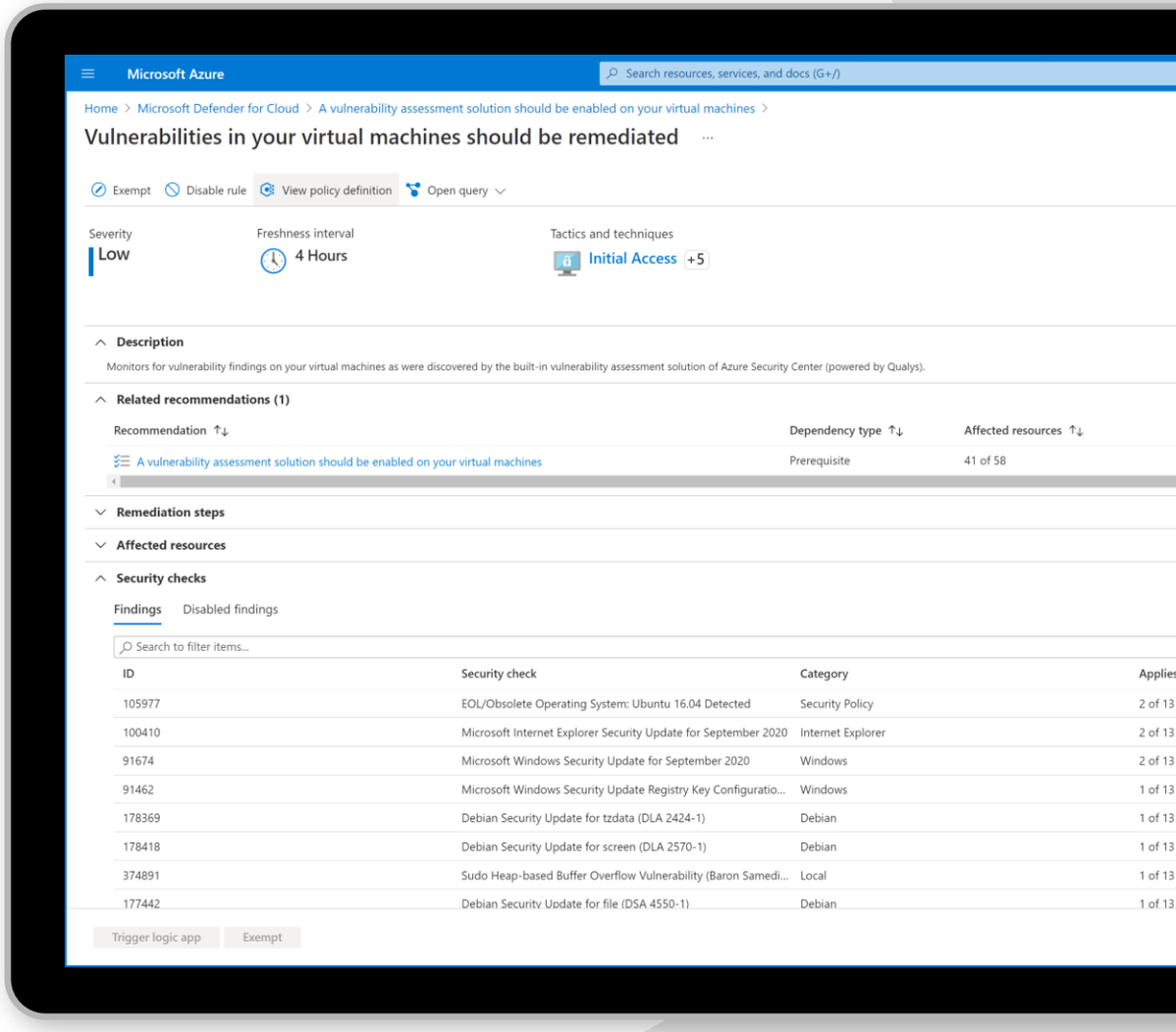
Adaptive application control

- Use intelligent and automated allow lists of known-safe applications for your machines to protect against malware, comply with organisational policies, and increase oversight of apps that access sensitive data



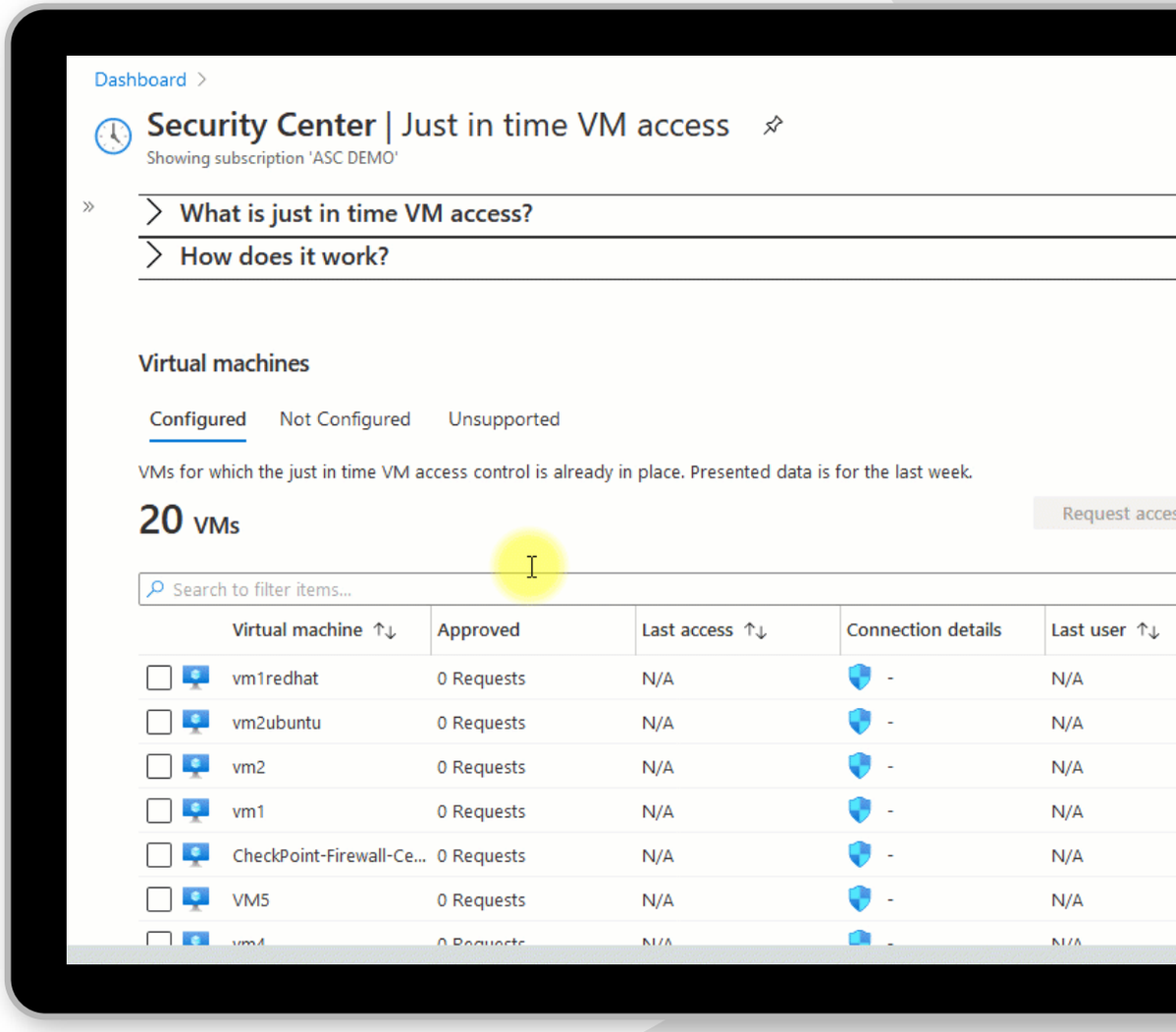
Assess your VMs and containers for vulnerabilities

- 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



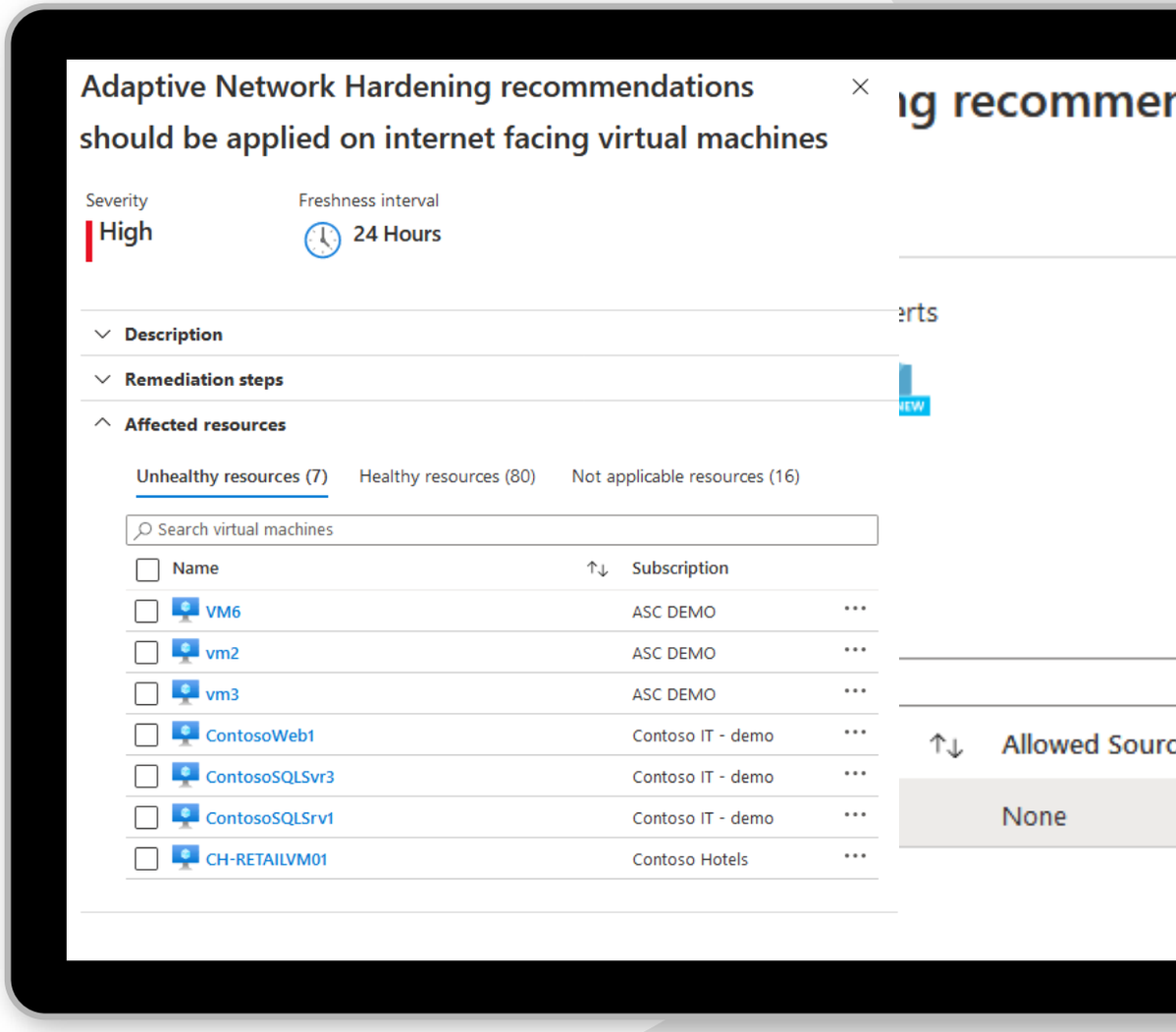
Just-in-time VM access

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



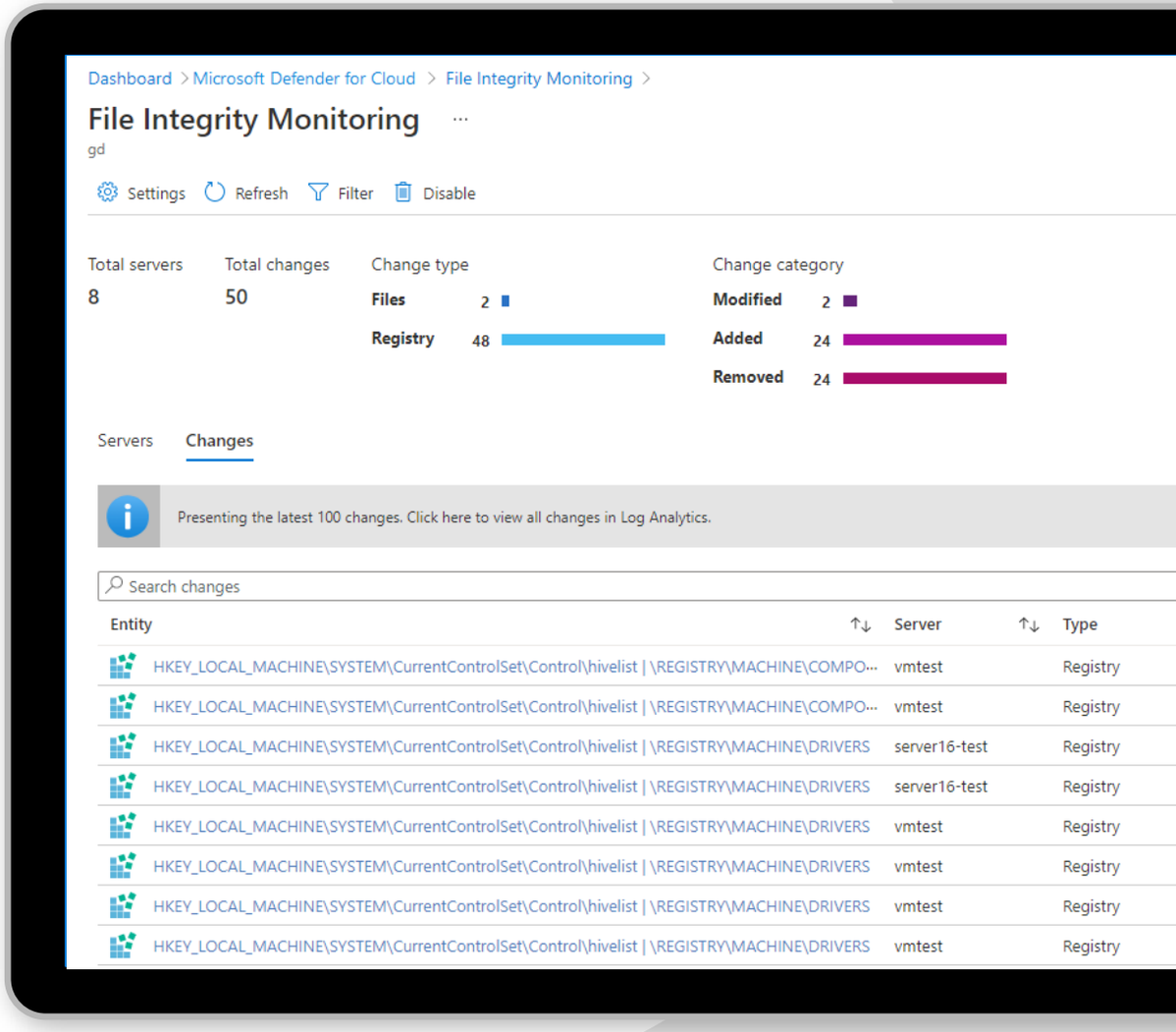
Adaptive network hardening

- Provides recommendations to further harden the NSG rules
- Uses machine learning that factors in actual traffic, known trusted configuration, threat intelligence, and other indicators of compromise



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



The Rise of Containers

Container adoption is booming

- The use of containers in production increased by **300%** between 2016 and 2021 [1]

  Kubernetes use in production has increased to **83%** [1]

Increase in number and sophistication of attacks targeting containers and Kubernetes

- **94%** orgs experienced at least one security incident in Kubernetes during 2021 [3]

  Attack volume continued to increase, growing by **26%** in 2020 [2]

Extra focus on shift-left

- Infamous cases: SolarWinds, Log4j

  Supply chain risks is one of the common sources of compromise in Kubernetes [4]

[1] CNCF 2020 Container Adoption Survey
[2] Cloud Native Threat Report: Attacks in the wild on the Container Supply Chain and Infrastructure
[3] State of Kubernetes Security Report 2021
[4] Kubernetes Hardening Guidance - Cybersecurity Technical Repot by the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA)

Microsoft Security

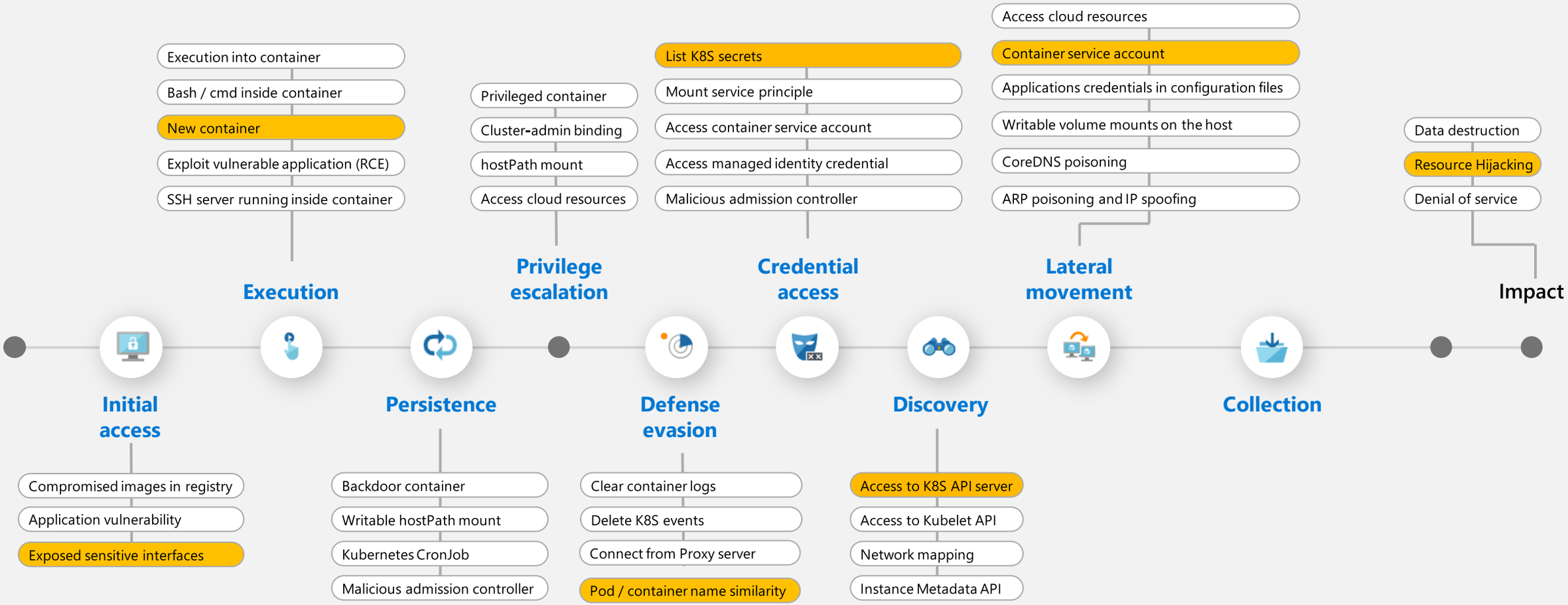
Container security is different

- Containerized applications are elastic, spawn and re-size rapidly.
- Images are immutable , containers are short lived.
- Visibility of containers traffic flows are difficult to track with traditional tools.
- Runtime environment is complex, with different configuration layers and options.

The goal: assuring that container environment is running as intended, including protection of infrastructure, software supply chain, runtime, and everything between.

Threat detections aligned to the K8s Attack Matrix

[How ATT&CK for Containers was built](#) ; [Secure containerized environments with threat matrix for Kubernetes](#)



Microsoft Security

Microsoft Defender for Containers

Protect multi-cloud and hybrid container deployments

Hardening

Continuously assess and improve the security posture of your containerized environments and workloads.

Agentless Vulnerability management

Reduce your attack surface by continuously scanning workloads to identify and manage container vulnerabilities.

Advanced threat detection

Identify runtime threats with prioritized, container-specific alerts – using powerful insights from Microsoft Threat Intelligence.

Multi-cloud support

Single container security solution for Kubernetes clusters, across Azure, AWS, GCP and on-premise.

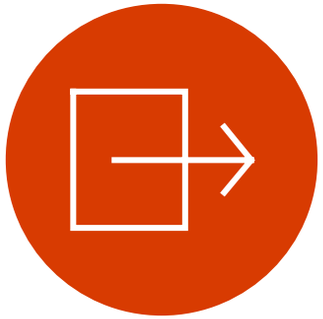
Deployment and monitoring

Frictionless deployment provisioning at scale with easy onboarding and support for standard Kubernetes monitoring tools.

Top concerns in cloud storage

Malware upload

Storage is an **entry point** and a **distribution point** into the organization.



Data exfiltration

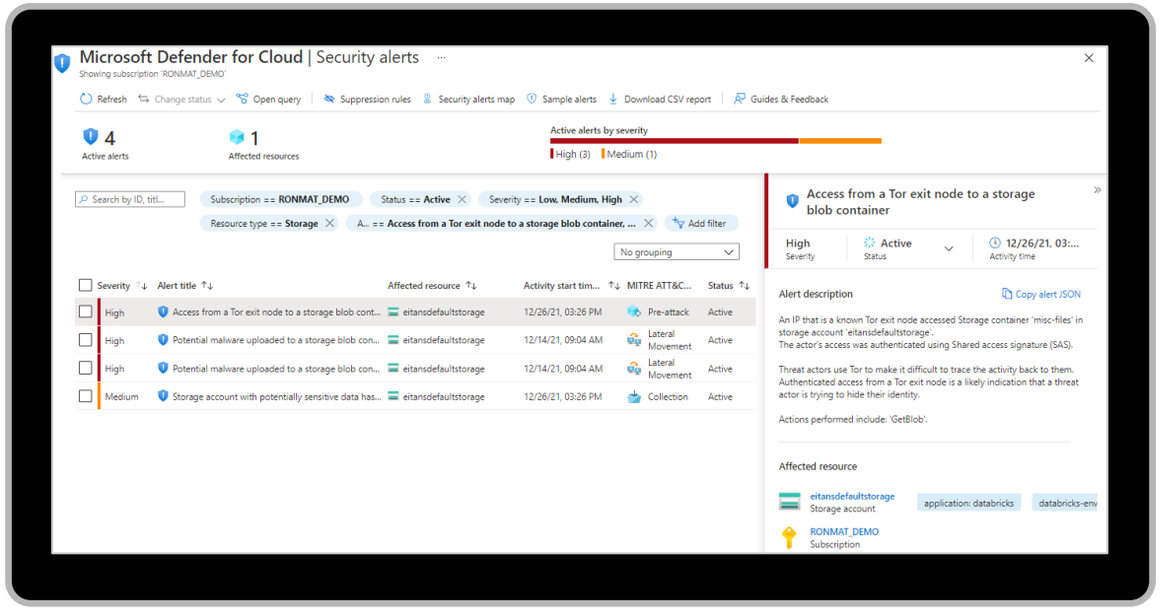
Storage is a **sensitive data treasure chest.**

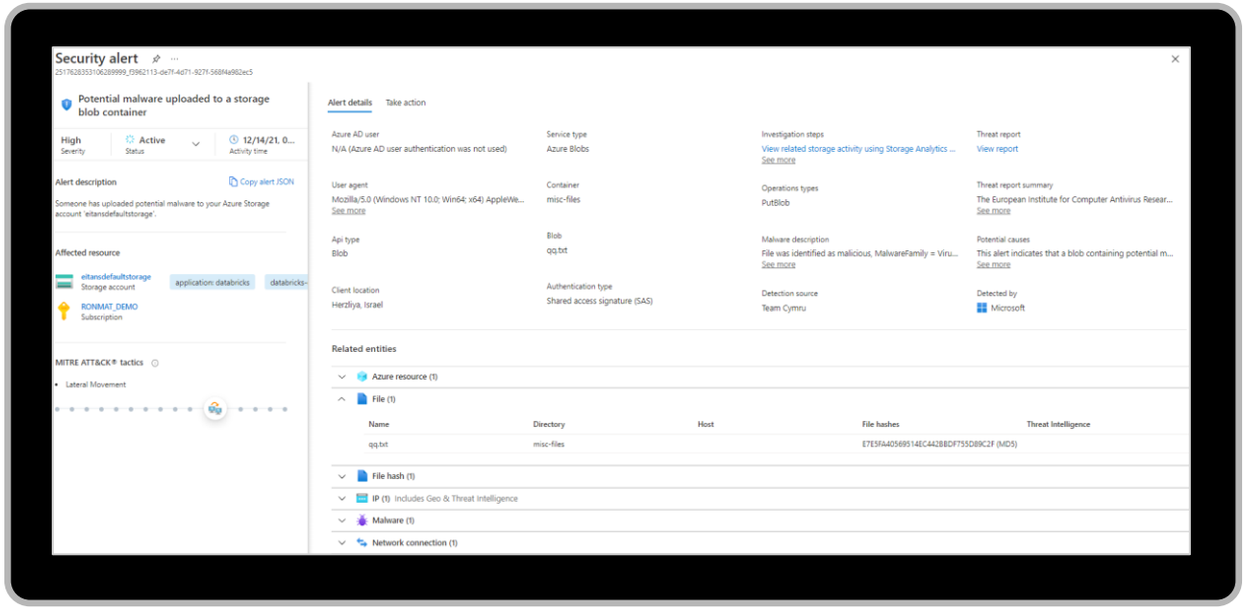
Cloud ransomware

Malicious actors can use infrastructure tools to **encrypt and delete data** inside the storage account.

What is Microsoft Defender for Storage

A native threat protection for blobs containers, file shares and data lakes in Azure





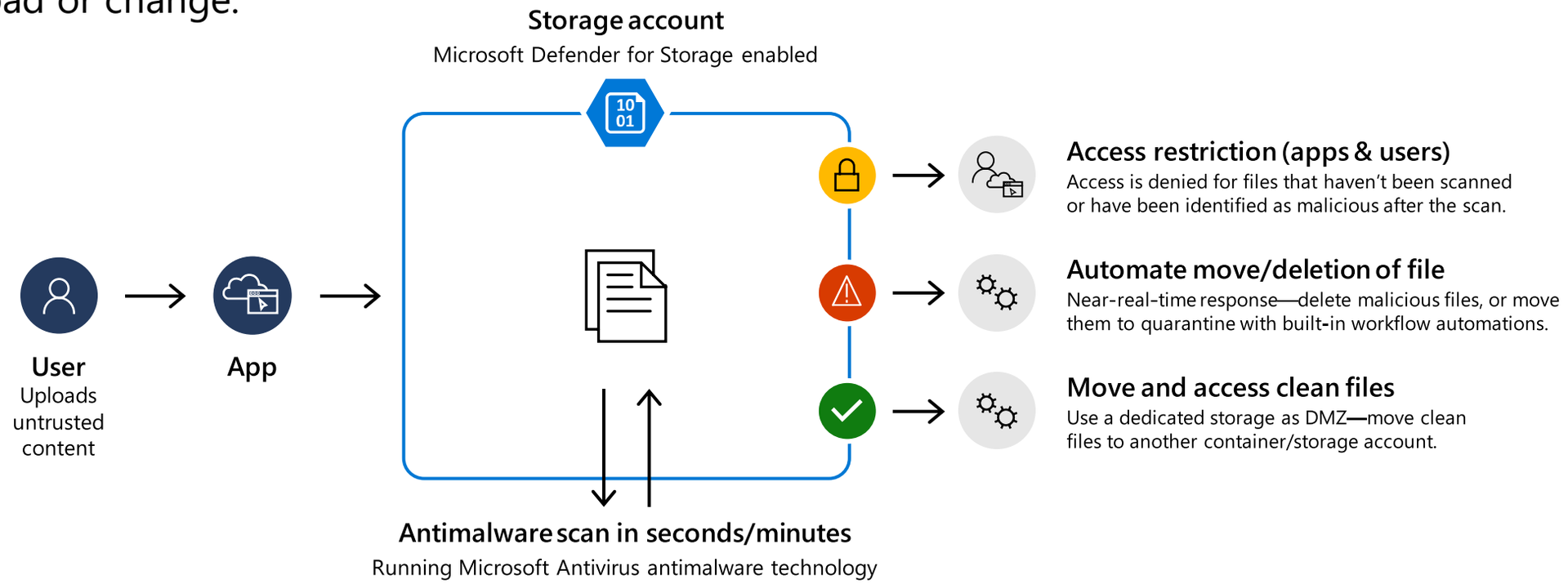
- Provides an **advanced layer of security** to better protect storage workloads.
- Provides **contextual alerts** upon unusual and potentially harmful attempts to breach storage workloads.
- Provides **recommendations** to help harden the security posture of storage environment.
- Powered by **Microsoft advanced technologies** including it's unique Threat Intelligence capabilities.

Microsoft Security

Antimalware scanning for storage

Microsoft Security

Protect your storage estate from malware distribution and help meet compliance requirements using built-in near real time antimalware scanning at scale. Initially this offering will be available for Azure Blob Storage for upon upload or change.



Detect

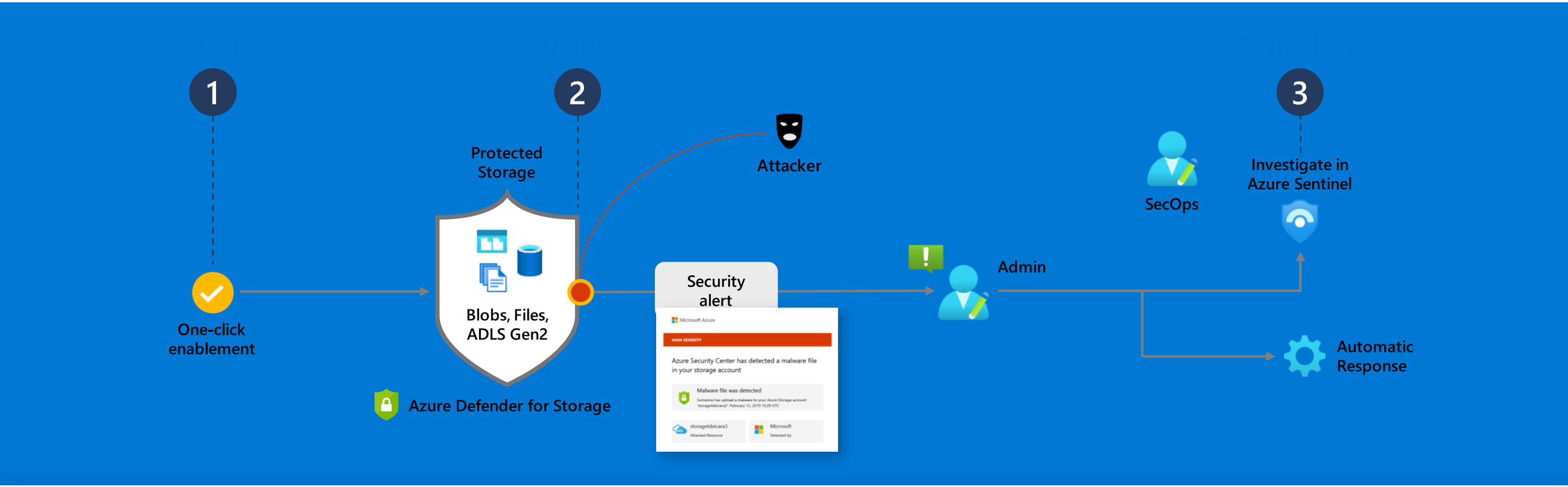
- Near-real-time scan on upload.
- Full antimalware scan.
- Periodic scans with continuously updated malware signatures.

Respond

- Near-real-time response options.
- Strict access restriction.
- Seamless integration with Microsoft Sentinel for incident investigation and remediation.

Microsoft Defender for Storage

Protect blobs containers, file shares and data lakes in Azure



Azure Native Security

Built-in within Azure with **1-click enablement.** Protect Azure Blob, Azure Files and Data Lakes

Rich Detection Suite

Covering top Storage threats – unauthenticated access, compromised credentials, malicious content etc powered by Microsoft Threat Intelligence

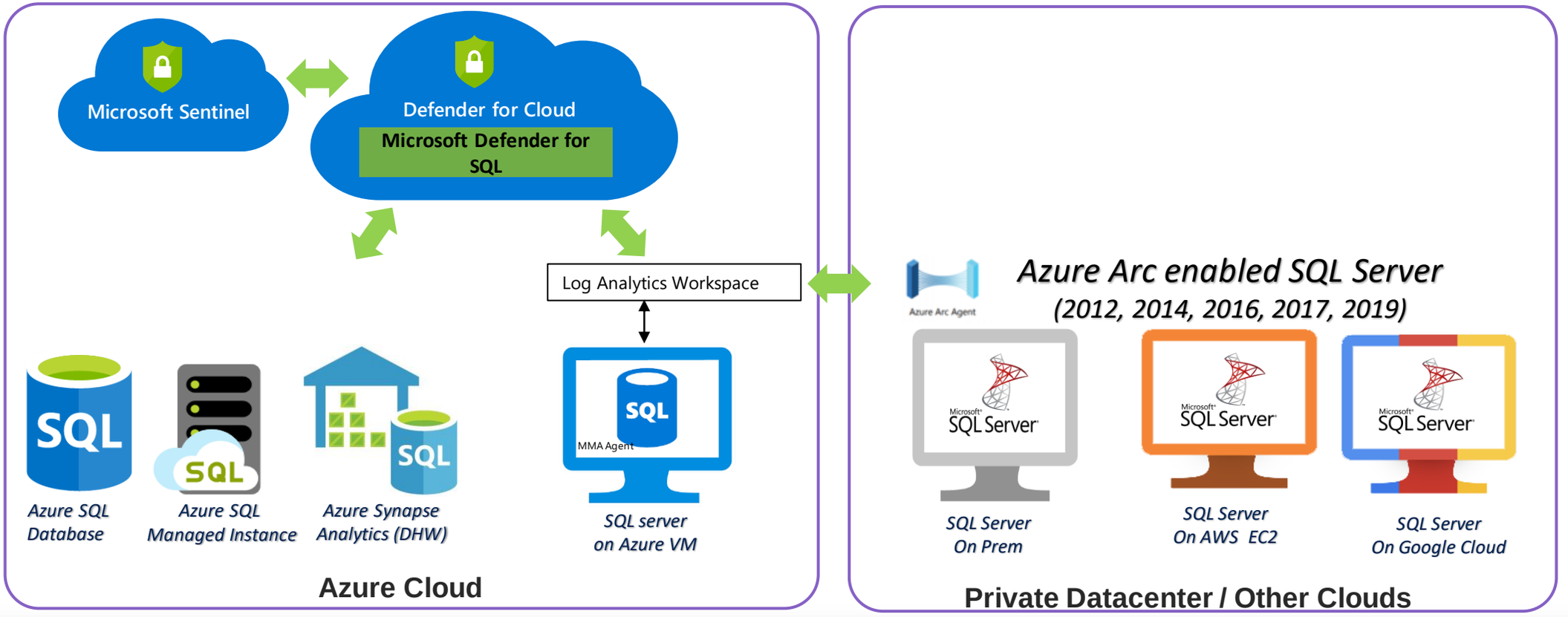
Response at scale

Reduce frictions preventing and responding to top threats – automation tools available

Centralized & Integrated

Centralize security across all data assets managed by Azure and built-in integration with Azure Sentinel & Azure Purview

Microsoft Defender for SQL

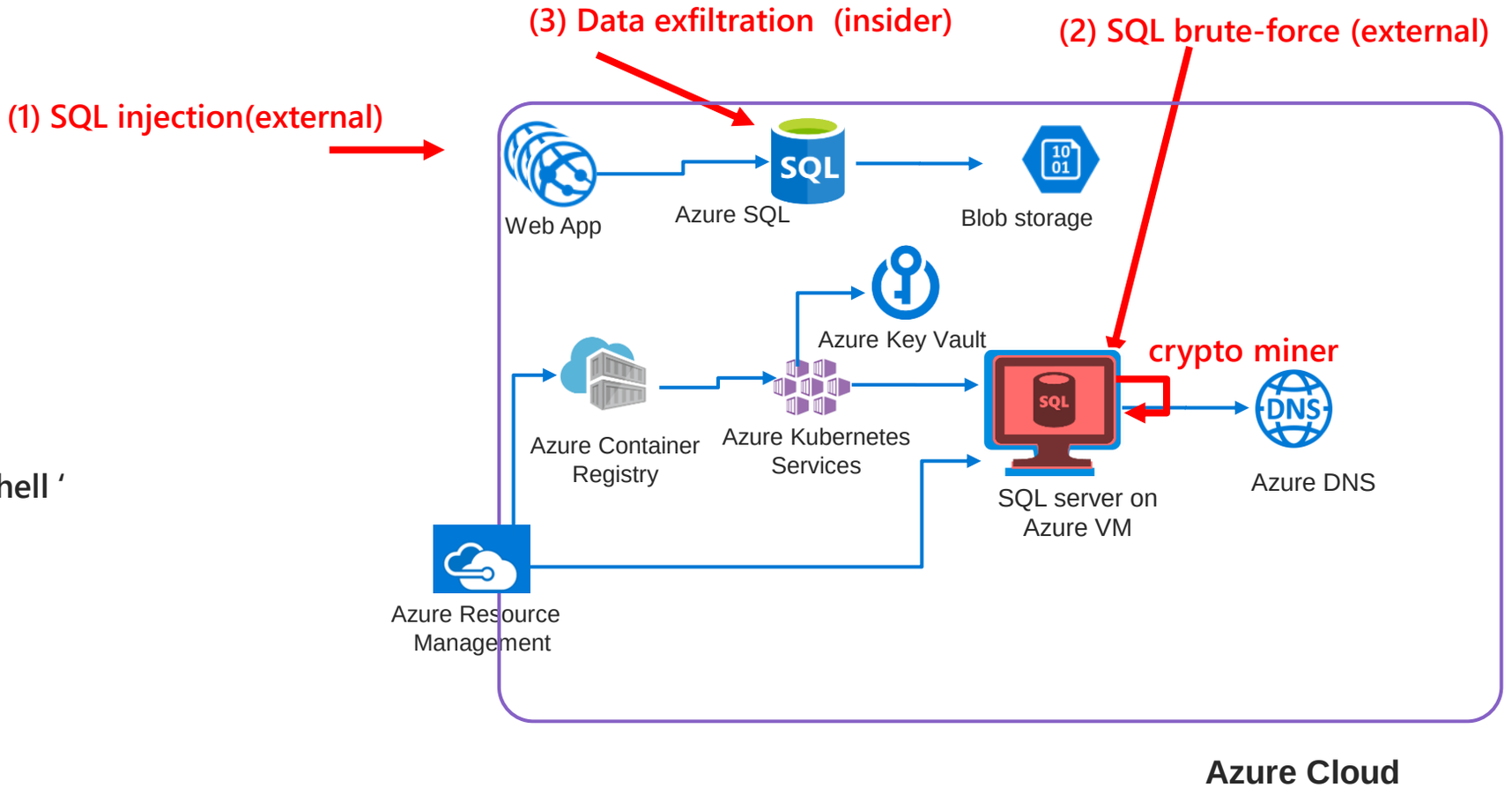


Advanced Threat Protection : detect unusual and harmful attempts to breach SQL servers across hybrid estate

Vulnerability Assessment : discover and remediate security misconfigurations, database vulnerabilities in SQL servers

Use case scenarios

- Recommends to disable 'sa' login
- Recommends to disable 'xp_cmdshell '
- Detects potential SQL Injection
- Detects SQL brute force
- Detects crypto miner in a VM
- Detects potential data exfiltration



For more information about the SQL brute force automation, visit https://aka.ms/BlockBruteforceAttack

Microsoft Security

Protect SQL workloads anywhere

Defender for SQL PaaS

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

Defender for SQL IaaS

- SQL Server on-prem
- Azure Arc enabled SQL Server
- SQL Server on Azure VM
- SQL Server on any other cloud

Defender for OSS DB

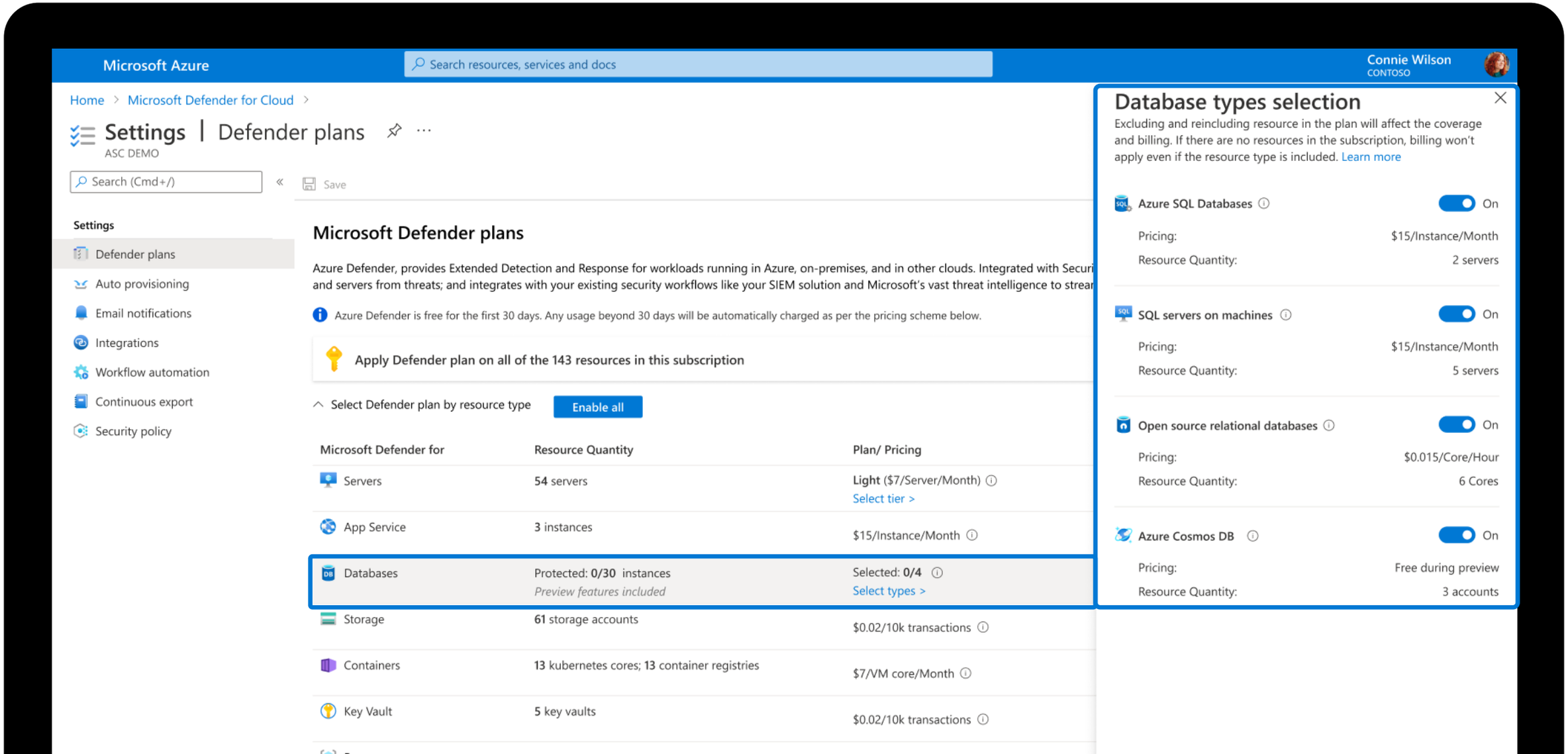
- Azure Database for MariaDB
- Azure Database for MySQL
- Azure Database for PostgreSQL

Defender for Azure Cosmos DB

- Azure Cosmos DB

Microsoft Security

Enable: One-click experience to protect your database estate



Detect: database-focused threat detections powered by Microsoft Threat Intelligence

Query analysis

- Potential SQL Injection
- Vulnerability to SQL Injection
- Anomalous amount of data extraction
- Anomalous destination of data extraction

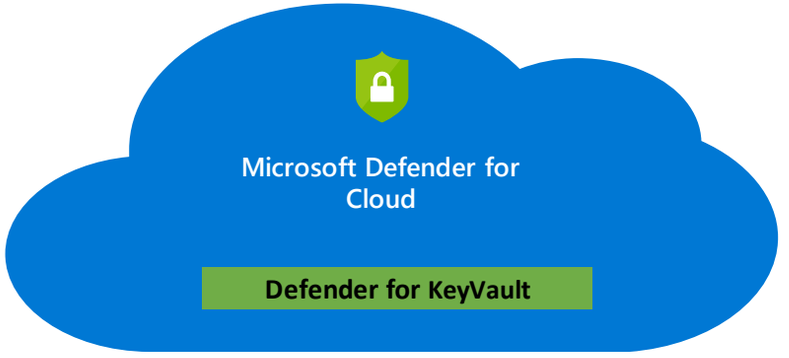
Threat intelligence

- Access from an unusual location
- Access from a suspicious IP
- Data center anomaly
- Principal anomaly
- Domain anomaly
- Suspicious app

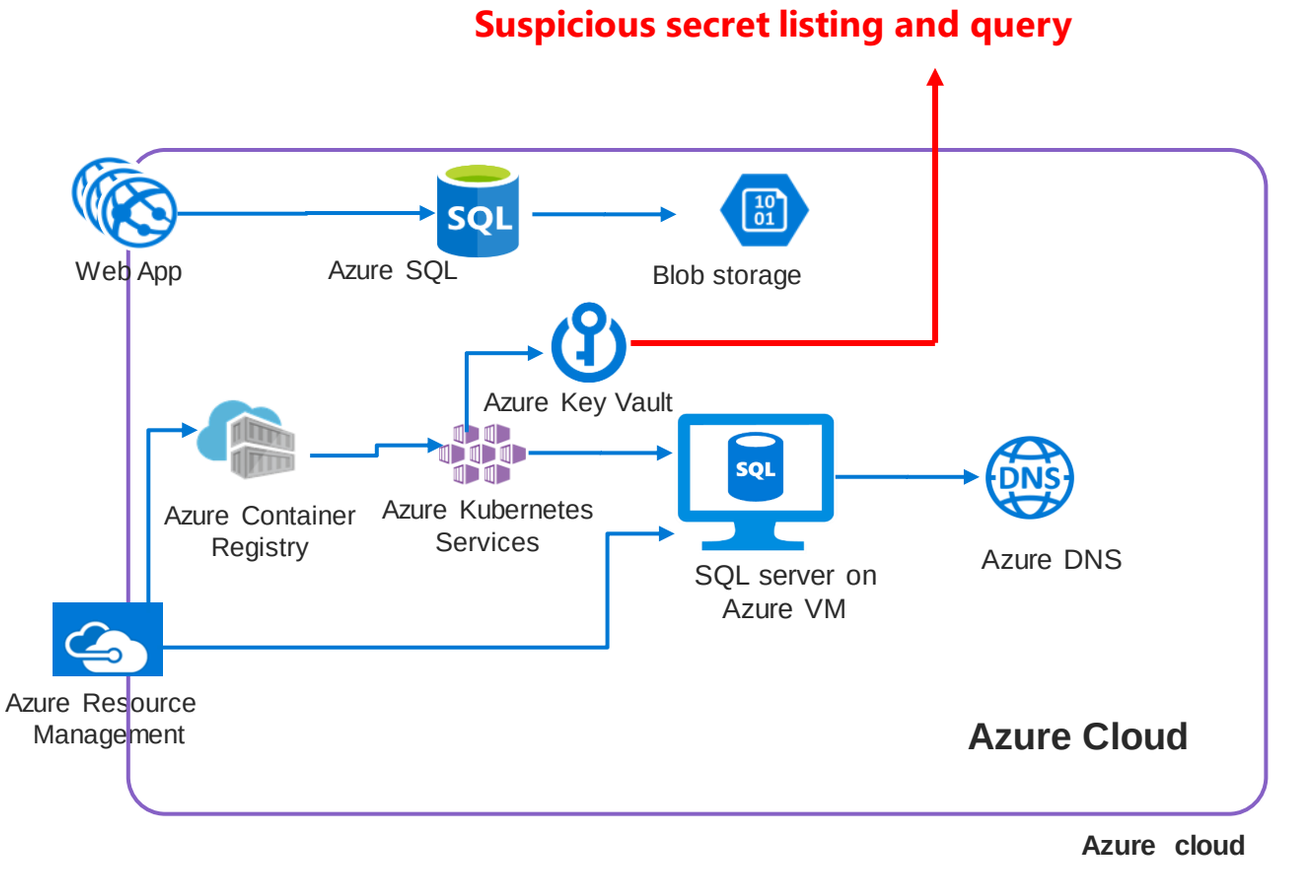
Brute force

- Potential brute force
- Potential brute force on a valid user
- Potential successful brute force

Defender for Key Vault

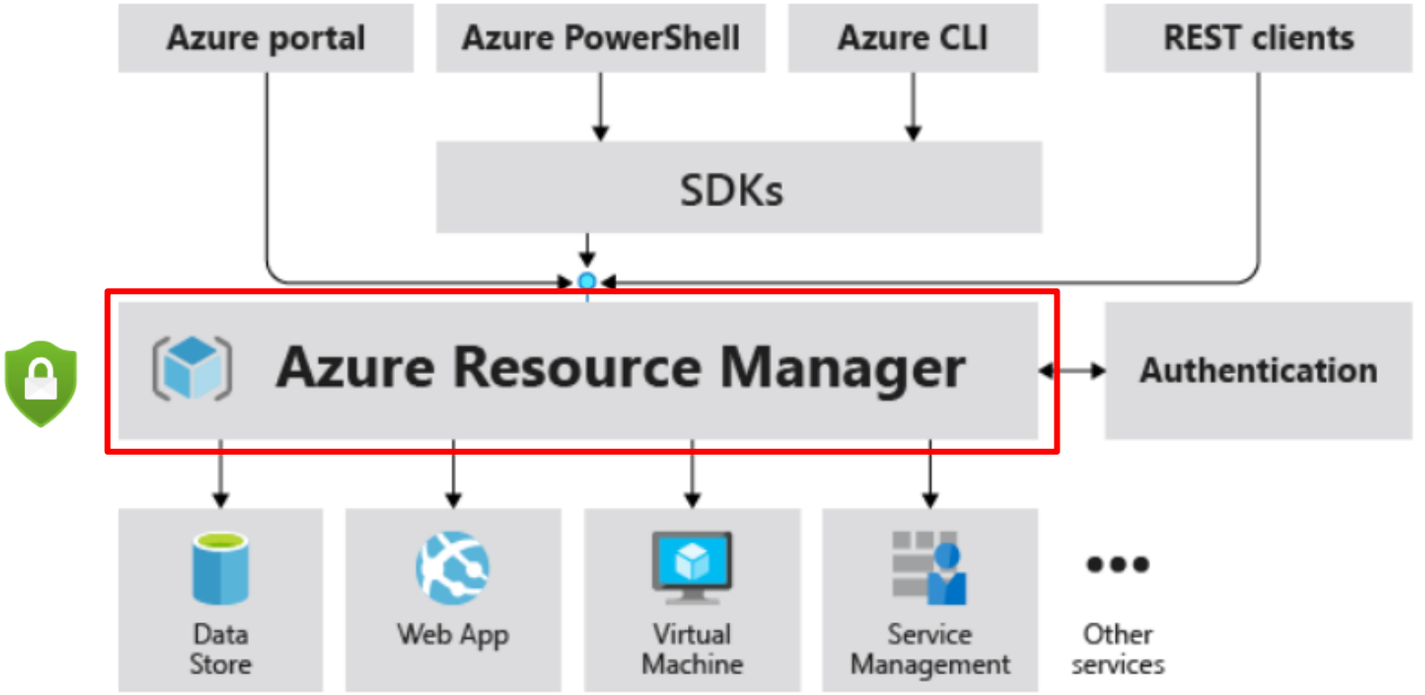


- Detects user accessed high volume of key vaults
- Detects access from a TOR exit node to a key vault
- Detects suspicious policy change and secret query in a key vault
- Detects unusual user accessed a key vault



Microsoft Defender for Azure Resource Manager (ARM)

- Protection against malicious usage of Azure Resource Management Layer (Portal, Rest, API, PowerShell)
- Protect against credential theft, permissions abuse, malicious insider

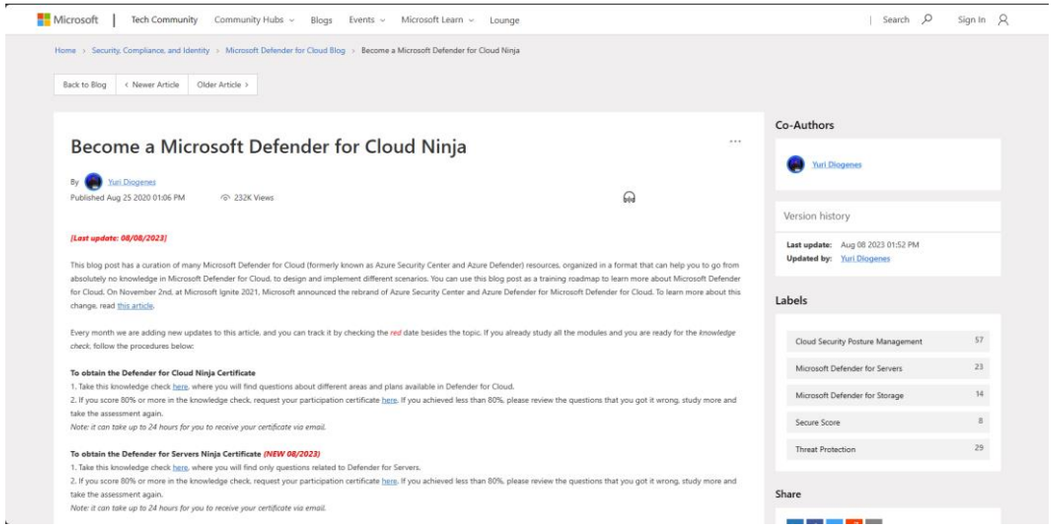


Wrap-up

Further Training Resources

Defender Ninja Training

- Microsoft Defender for Cloud : http://aka.ms/ascninja
- Microsoft Defender for IoT: https://aka.ms/d4iotninja
- External Attack Surface Mgmt (EASM) : EASM Level 400 training



- Exam SC-900: https://learn.microsoft.com/en-us/certifications/exams/sc-900
- Exam SC-200: https://learn.microsoft.com/en-us/certifications/exams/sc-200

Some Links

Defender on Servers

- Server Deployment

  Plan a Defender for Servers deployment to protect on-premises and multicloud servers | Microsoft Learn
- Airgapped Networks Configure device proxy and Internet connection settings | Microsoft Learn
- (Old) Protecting disconnected devices with Microsoft Defender ATP - Microsoft Community Hub & Whitepaper (PDF)

- Blog Posts – MDE & Proxies Part 2 Part 3
- MDE URLs https://aka.ms/MDEURL
- MDE Deployment Status workbook https://aka.ms/MDEStatus
- Advanced Deployment guidelines for MDE on Linux https://learn.microsoft.com/en-us/microsoft-365/security/defender-endpoint/comprehensive-guidance-on-linux-deployment

Microsoft Security

Thank you.