

# 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	<ul style="list-style-type: none"><li>Defender for Server Plan 1 &amp; Plan 2</li></ul>
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

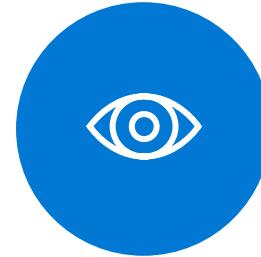
# Securing multicloud environments

Top-of-mind



Develop and operate  
secure apps in the cloud

**>54%**  
of enterprises do not  
integrate security into  
DevOps pipelines.<sup>1</sup>



Visibility into security  
and compliance

**86%**  
of surveyed security decision  
makers believe their cybersecurity  
strategy doesn't keep up with  
their multicloud environments.<sup>2</sup>



Protect against increasing,  
sophisticated attacks

**\$4.24M**  
is the average cost  
of a breach, 2021.<sup>3</sup>

1. Microsoft Enterprise DevOps Report

2. Microsoft Cloud Security Priorities and Practices Research

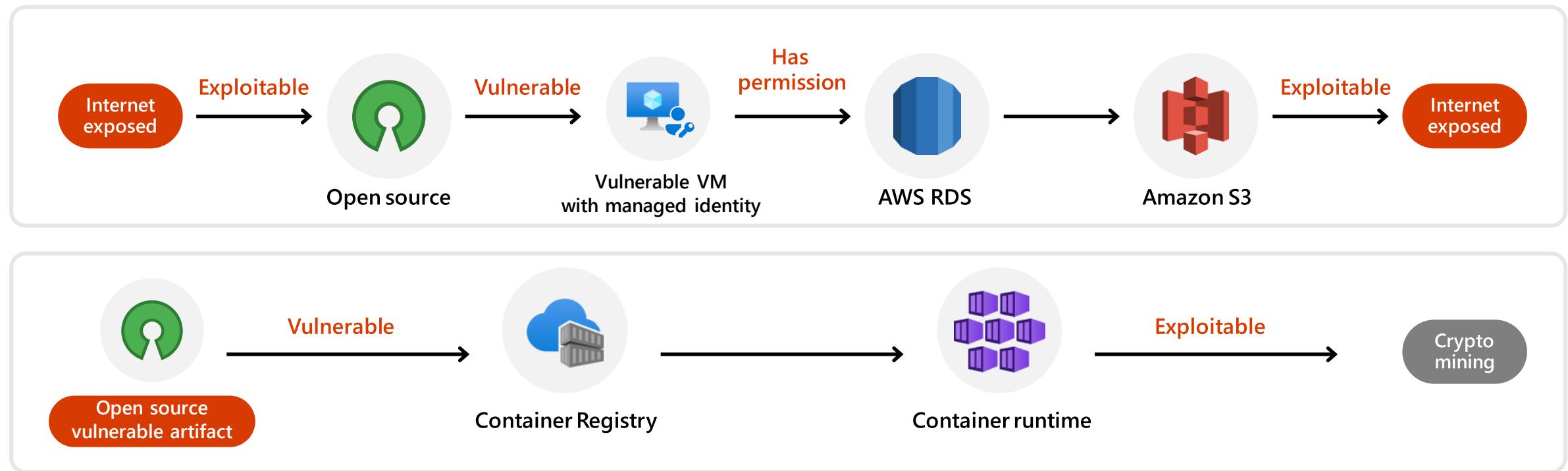
3. Ponemon Institute, Cost of a Breach Report

# 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

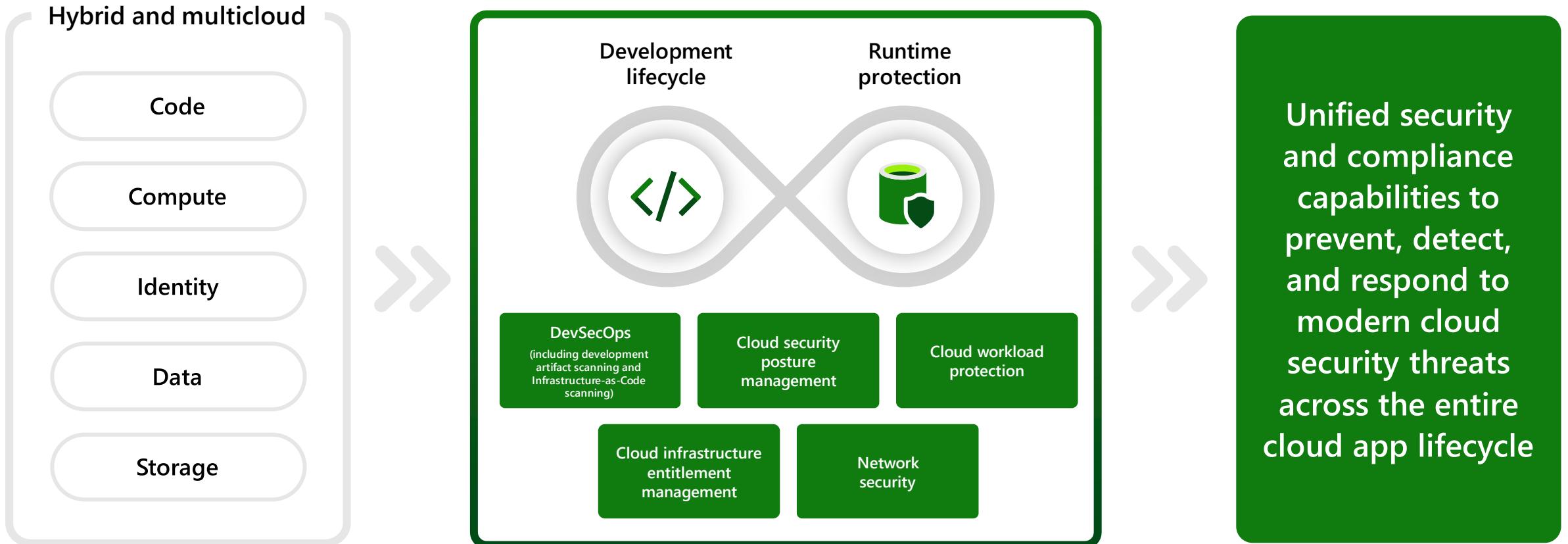
## Cloud infrastructure entitlement management

## Network security

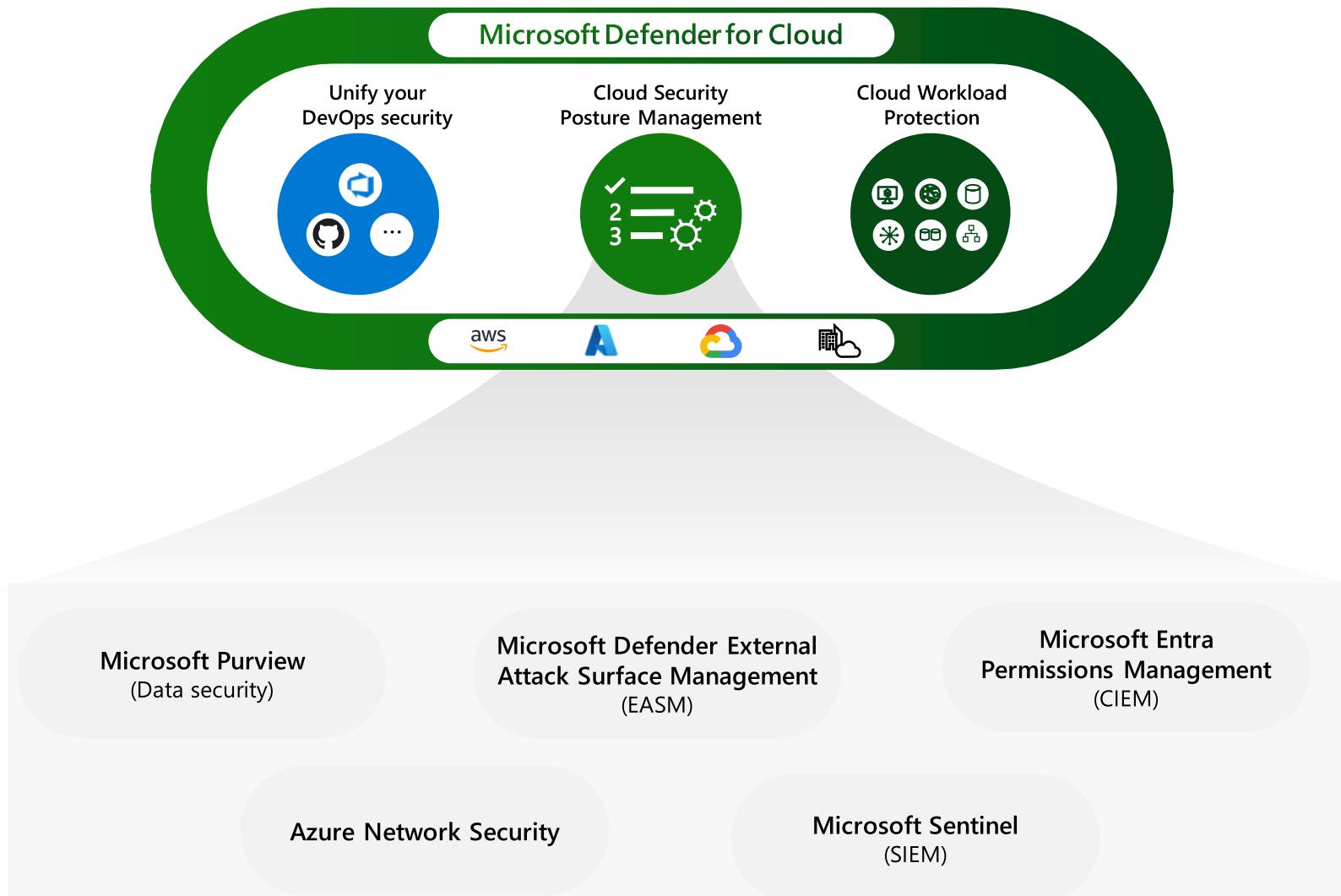
# Microsoft's cloud-native application protection platform (CNAPP)

Get integrated protection for your multicloud resources, app, and data.

Named by Gartner as a representative CNAPP provider.

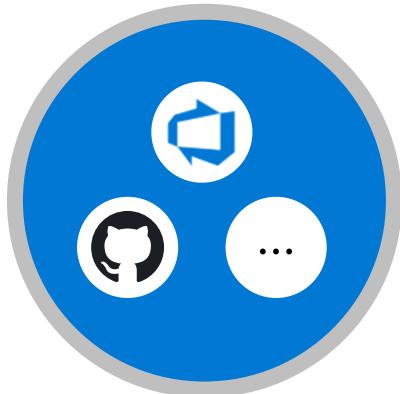


# Access CNAPP capabilities in Microsoft Defender for Cloud



# Microsoft Defender for Cloud

Unify your DevOps  
Security Management



Strengthen and manage your  
cloud security posture



Protect your cloud  
workloads



# 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



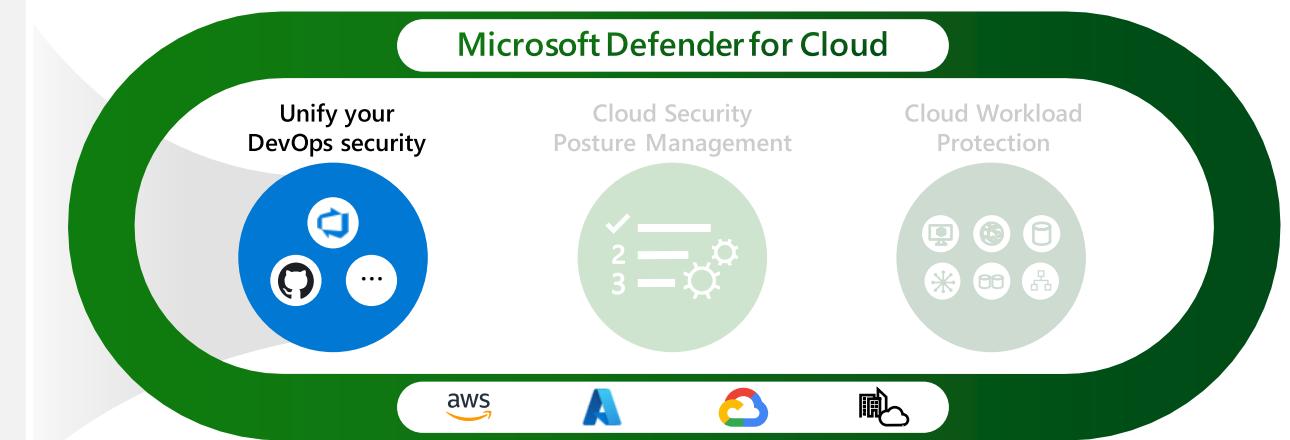
## Code-to-cloud contextualization

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



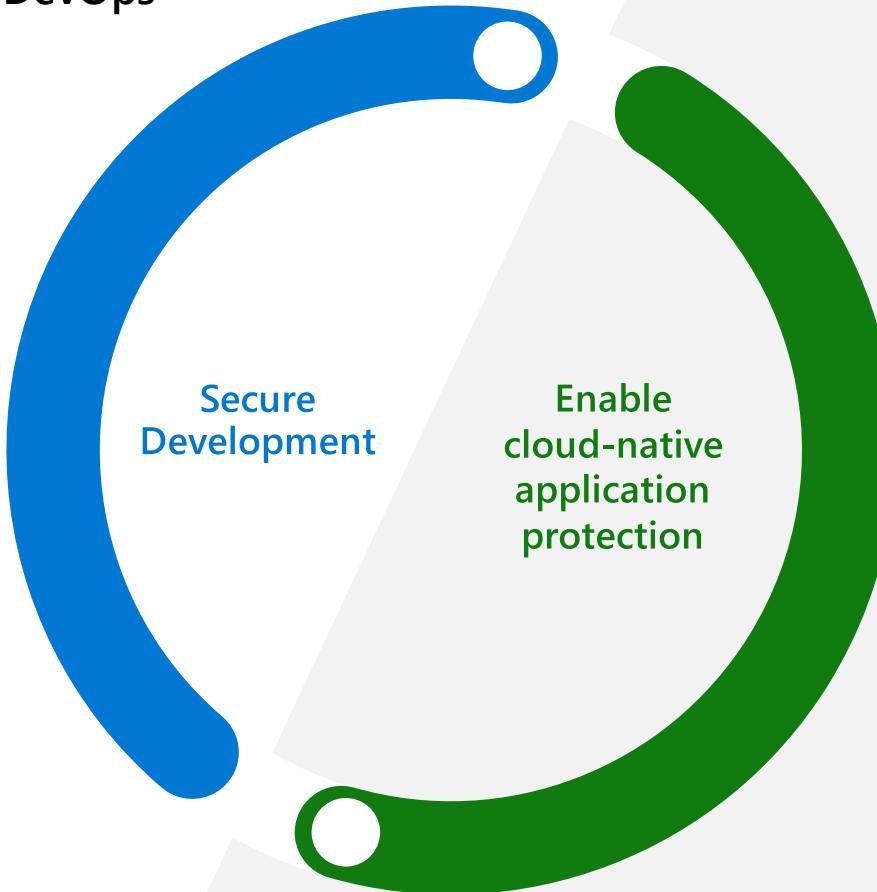
Dependencies security



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



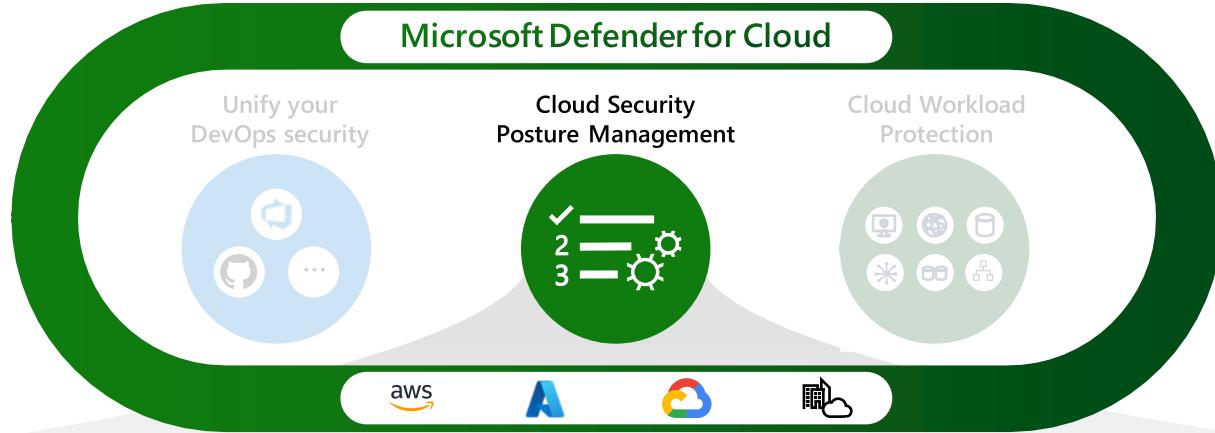
Automated workflows



# 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



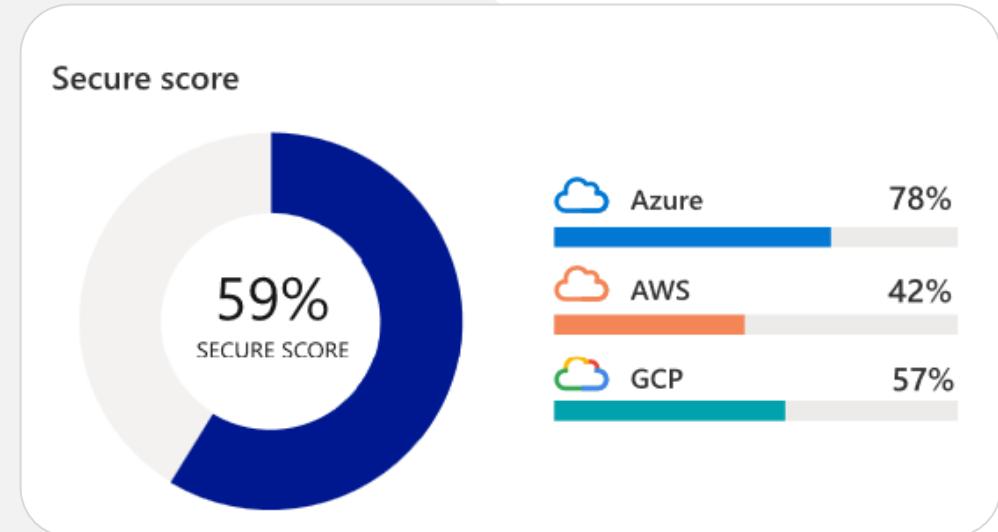
### Data-aware security posture

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

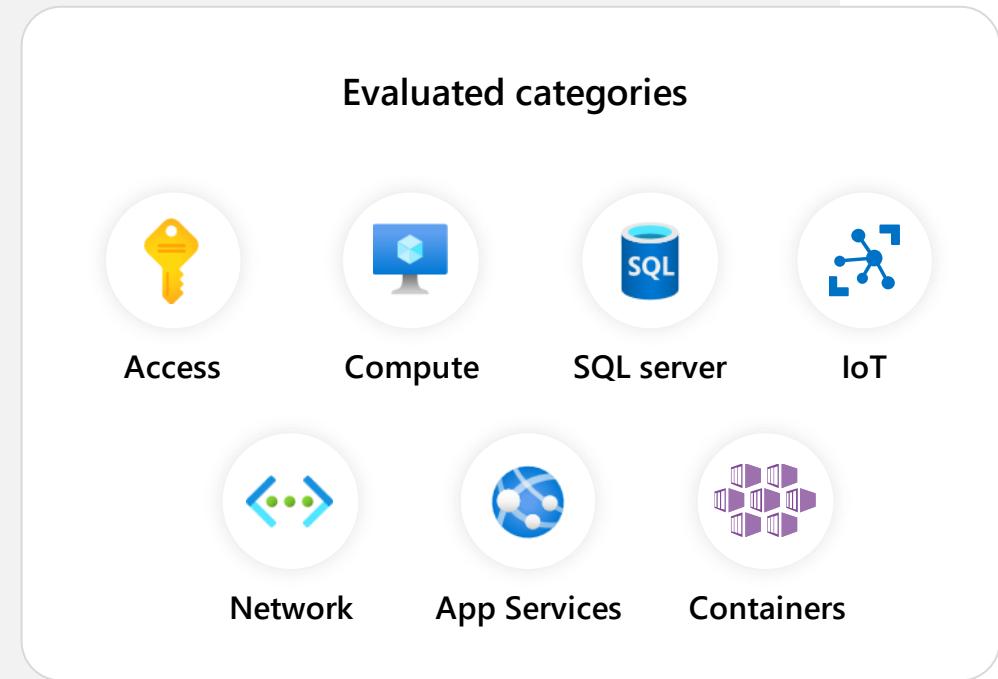
## Secure Score

- » 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 Management	●	●
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 ( <i>public preview on April 15</i> )		●
Agentless vulnerability assessments for container images, including registry scanning ( <i>public preview on April 15</i> )		●
Sensitive data discovery ( <i>generally available for Storage in May</i> )		●
Data flows discovery ( <i>generally available in May</i> )		●

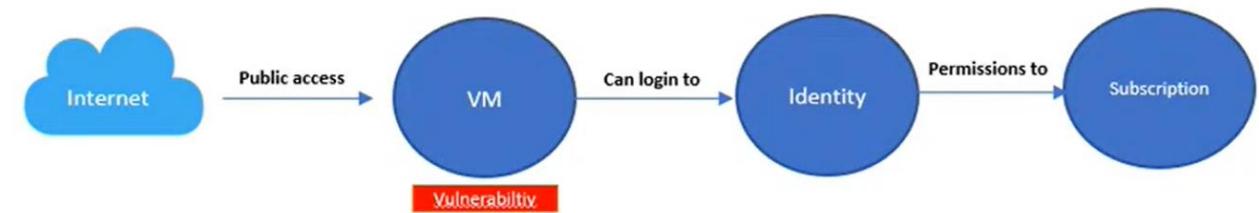
# Foundational CSPM vs Defender CSPM (Cloud coverage)

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



Security Explorer

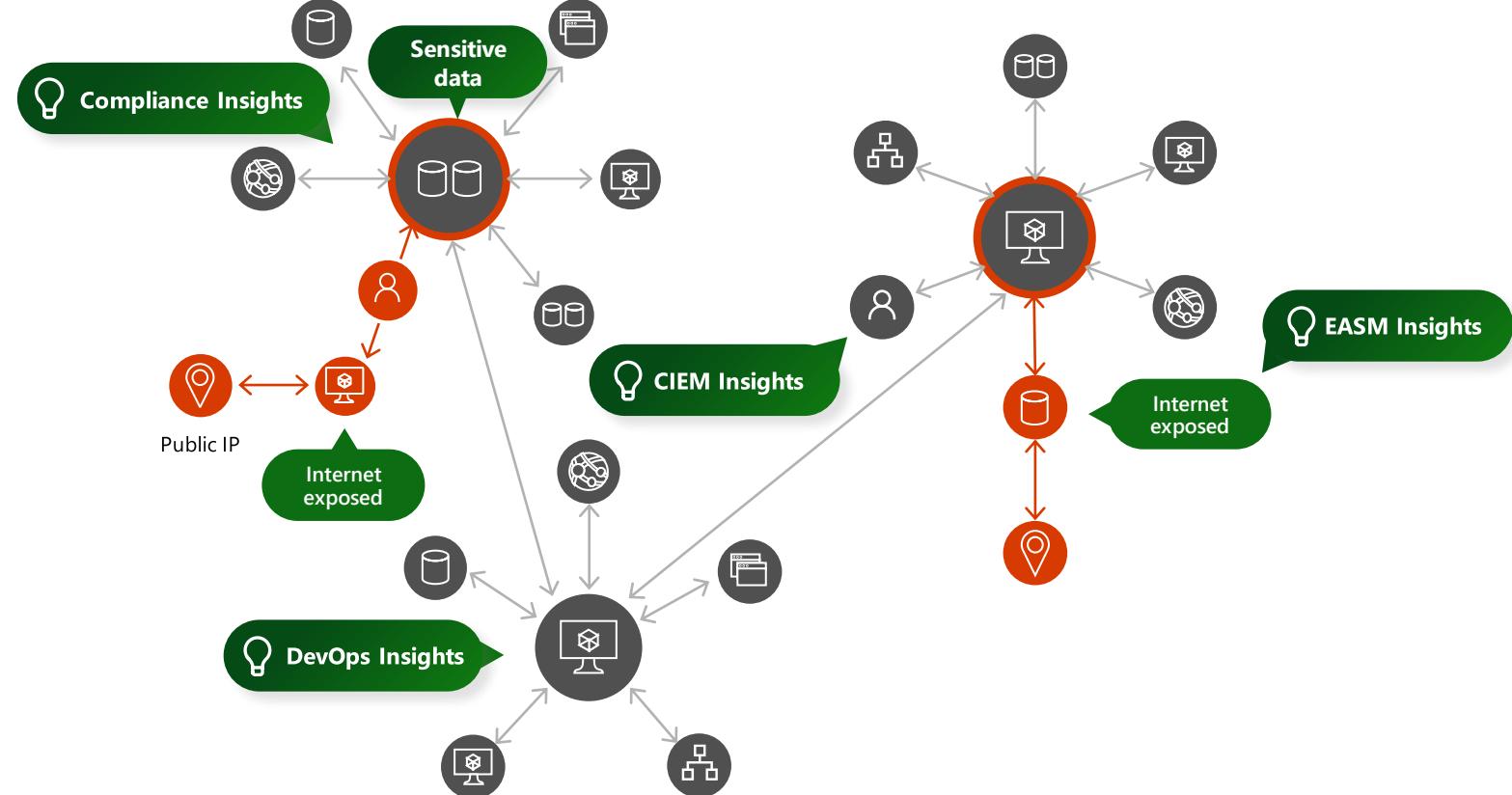
Select  that has  with  equals

and has  with  equals

and with  equals

# 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

The screenshot displays two search panels within the Cloud Security Explorer interface.

**Top Panel (Virtual machines):**

- Search term: Virtual machines (group)
- Filter: Has vulnerabilities
- Condition: Where CVE ID Equals CVE-2021-44228
- Condition: OR (linked to the first one)
- Condition: Where CVE ID Equals CVE-2021-45046

**Bottom Panel (Pods):**

- Search term: Pods
- Filter: Contains Containers
- Filter: Is running
- Filter: Images
- Filter: Has vulnerabilities
- Condition: Where Severity Equals High

Both panels include a "Clear all" button and a back arrow icon.

# 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 ↑↓

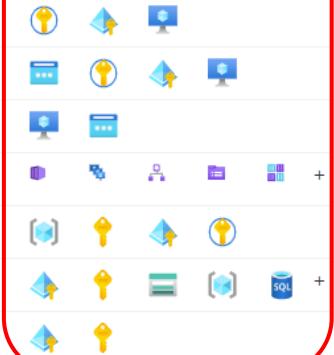
Environment ↑↓

Paths count ↑↓

Risk categories

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 Kev 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

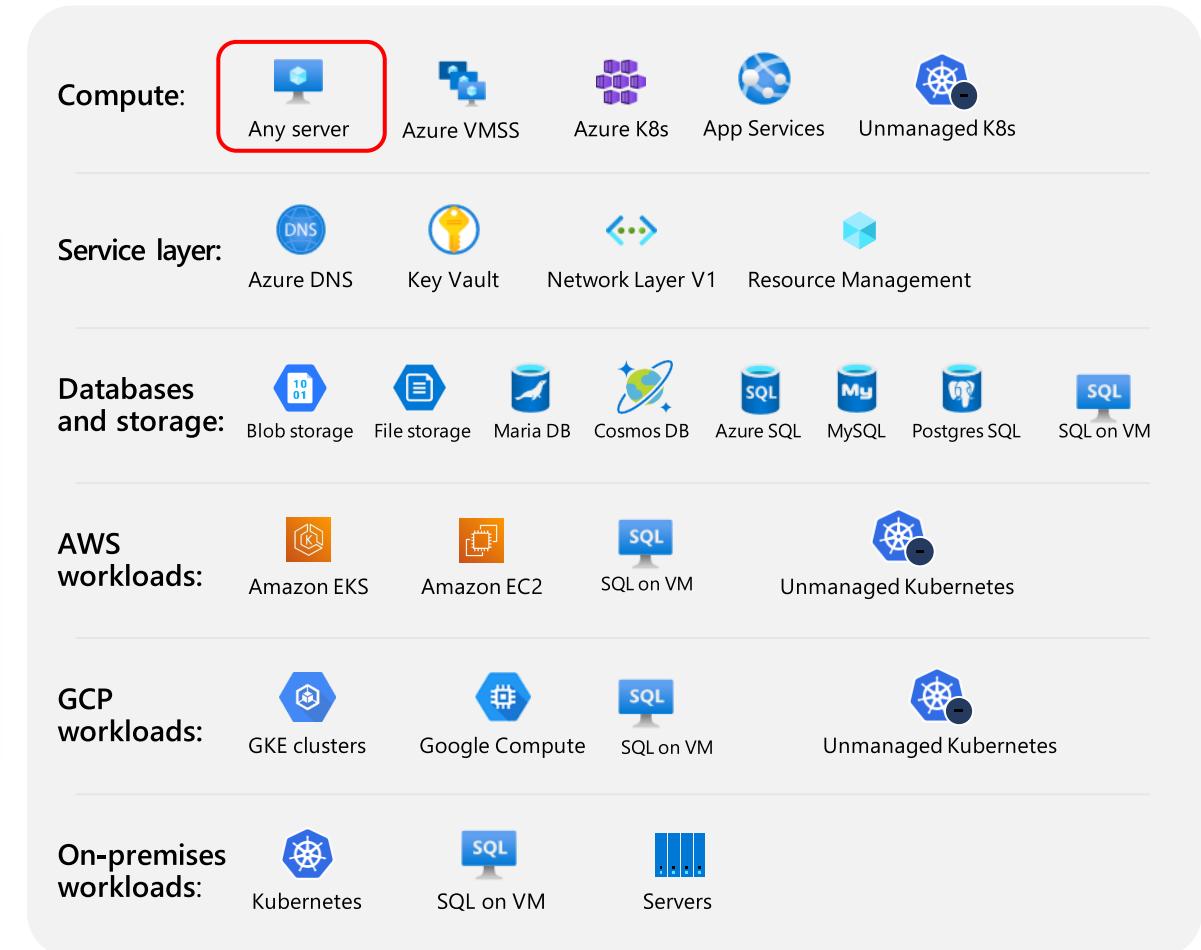
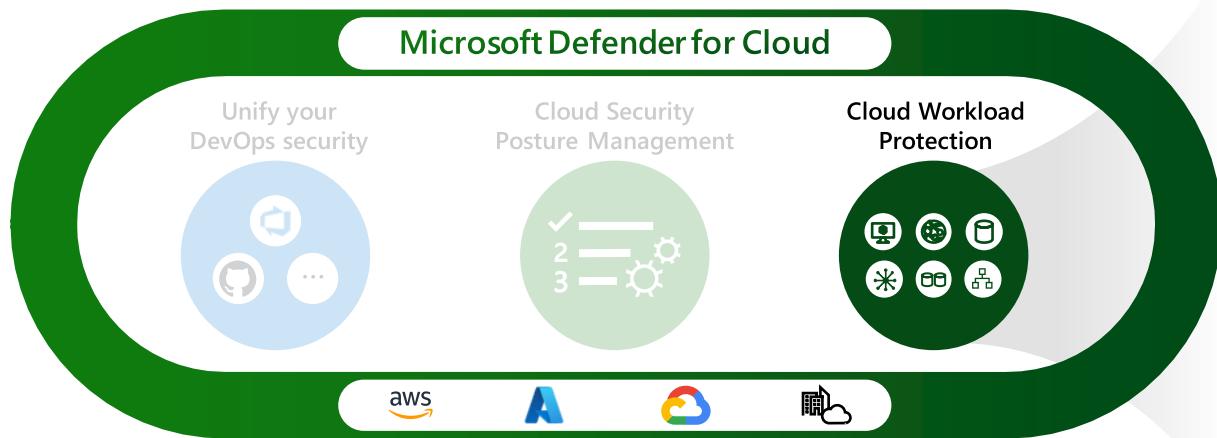
Affected resources



**Detect threats  
and protect  
your workloads**



# Cloud workload protection

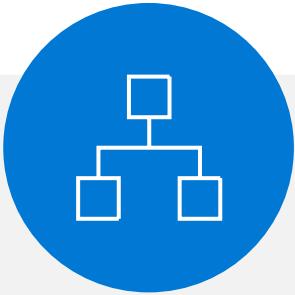


# Threat protection for all layers of the cloud and on-premises



## 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

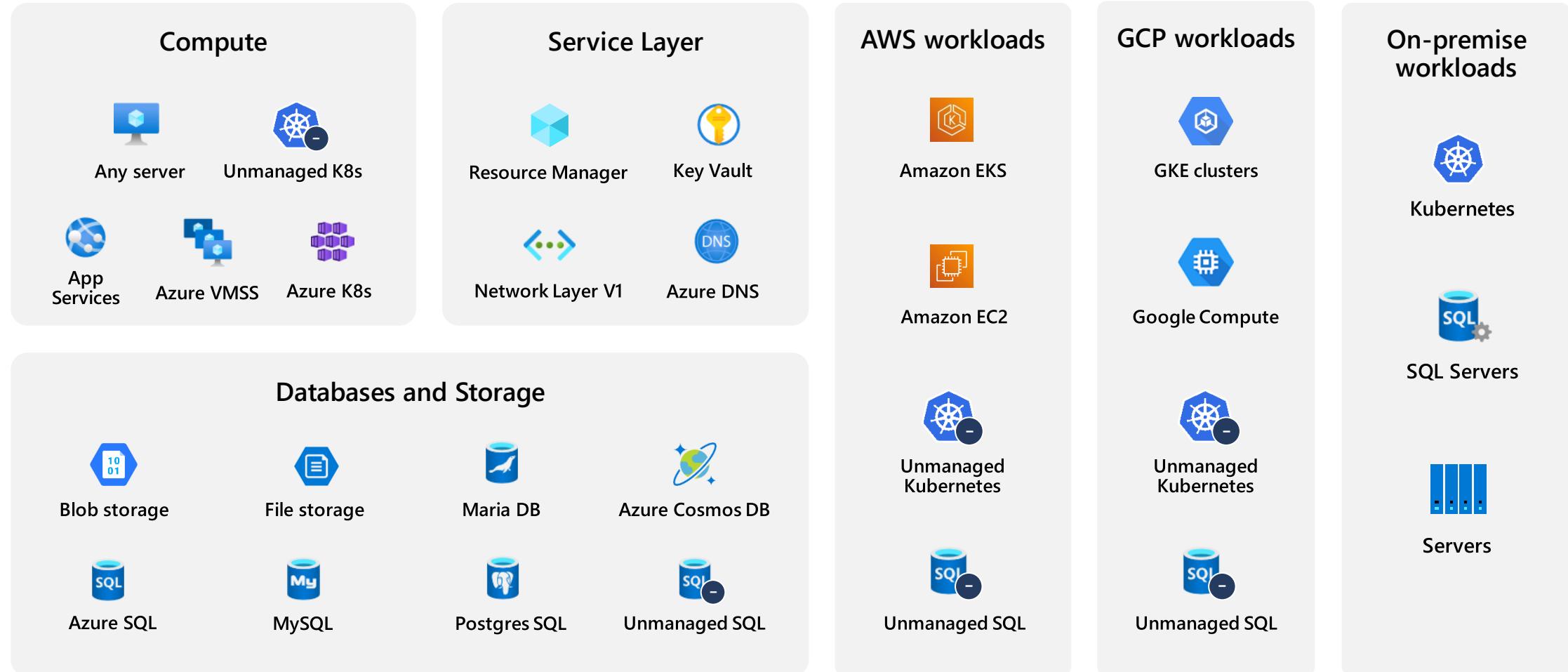
Identify and remediate vulnerabilities before they are exploited



## 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](#)\*\*

## 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](#)

\* Currently Azure Only

\*\*Azure and AWS

# 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

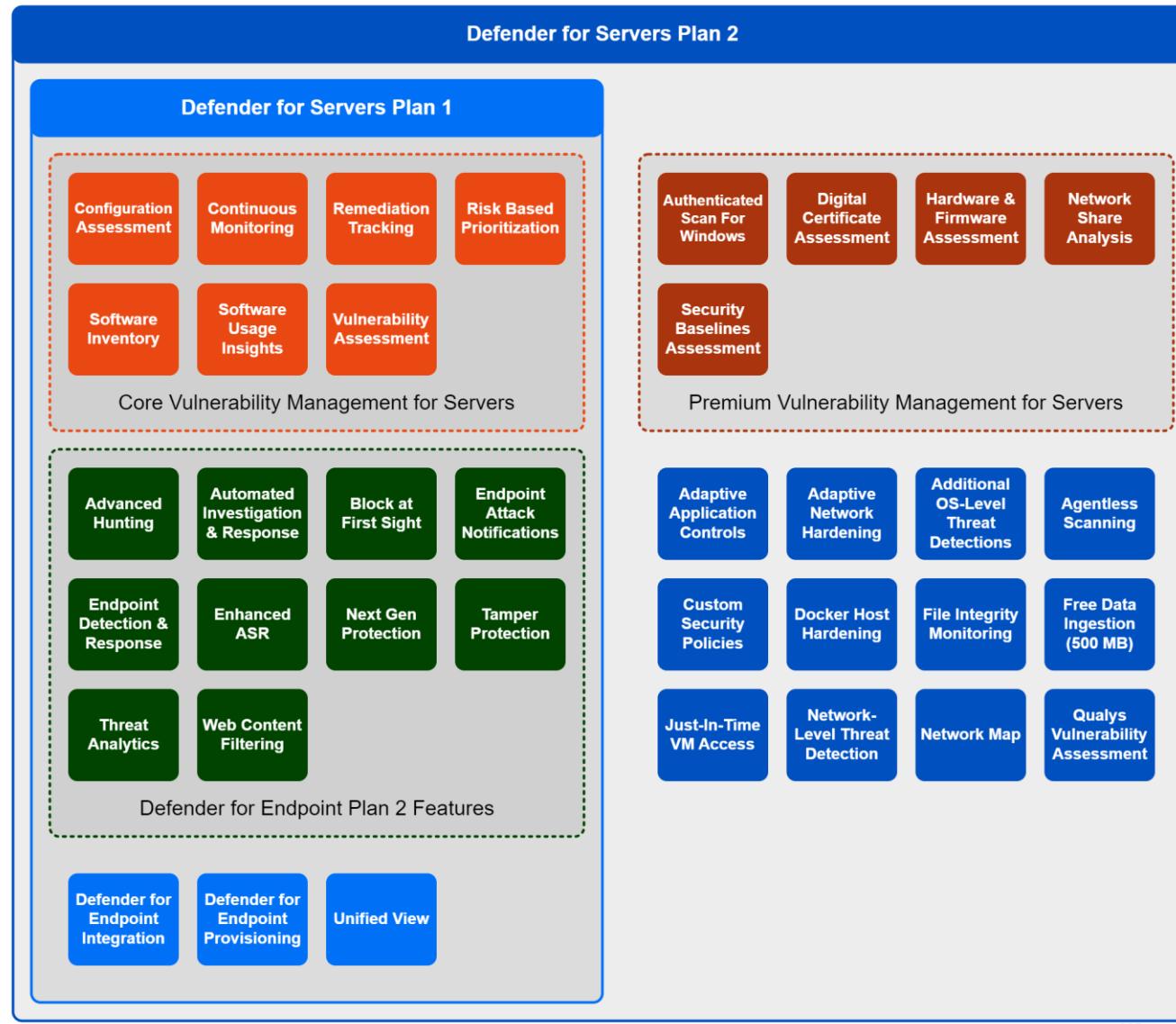
Key capabilities	MDVM capabilities included in foundational server protection <b>(Defender for Servers P1 &amp; Defender for Endpoint for servers)</b>	MDVM add-on (\$2) available to Defender for Endpoint for servers	MDVM capabilities included in Defender for Servers P2
Vulnerability assessment			
Configuration 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

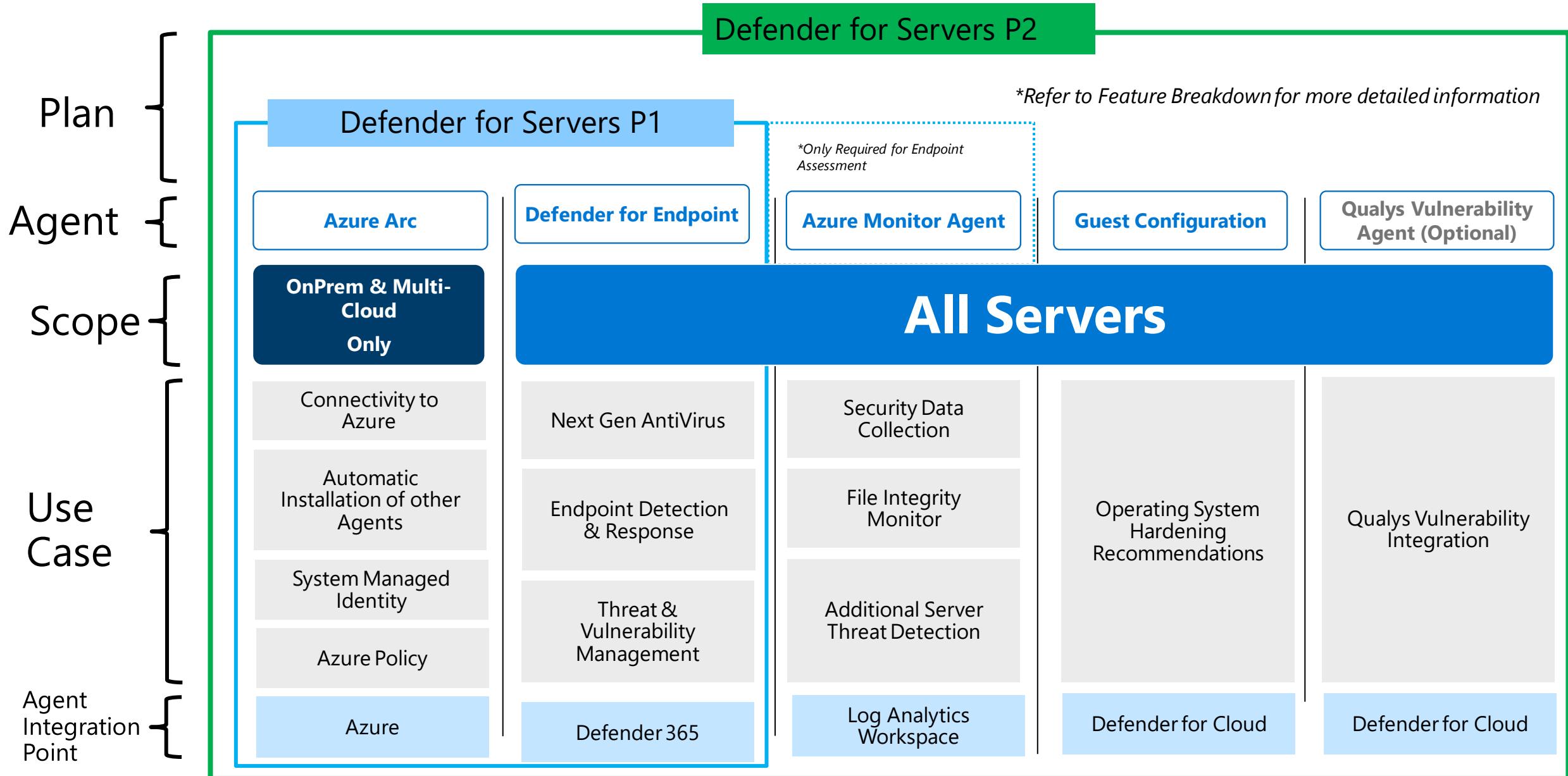
# Another view – from m365maps.com



m365maps.com

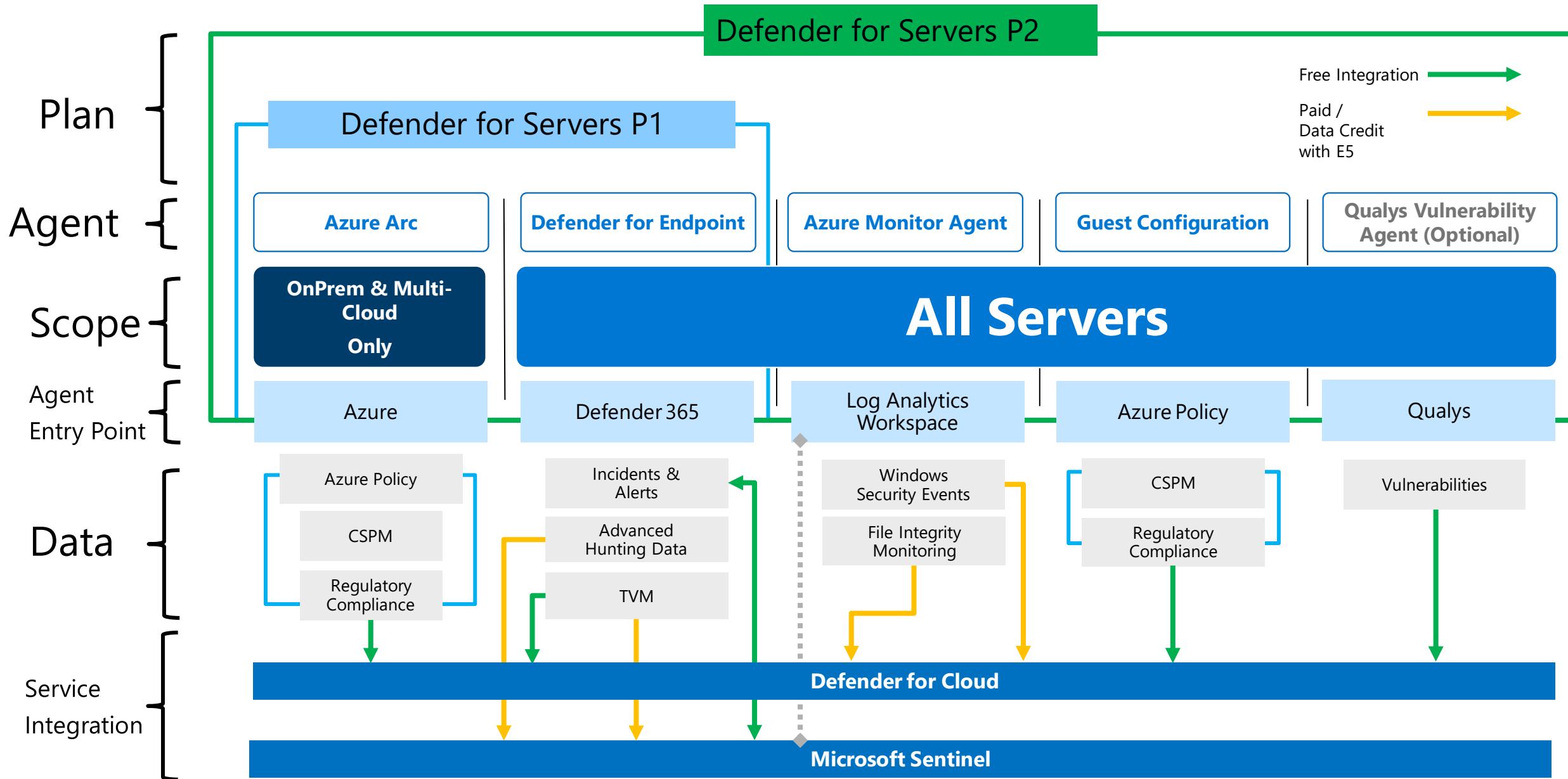
# Defender for Servers Agents

## High Level Breakdown



# Defender for Servers Agents

## Data Integration with Microsoft Security



# Defender for Servers

## Management

### Third Party System Management



### Antivirus Exclusions

### Defender for Endpoint Settings

### Defender for Endpoint Updates

### Defender 365 Portal

security.microsoft.com

A screenshot of the Microsoft 365 Defender Home page. It features a central 'Welcome to Microsoft 365 Defender' banner with a lock icon. Below it are three main sections: 'Microsoft Secure Score' (Secure Score: 49.08%), 'Device compliance' (No managed devices), and 'Devices with active malware' (3 users at risk). The left sidebar includes links for Home, Incident &amp; alerts, Hunting, Active B submissions, Threat analysis, Secure score, Learning hub, Assets, Devices, Identities, and Endpoints.

### Endpoint Detection & Response

### Deeper Investigation

### Advanced Hunting

### Threat Analytics

### Microsoft Secure Score

### Defender for Cloud Portal

portal.azure.com

A screenshot of the Microsoft Defender for Cloud Overview page. It displays a 'Security posture' section with a pie chart (7% remediated) and a progress bar (71%). Below it are sections for 'Regulatory compliance' (Microsoft cloud security benchmark) and 'OpenSSL v3 vulnerability fixer' (details about CVE-2022-3795 and CVE-2022-3796). The right sidebar shows statistics: 1 Azure subscriptions, 1 GCP projects, 99 Assessed resources, 16 Active recommendations, and 1 Security alerts.

### Incidents and Alerts

### Threat & Vulnerability Management

### 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



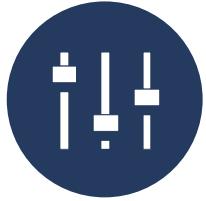
## Multicloud support

- 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

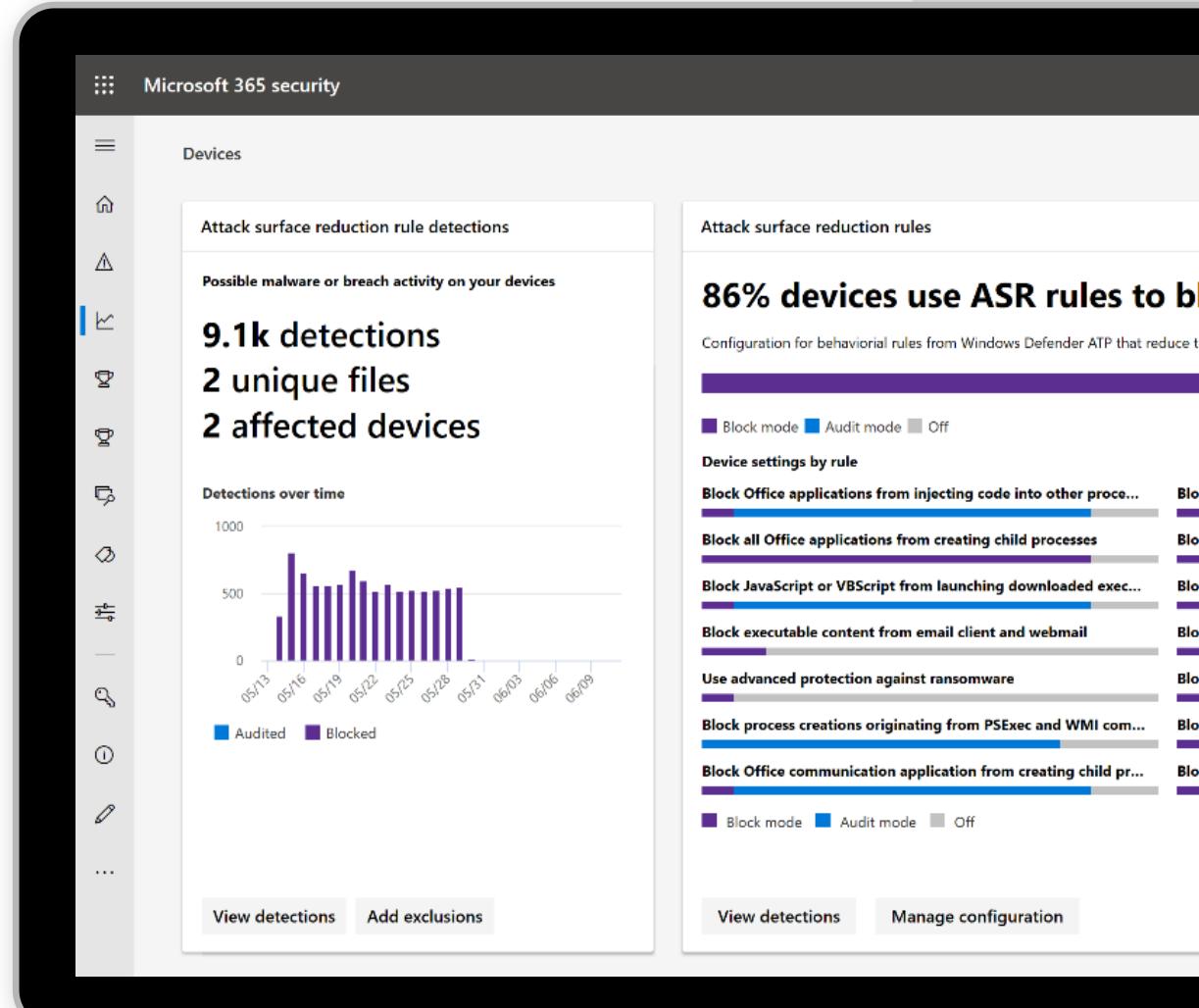


# Attack surface reduction

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

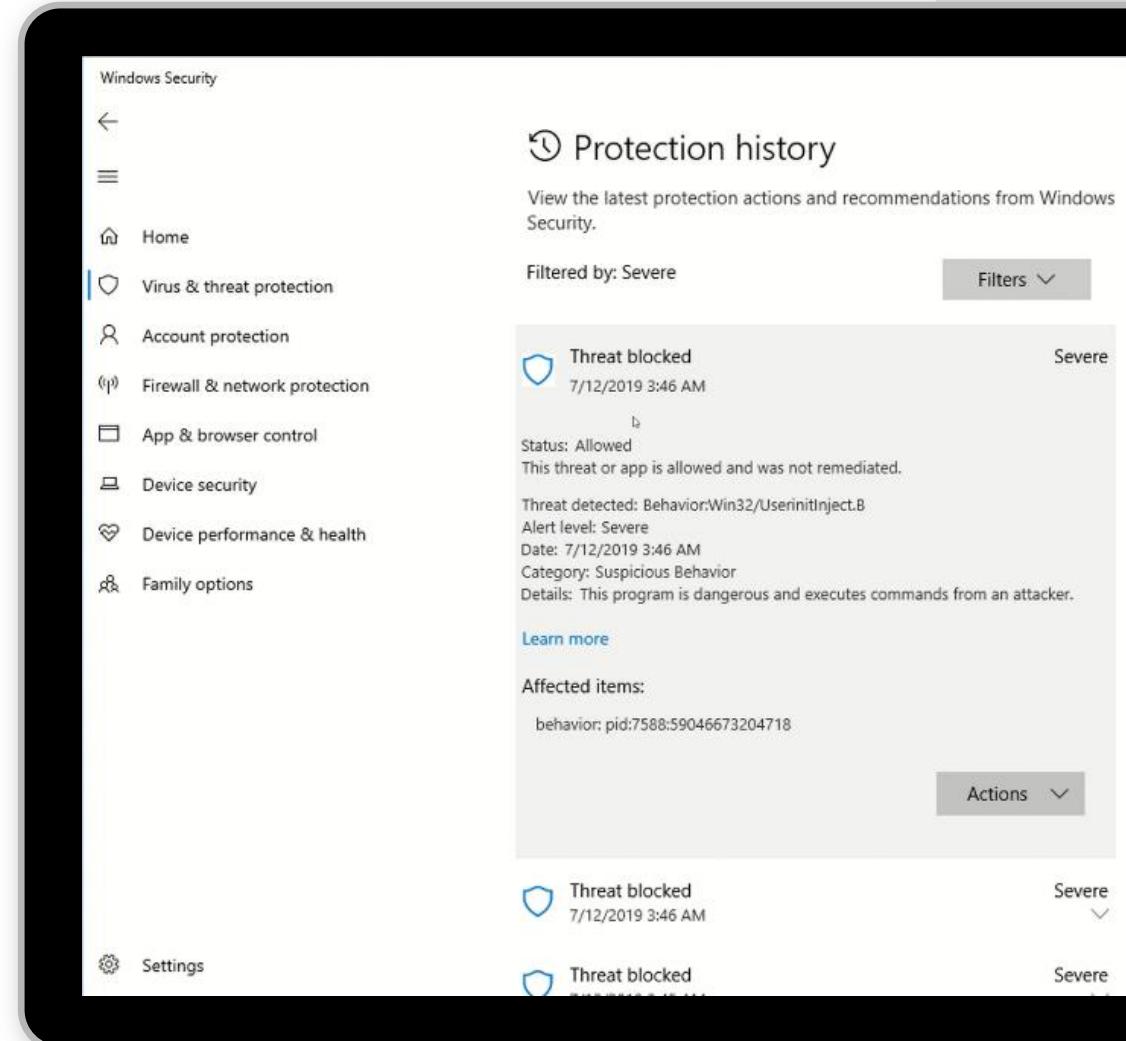


# Next generation antivirus protection

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

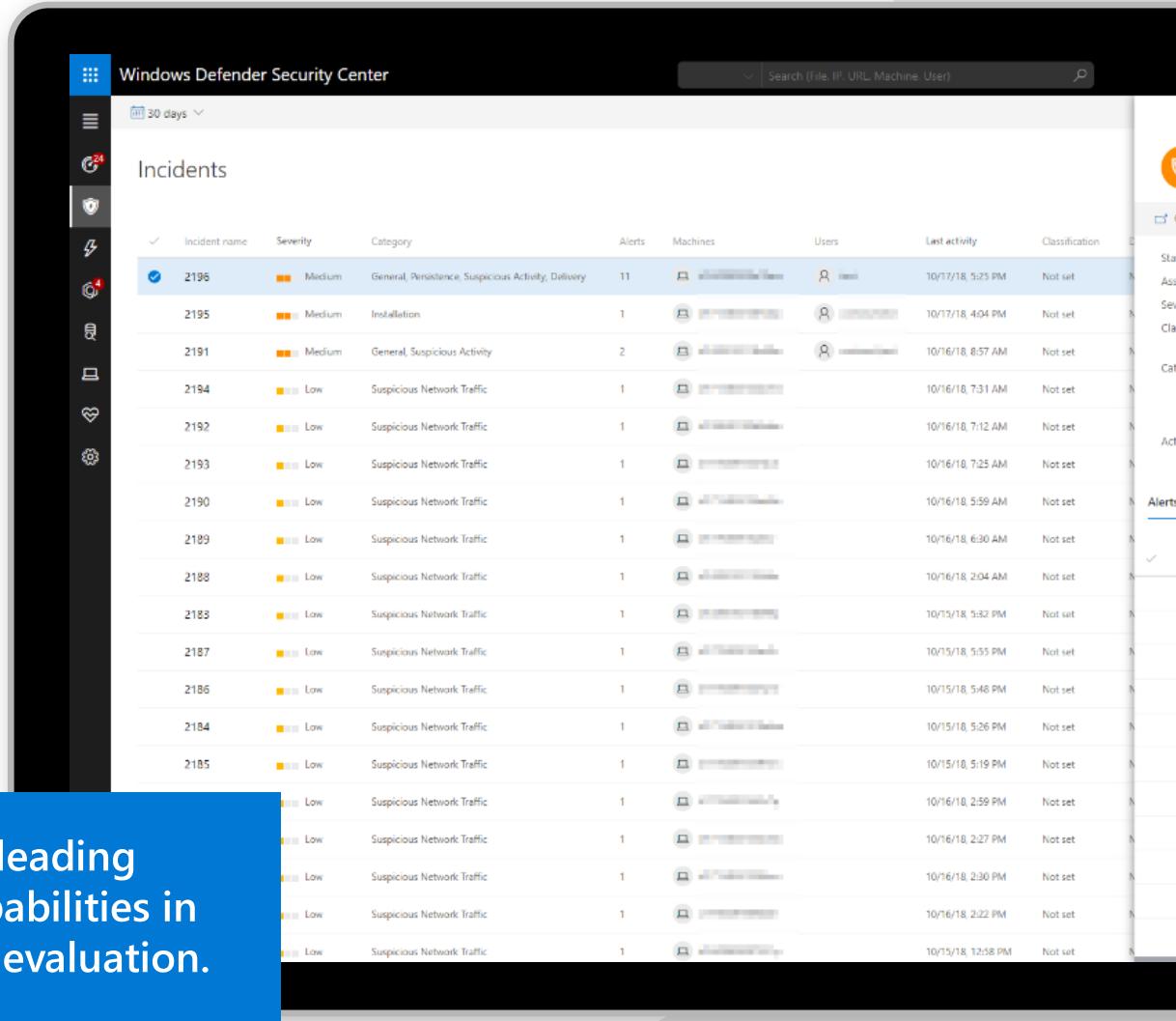


# Endpoint detection & response

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



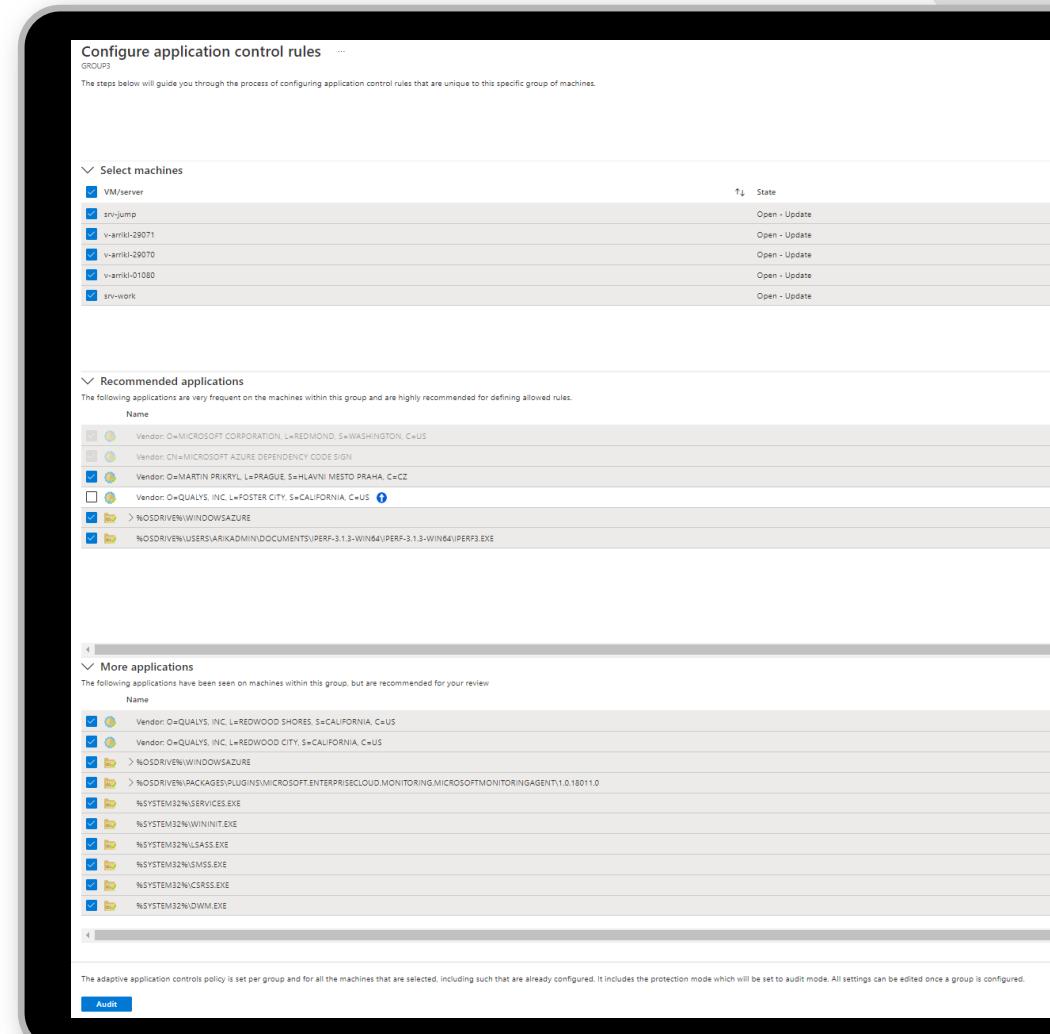
The screenshot shows the Windows Defender Security Center interface. At the top, there's a search bar with the placeholder "Search (File, IP, URL, Machine, User)" and a magnifying glass icon. Below the search bar is a date range selector set to "30 days". The main area is titled "Incidents" and displays a table of 21 recent events. The columns in the table are: Incident name, Severity, Category, Alerts, Machines, Users, Last activity, and Classification. The incidents listed are mostly "Suspicious Network Traffic" events, with one notable entry being "Installation". The "Last activity" column shows dates ranging from October 15, 2018, to October 17, 2018.



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

The screenshot shows a Microsoft Azure Security Center page titled "Vulnerabilities in your virtual machines should be remediated". The page displays a summary of findings: Severity is Low, Freshness interval is 4 Hours, and Tactics and techniques include Initial Access (+5). Below this, there are sections for Description, Related recommendations (1), Remediation steps, Affected resources, and Security checks. A table lists various findings, such as EOL/Obsolete Operating System: Ubuntu 16.04 Detected and Microsoft Internet Explorer Security Update for September 2020. The table includes columns for ID, Security check, Category, and Applies.

ID	Security check	Category	Applies
105977	EOL/Obsolete Operating System: Ubuntu 16.04 Detected	Security Policy	2 of 13
100410	Microsoft Internet Explorer Security Update for September 2020	Internet Explorer	2 of 13
91674	Microsoft Windows Security Update for September 2020	Windows	2 of 13
91462	Microsoft Windows Security Update Registry Key Configuratio...	Windows	1 of 13
178369	Debian Security Update for tzdata (DLA 2424-1)	Debian	1 of 13
178418	Debian Security Update for screen (DLA 2570-1)	Debian	1 of 13
374891	Sudo Heap-based Buffer Overflow Vulnerability (Baron Samedi... Local	Local	1 of 13
177442	Debian Security Update for file (DSA 4550-1)	Debian	1 of 13

# 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

The screenshot shows a tablet displaying the Microsoft Security Center Just in time VM access dashboard. The title bar reads "Dashboard > Security Center | Just in time VM access" and "Showing subscription 'ASC DEMO'". Below the title, there are two links: "What is just in time VM access?" and "How does it work?". A large yellow circle highlights the search bar labeled "Search to filter items...". The main section is titled "Virtual machines" and includes three filter buttons: "Configured" (underlined), "Not Configured", and "Unsupported". A message states: "VMs for which the just in time VM access control is already in place. Presented data is for the last week." Below this, a summary says "20 VMs" and features a "Request access" button. A yellow circle also highlights the "Request access" button. A table lists 10 VMs with columns: Virtual machine, Approved, Last access, Connection details, and Last user. All VMs listed have 0 Requests and N/A for Last access and Last user. The Connection details column shows a shield icon with a minus sign.

Virtual machine	Approved	Last access	Connection details	Last user
vm1redhat	0 Requests	N/A	shield -	N/A
vm2ubuntu	0 Requests	N/A	shield -	N/A
vm2	0 Requests	N/A	shield -	N/A
vm1	0 Requests	N/A	shield -	N/A
CheckPoint-Firewall-Ce...	0 Requests	N/A	shield -	N/A
VM5	0 Requests	N/A	shield -	N/A
vm4	0 Requests	N/A	shield -	N/A

# 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

The screenshot shows a user interface for 'Adaptive Network Hardening recommendations'. At the top, it says 'Adaptive Network Hardening recommendations should be applied on internet facing virtual machines'. Below this, there are sections for 'Severity' (High) and 'Freshness interval' (24 Hours). The main content area has three expandable sections: 'Description', 'Remediation steps', and 'Affected resources'. Under 'Affected resources', there are tabs for 'Unhealthy resources (7)', 'Healthy resources (80)', and 'Not applicable resources (16)'. A search bar at the top of the list allows filtering by 'Name'. The list of unhealthy resources includes:

Name	Subscription	Actions
VM6	ASC DEMO	...
vm2	ASC DEMO	...
vm3	ASC DEMO	...
ContosoWeb1	Contoso IT - demo	...
ContosoSQLSvr3	Contoso IT - demo	...
ContosoSQLSrv1	Contoso IT - demo	...
CH-RETAILVM01	Contoso Hotels	...

Below the resource list, there is a section titled 'Allowed Sources' with a note 'None'.

# 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 screenshot shows the Microsoft Defender for Cloud File Integrity Monitoring dashboard. At the top, it displays summary statistics: Total servers (8), Total changes (50), Change type (Files: 2, Registry: 48), and Change category (Modified: 2, Added: 24, Removed: 24). Below this, there are two tabs: 'Servers' and 'Changes'. The 'Changes' tab is selected, showing a message about presenting the latest 100 changes and a search bar labeled 'Search changes'. A table lists eight recent changes, all of which are registry modifications on the server 'vmtest'. The table columns include Entity, Server, and Type.

Entity	Server	Type
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist   \REGISTRY\MACHINE\COMPO...	vmtest	Registry
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist   \REGISTRY\MACHINE\COMPO...	vmtest	Registry
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist   \REGISTRY\MACHINE\DRIVERS	server16-test	Registry
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist   \REGISTRY\MACHINE\DRIVERS	server16-test	Registry
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist   \REGISTRY\MACHINE\DRIVERS	vmtest	Registry

# The Rise of Containers



## Container adoption is booming

» The use of containers in production increased by **300%** between 2016 and 2021<sup>1</sup>

Kubernetes use in production has increased to **83%**<sup>1</sup>



## Increase in number and sophistication of attacks targeting containers and Kubernetes

» **94%** orgs experienced at least one security incident in Kubernetes during 2021<sup>3</sup>

Attack volume continued to increase, growing by **26%** in 2020<sup>2</sup>



## Extra focus on shift-left

» Infamous cases: SolarWinds, Log4j Supply chain risks is one of the common sources of compromise in Kubernetes<sup>4</sup>

<sup>1</sup> [CNCF 2020 Container Adoption Survey](#)

<sup>2</sup> Cloud Native Threat Report: Attacks in the wild on the Container Supply Chain and Infrastructure

<sup>3</sup> State of Kubernetes Security Report 2021

<sup>4</sup> [Kubernetes Hardening Guidance](#) - Cybersecurity Technical Report by the National Security Agency (NSA) and the Cybersecurity and Infrastructure Security Agency (CISA)

# Container security is different

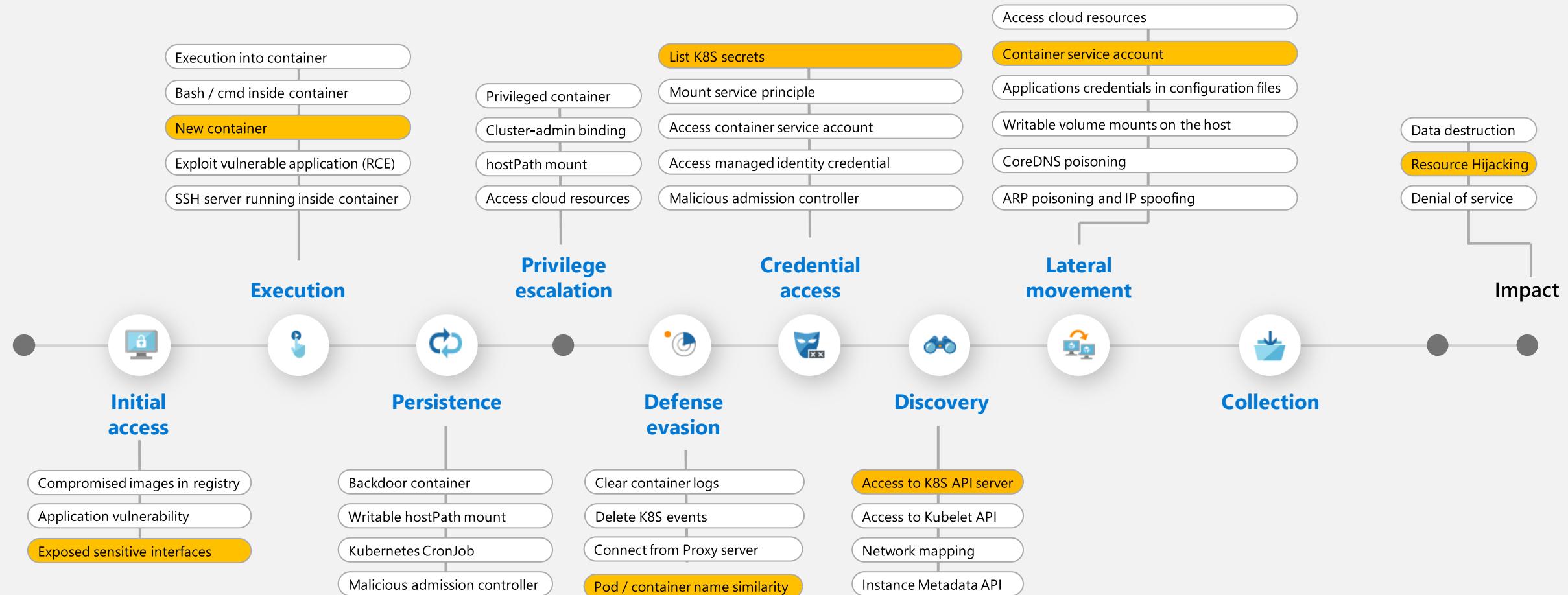
- Containerized applications are elastic, spawn and re-size rapidly.
- Images are immutable , containers are short lived.
- Visibility of containers traffic flows are difficult to track with traditional tools.
- Runtime environment is complex, with different configuration layers and options.



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 Defender for Containers

Protect multi-cloud and hybrid container deployments



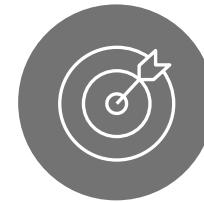
## Hardening

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.



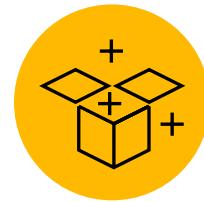
## Advanced threat detection

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.

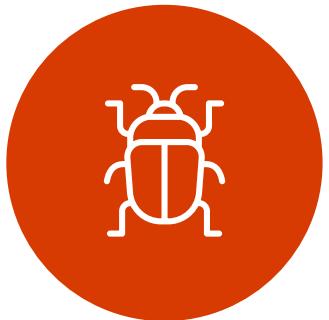


## Deployment and monitoring

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

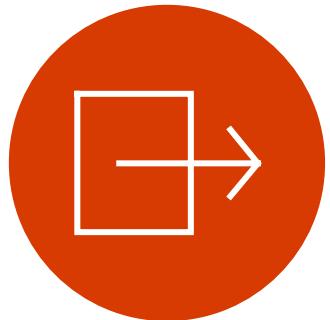


# Top concerns in cloud storage



## 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

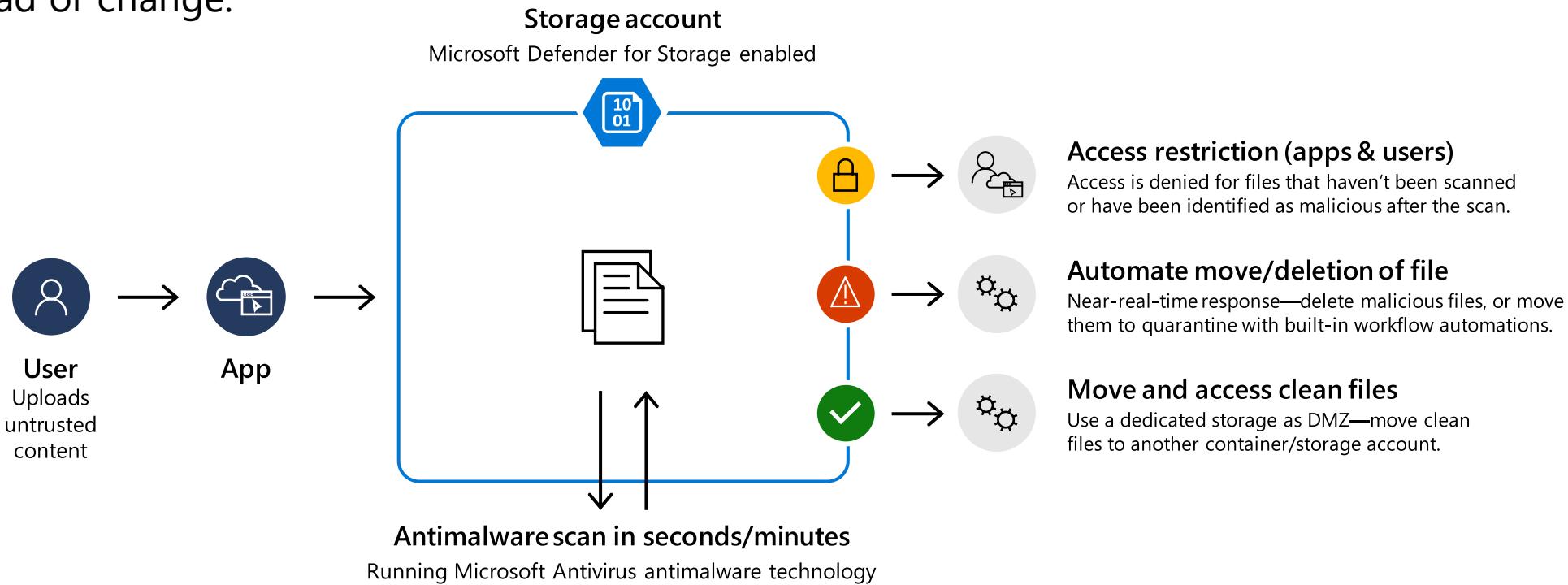
The screenshot shows the Microsoft Defender for Cloud Security alerts interface. It displays 4 active alerts and 1 affected resource. One alert is highlighted: "Access from a Tor exit node to a storage blob container". The alert details show an IP address (104.16.101.11) accessed a storage account ('eitandefaultstorage') at 12/26/21, 03:26 PM. The threat actor used 'Pre-attack' tactics like 'Lateral Movement'. The alert is categorized as 'High' severity, 'Active' status, and 'Low, Medium, High' severity. The affected resource is 'eitandefaultstorage'.

The screenshot shows the Microsoft Defender for Storage Security alert details page for a potential malware upload. The alert ID is 251762333106289999\_05962113-de7f-4d71-9271-56894a982ec5. The alert is titled "Potential malware uploaded to a storage blob container". It is a high-severity alert from an Azure AD user (N/A) at 12/14/21, 09:04 AM. The user agent is Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36. The affected resource is 'eitandefaultstorage' (Storage account). The threat actor used 'PutBlob' operations to upload a file named 'qq.txt' to the 'misc-files' directory. The file was identified as malicious, belonging to the MalwareFamily Virus. The detection source is Team Cymru. Related entities include the Azure resource and the file itself.

- » 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 its unique Threat Intelligence capabilities.

# Antimalware scanning for storage

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

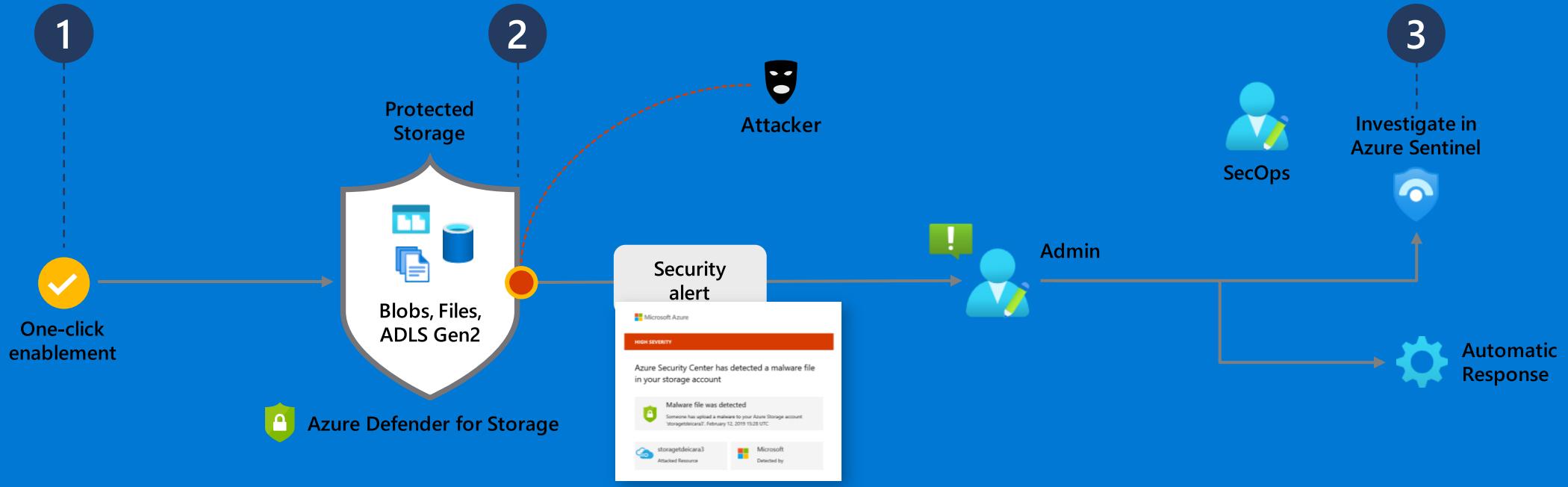
- Near-real-time scan on upload.
- Full antimalware scan.
- Periodic scans with continuously updated malware signatures.

## 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

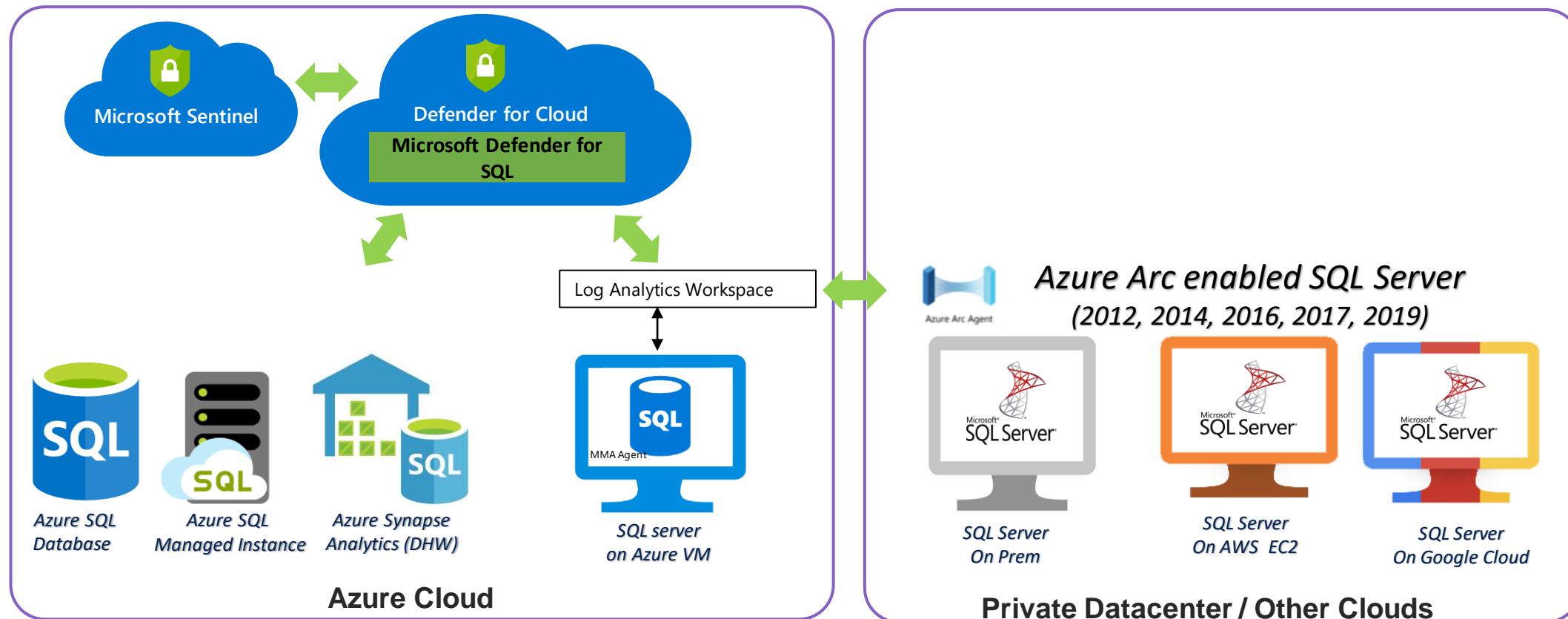
## Response at scale

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

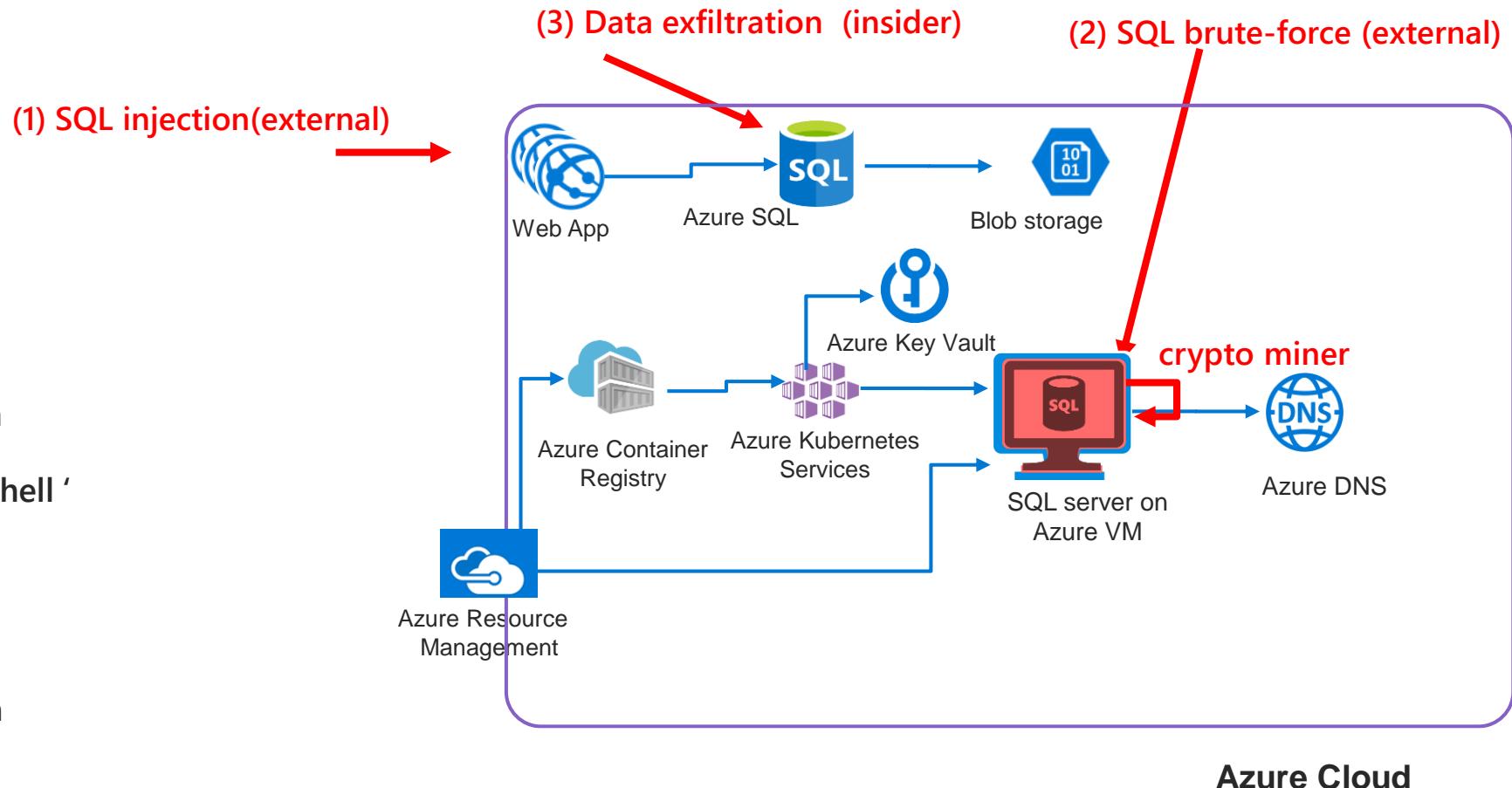


**Vulnerability Assessment** : discover and remediate security misconfigurations, database vulnerabilities in SQL servers

# 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>

# 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

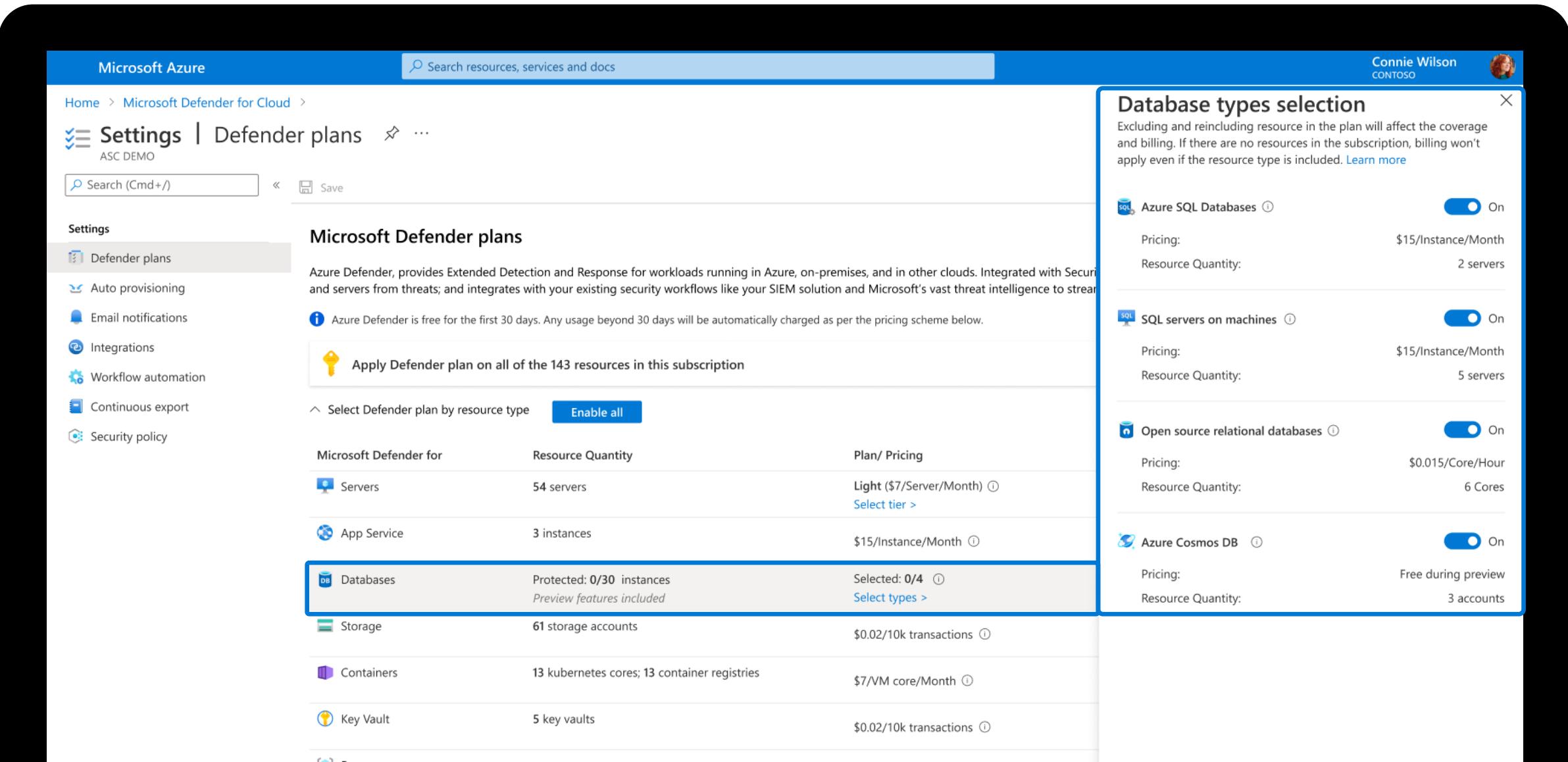
## Defender for Azure Cosmos DB



Azure Cosmos DB



# Enable: One-click experience to protect your database estate



**Microsoft Azure** Search resources, services and docs Connie Wilson  
CONTOSO

Home > Microsoft Defender for Cloud >

**Settings | Defender plans** ASC DEMO

**Microsoft Defender plans**

Azure Defender provides Extended Detection and Response for workloads running in Azure, on-premises, and in other clouds. Integrated with Security and servers from threats; and integrates with your existing security workflows like your SIEM solution and Microsoft's vast threat intelligence to stream

**Apply Defender plan on all of the 143 resources in this subscription**

**Select Defender plan by resource type** Enable all

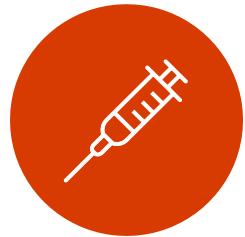
Microsoft Defender for	Resource Quantity	Plan/ Pricing
Servers	54 servers	Light (\$7/Server/Month) <span>Select tier &gt;</span>
App Service	3 instances	\$15/Instance/Month <span>...</span>
Databases	Protected: 0/30 instances <i>Preview features included</i>	Selected: 0/4 <span>Select types &gt;</span>
Storage	61 storage accounts	\$0.02/10k transactions <span>...</span>
Containers	13 kubernetes cores; 13 container registries	\$7/VM core/Month <span>...</span>
Key Vault	5 key vaults	\$0.02/10k transactions <span>...</span>

**Database types selection**

Excluding and reincluding resource in the plan will affect the coverage and billing. If there are no resources in the subscription, billing won't apply even if the resource type is included. [Learn more](#)

<b>Azure SQL Databases</b> <span>On</span>	Pricing: \$15/Instance/Month
Resource Quantity: 2 servers	
<b>SQL servers on machines</b> <span>On</span>	Pricing: \$15/Instance/Month
Resource Quantity: 5 servers	
<b>Open source relational databases</b> <span>On</span>	Pricing: \$0.015/Core/Hour
Resource Quantity: 6 Cores	
<b>Azure Cosmos DB</b> <span>On</span>	Pricing: Free during preview
Resource Quantity: 3 accounts	

# 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

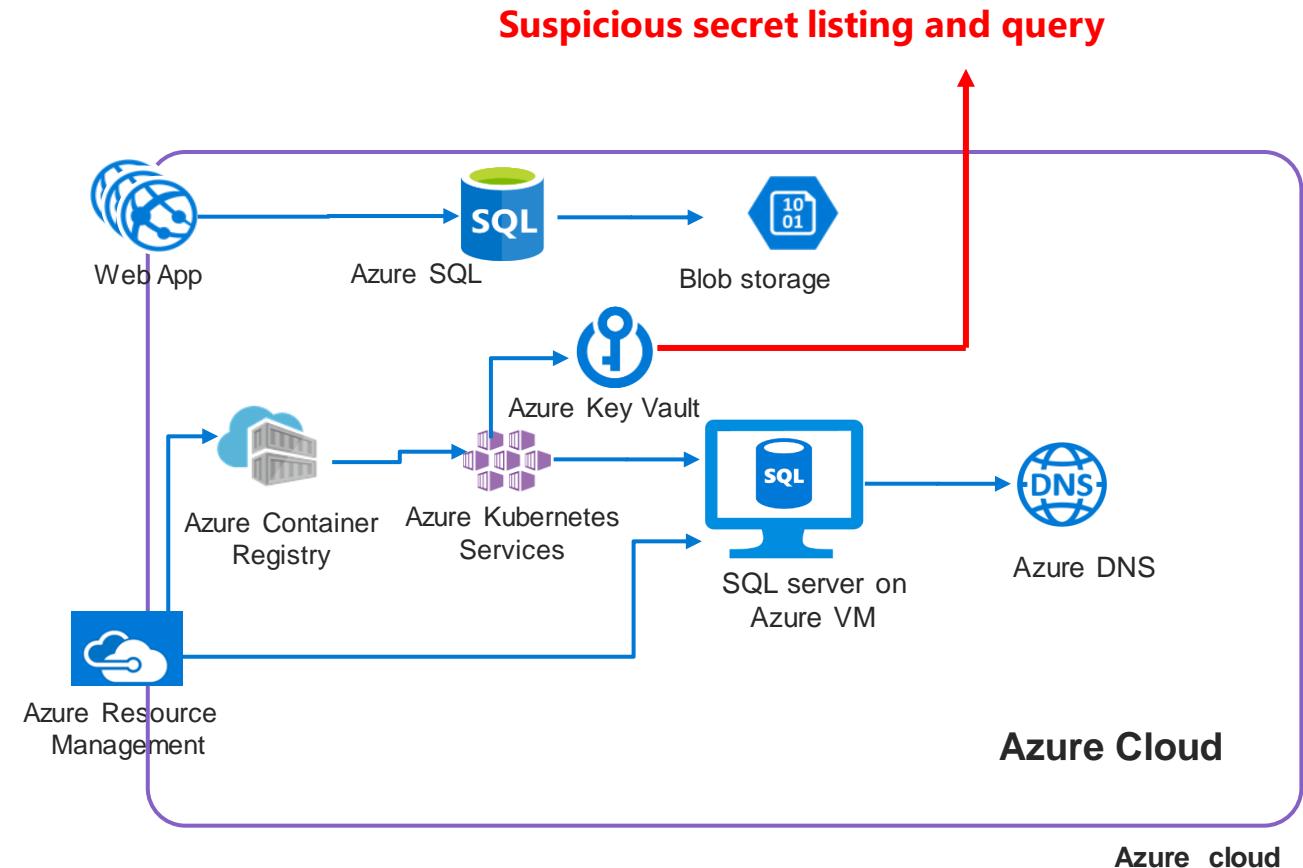
## Brute force

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

# Defender for Key Vault

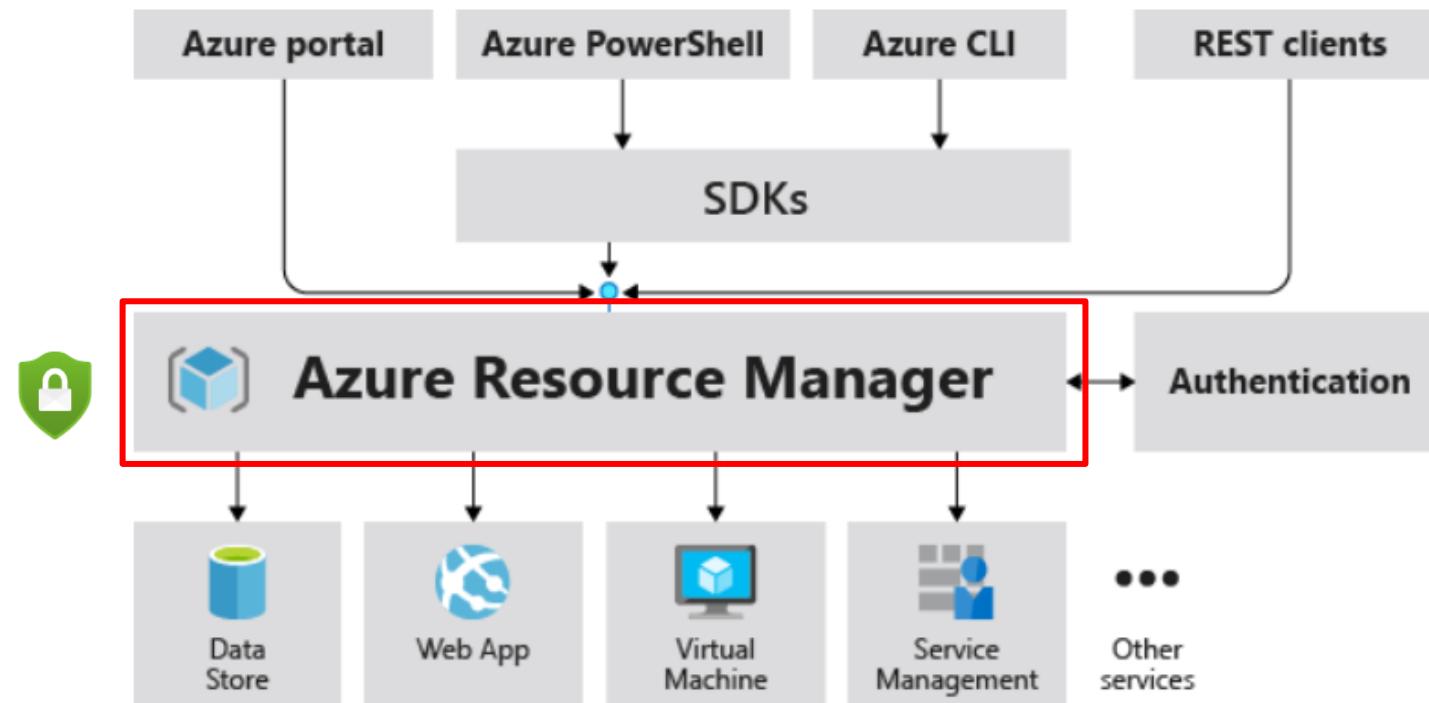


- ⚠️ Detects user accessed high volume of key vaults
- ⚠️ Detects access from a TOR exit node to a key vault
- ⚠️ Detects suspicious policy change and secret query in a key vault
- ⚠️ Detects unusual user accessed a key vault



# 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



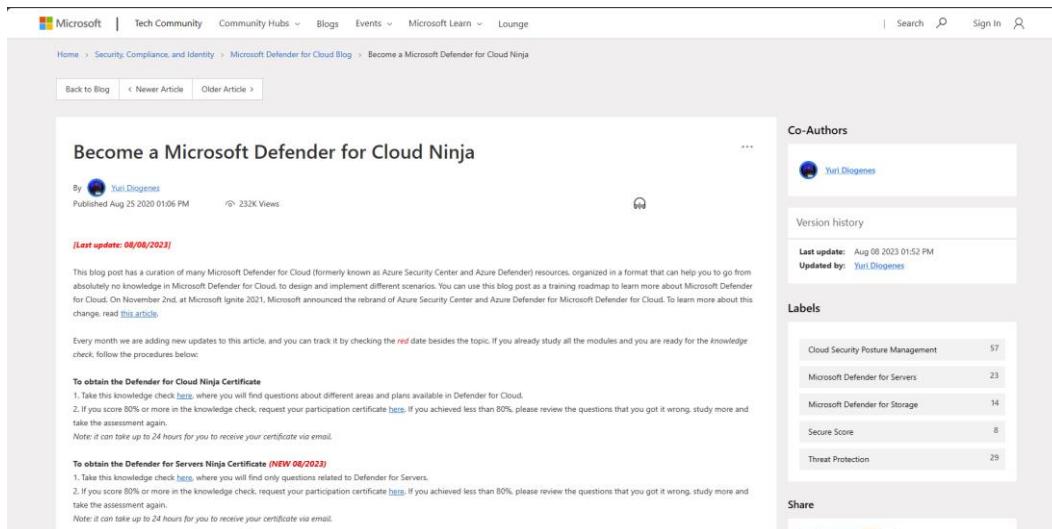
# Wrap-up



# 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](#)



The screenshot shows a Microsoft Learn article titled "Become a Microsoft Defender for Cloud Ninja". It includes sections for Co-Authors (Yuri Diogenes), Version history (last updated Aug 08 2023), Labels (Cloud Security Posture Management, Microsoft Defender for Servers, Microsoft Defender for Storage, Secure Score, Threat Protection), and a Share button.

- 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>



The screenshot shows the Microsoft SC-200 learning path titled "SC-200: Mitigate threats using Microsoft Defender for Cloud". It includes a summary (4 hr 17 min, 6 modules), prerequisites (Intermediate, Security Operations Analyst, Azure, Microsoft Defender for Cloud, Microsoft Defender for External Attack Surface Management), and a note about preparing for Exam SC-200: Microsoft Security Operations Analyst.

# 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>



# Thank you.

