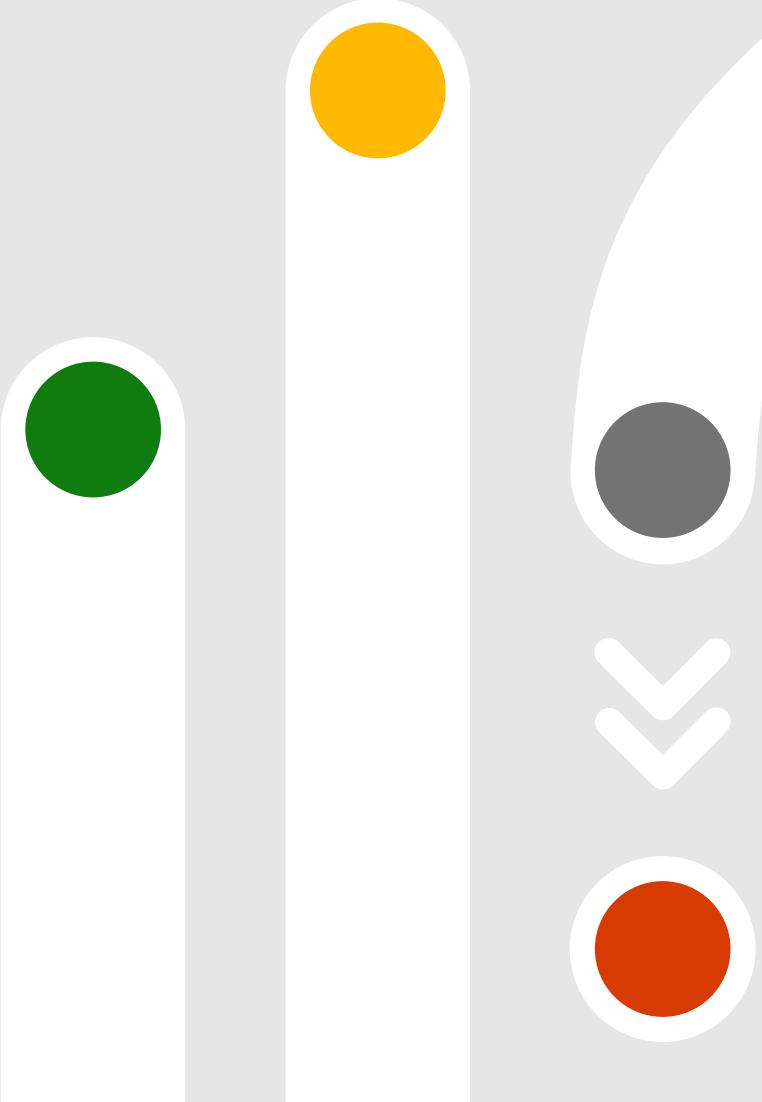




# Microsoft Defender for Cloud

Protect your multicloud and hybrid environments

Insert name here



# Cloud security challenges



## Visibility into security and compliance

» 52% of organizations cite secure configuration of cloud resources as a top priority.<sup>1</sup>



## Increase in number and sophistication of attacks

» In 2021, the average cost of a breach was **\$4.24M**.<sup>2</sup>



## Complexity managing multi-cloud environments

» 92% of organizations are embracing a multi-cloud strategy



<sup>1</sup>Source: 451 Research

<sup>2</sup>Source: [Ponemon Institute, Cost of a Breach Report](#)

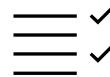
# Microsoft Defender For Cloud

Cloud native protection across clouds and hybrid environments

Harden and manage your Security Posture



Secure configuration of resources



Management of compliance requirements

Detect threats and protect your workloads



Full-stack threat protection



Vulnerability assessment & management

Respond & Automate



Assess and resolve security alerts and incidents

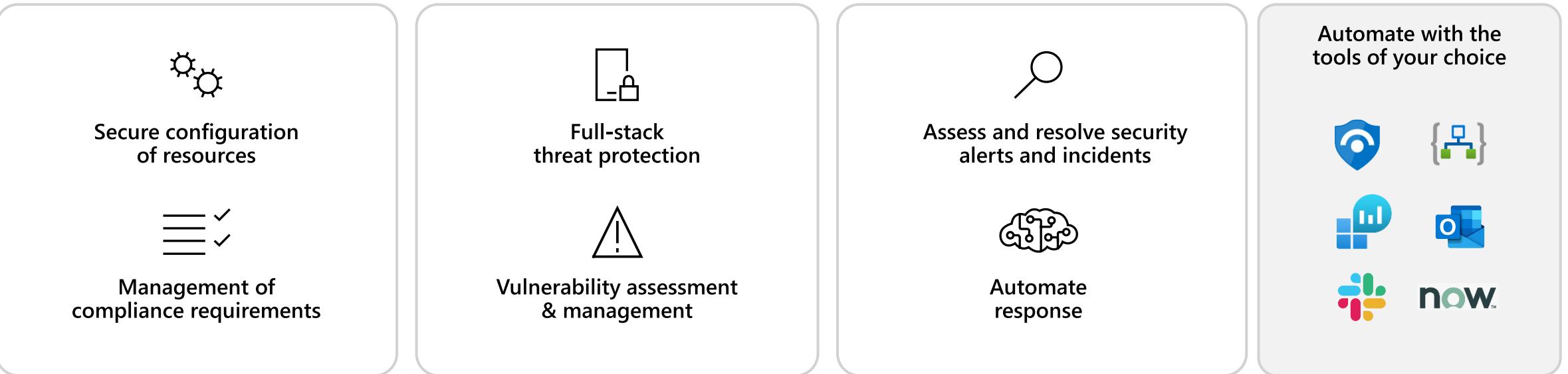


Automate response

Automate with the tools of your choice



now™



Microsoft Azure



Amazon Web Services



Google Cloud Platform



On-prem

# How we're different



## Built-in with Azure

- No deployment, just enable
- Built into the resource provisioning process
- Broadest protection coverage
- Remediate with a click



## Multi-cloud and hybrid support

- Agentless onboarding for AWS and GCP posture management
- Auto provisioning for new resources
- Onboard on-prem resources with Azure Arc



## Secure Score

- Birds-eye view of the security posture of all your clouds
- Prioritized security recommendations
- Track and manage your security posture state over time



## Advanced Threat Protection

- Workload-specific signals and threat alerts
- Deterministic, AI, and anomaly-based detection mechanisms
- Leverages the power of Microsoft Threat Intelligence with 24 trillion signals daily

Detect threats and  
protect your  
workloads

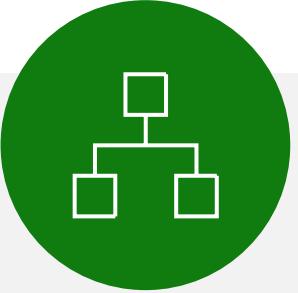


# Threat protection for all layers of the cloud and on-prem



## 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



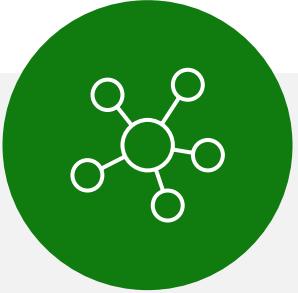
## Leading threat intelligence

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



## Vulnerability management

Identify and remediate vulnerabilities before they are exploited

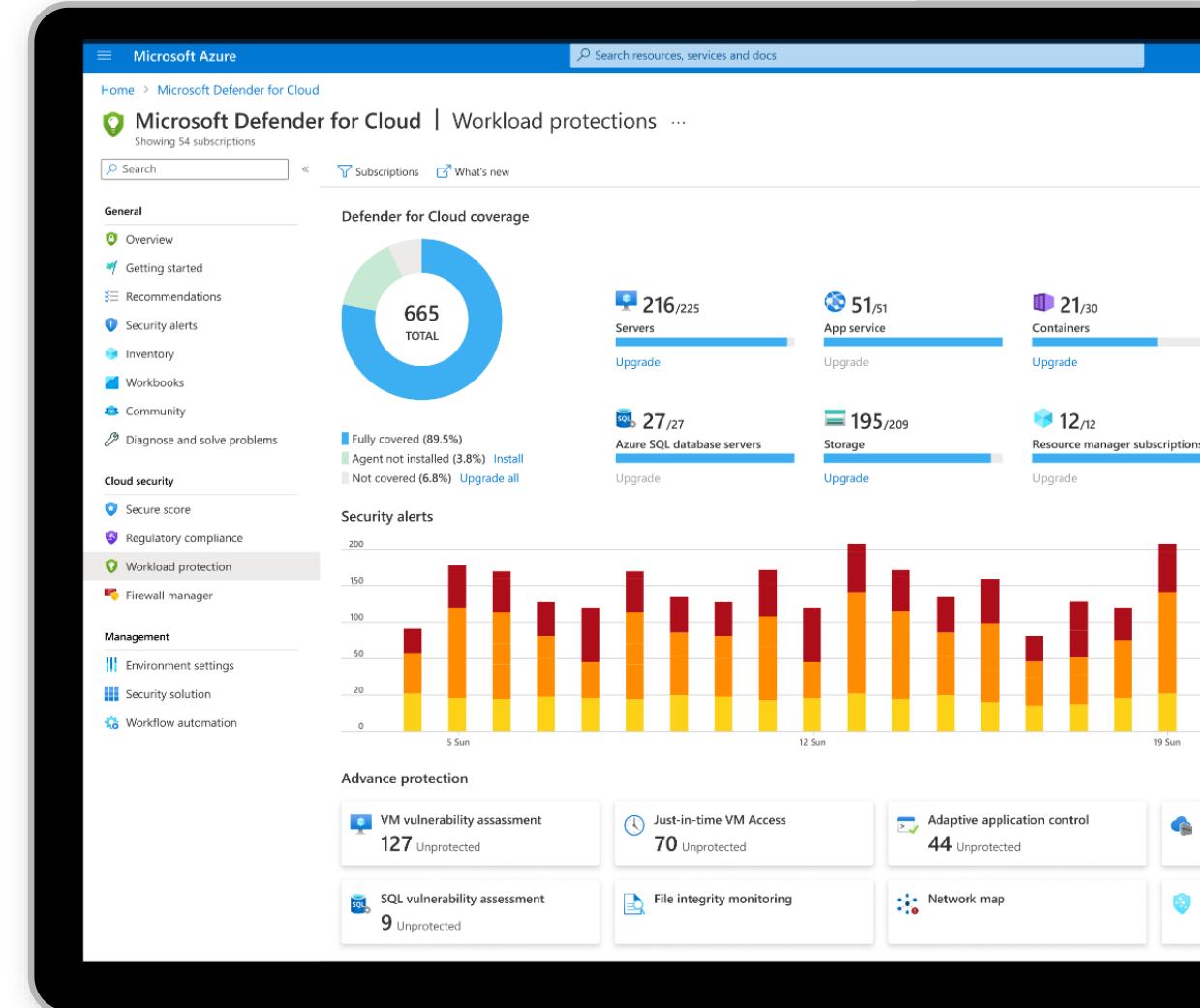


## Alert correlation

Prioritize more easily with connected alerts that are grouped into incidents

# Protect your workloads in the cloud and on-premises

- Use detections that are built for the unique attack vectors of each resource type, built on the powerful insights of Microsoft Threat Intelligence
- Reduce your attack surface by continuously scanning workloads to identify and manage vulnerabilities
- Automatically protect new workloads as soon as they are deployed
- Integrate with your SIEM for easy management of incidents.



# Security alerts and incidents

- Use prioritized alerts when threats are detected on your resources.
- Investigate effectively with smart alert correlation that combines different alerts and low fidelity signals into security incidents.
- Manage incidents with a central view of attack campaigns and related alerts.

The screenshot shows a Microsoft Azure Defender for Cloud security alert for a suspected brute-force attack attempt. The alert is categorized as High Severity, Active, and occurred on 01/15/22. The alert description explains that brute-force attacks involve guessing valid credentials to gain access to a database. It advises taking safety measures like using strong passwords and AAD authentication. The affected resource is a SQL server named 'ninjaqlattack'. The MITRE ATT&CK® tactics section lists 'Pre-attack' under the 'Exploitation' category. The related entities section includes an account, Azure resource, host, and IP address (52.173.24.82) which includes geo and threat intelligence. The IP is associated with the United States, Des Moines city, and a source port.

Microsoft Azure

Home > Microsoft Defender for Cloud >

Security alert

251759991583999999\_02ebccf5-12d3-4cb7-a802-3a0acb50a355

Suspected brute-force attack attempt

High Severity

Active Status

01/15/22, 0... Activity time

Alert description

Brute-force attack is a common attack technique for finding valid credentials to the database. By submitting many users/passwords combinations, an attacker can guess a correct one. Once obtained, an attacker can have full access to the database. While this specific alert doesn't indicate a successful brute-force, it is advised to take safety measures to protect your resource against this attack. To investigate this suspected brute-force attempt, review its origin (based on the application name and IP/Location), and try to find out whether it's recognized to you, or suspicious. If you believe this to be an attack on your database, use firewall rules to limit the access to your resource, and make sure you use strong passwords and not well known user names. Also, consider using only AAD authentication to further enhance your security posture.

Affected resource

ninjaqlattack SQL server

CyberSecSOC Subscription

MITRE ATT&CK® tactics

- Pre-attack

Related entities

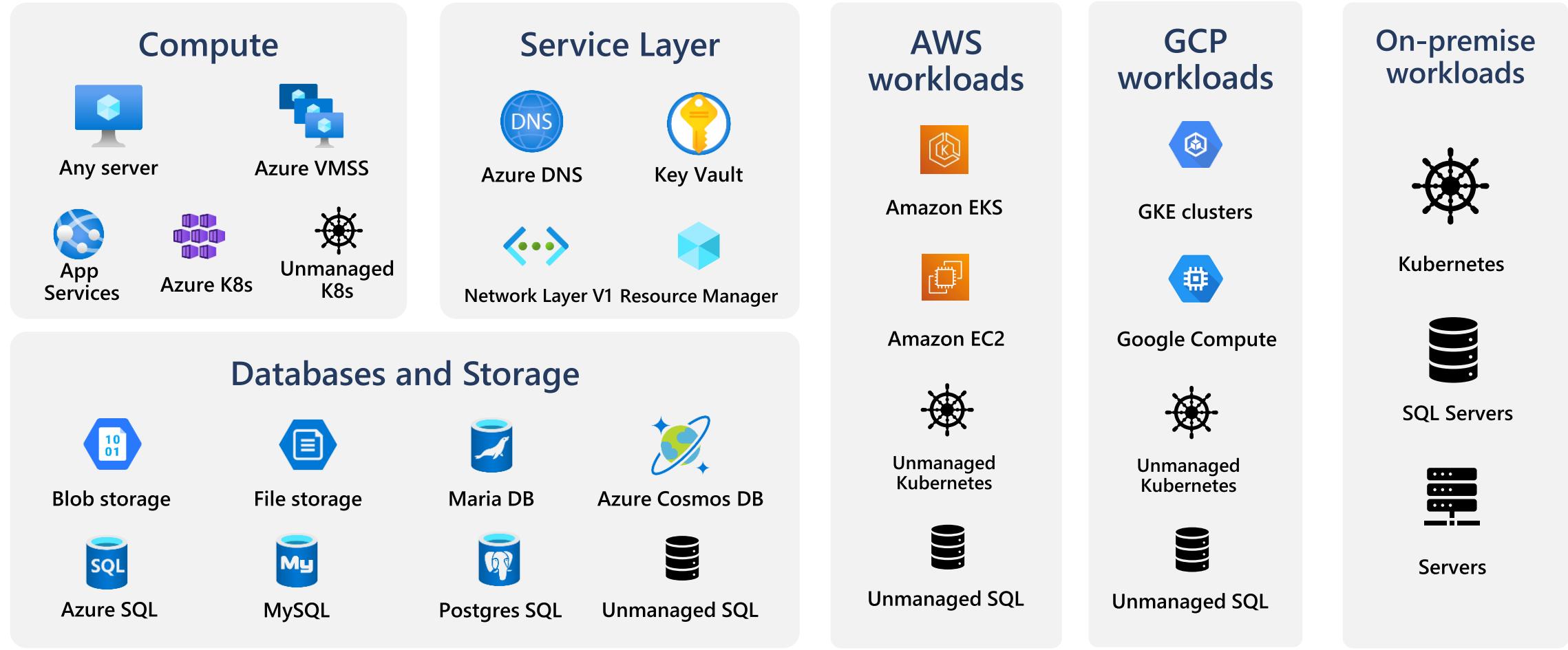
- Account (1)
- Azure resource (1)
- Host (1)
- IP (1) Includes Geo & Threat Intelligence

Address	State	City
52.173.24.82	united states	des moines

Network connection (1)

Source IP	Source port	Destin...

# Full-stack coverage with dedicated detections



On-premise



Protect your VMs

# Server security in the cloud is different

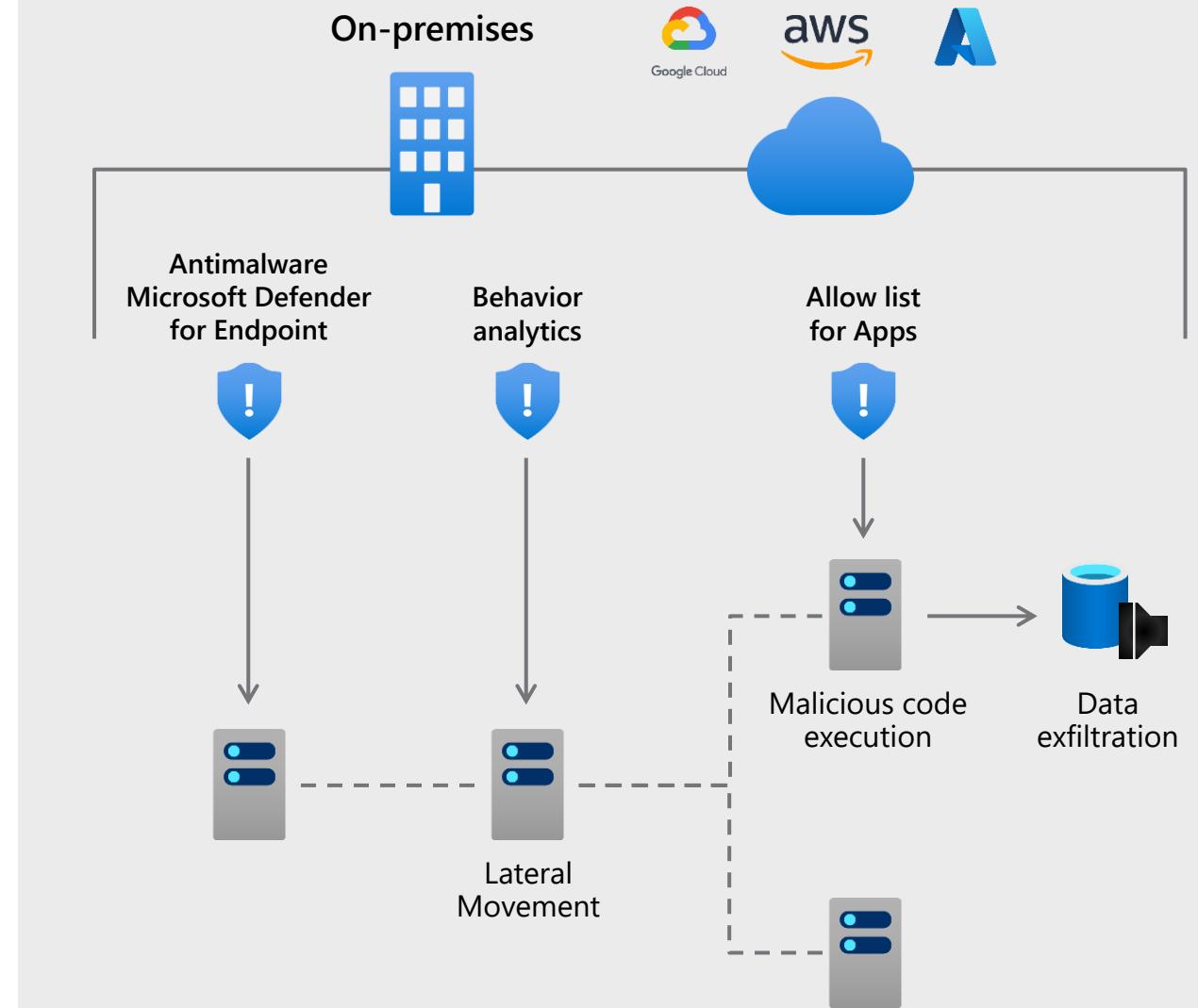
- Running VMs in the cloud requires an additional layer of security to protect the control plane surrounding your servers
- Threat detections need to extend to connected, cloud-native components including network, storage, and the control plane to fully assess and protect the security state of your servers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



# Microsoft Defender for Servers

Protect your servers from threats

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



# Microsoft Defender for Servers

Protect machines in hybrid and multi-cloud environments



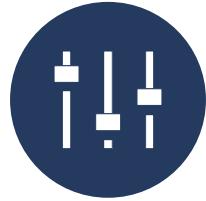
## Multicloud support

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



## Leading EDR solution

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



## Optimized for Cloud environments

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

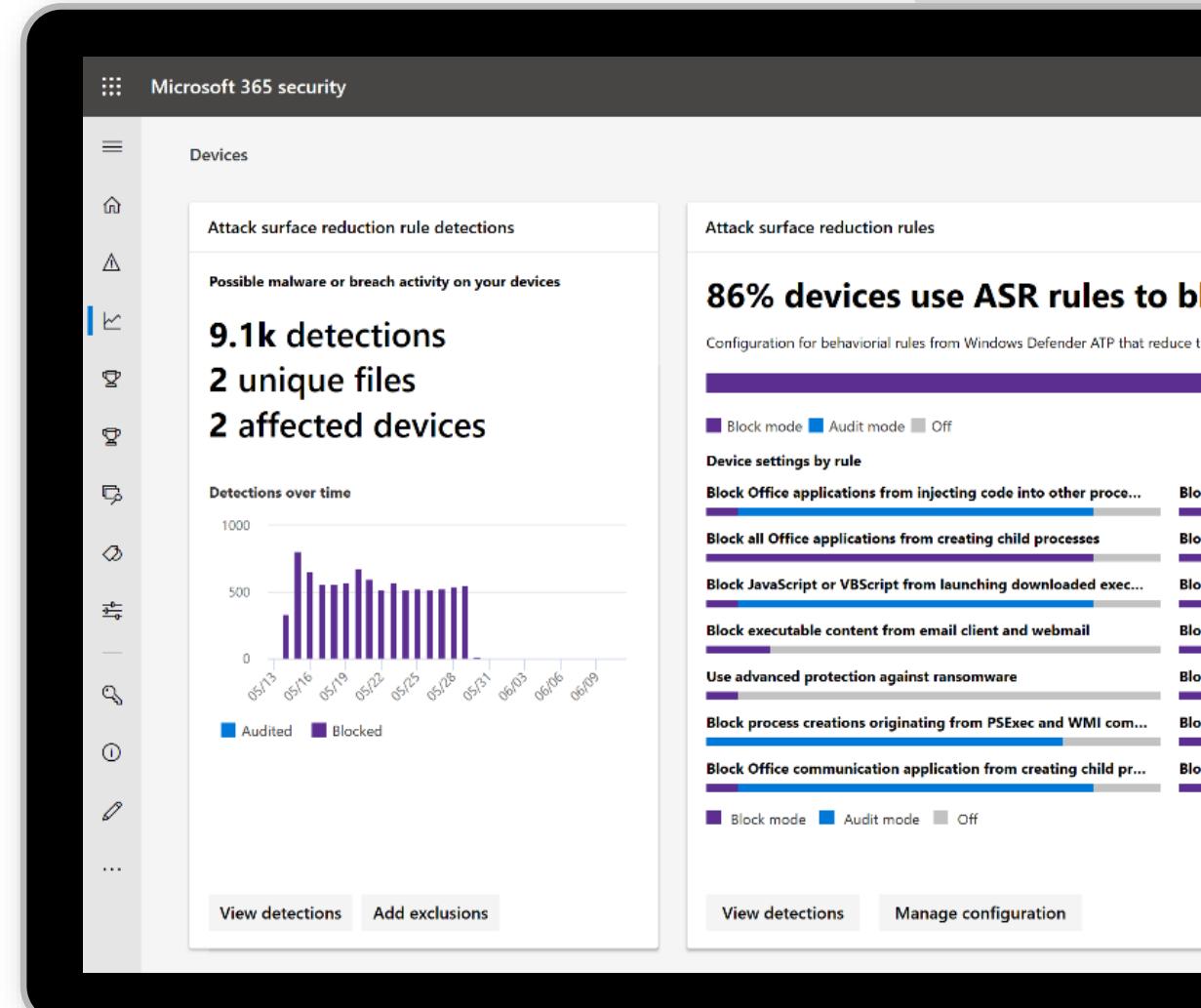


# Attack surface reduction

Powered by Microsoft Defender for Endpoint

Eliminate risks by reducing the surface area of attack

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

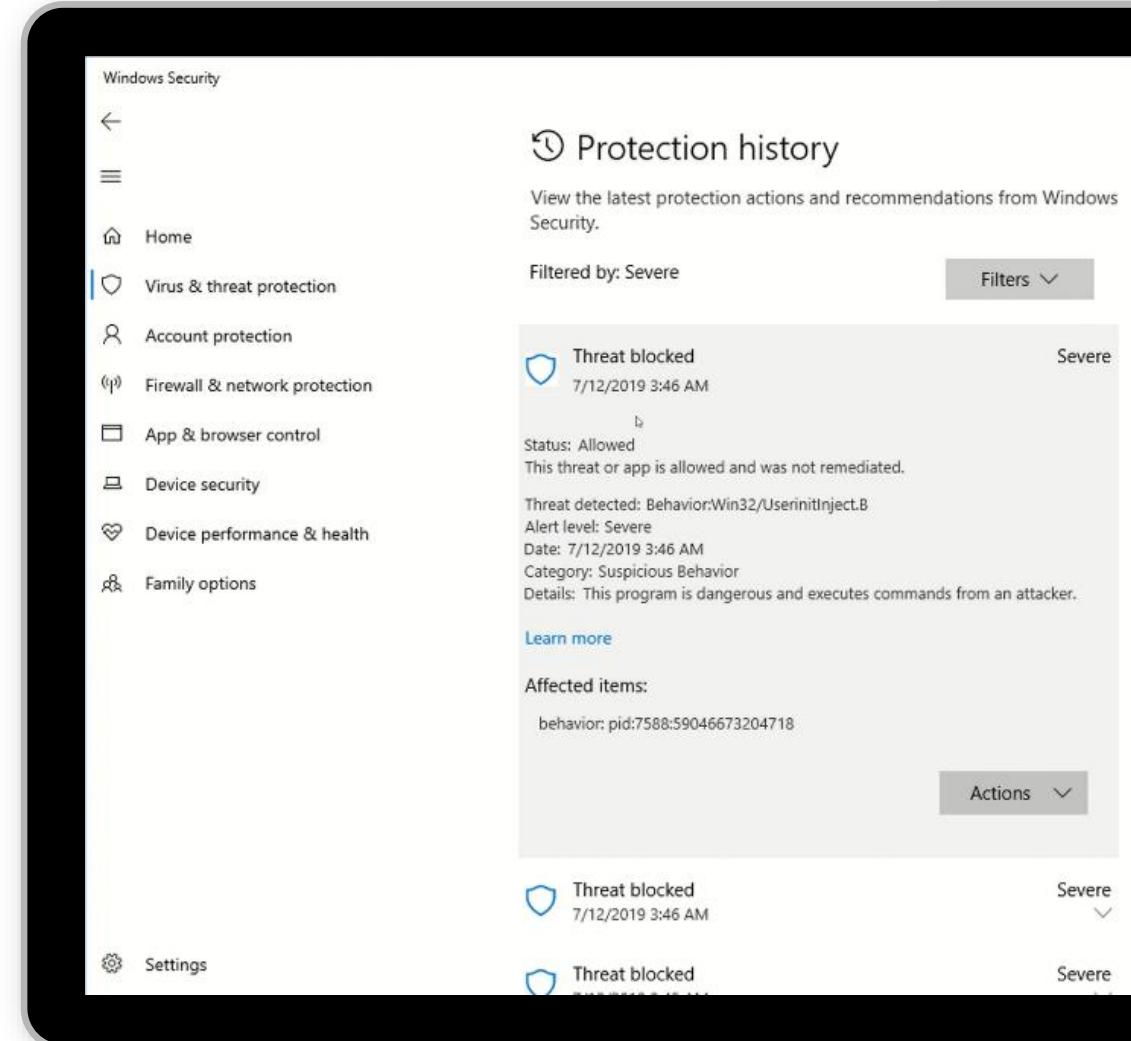


# Next generation antivirus protection

Powered by Microsoft Defender for Endpoint

Blocks and tackles sophisticated threats and malware

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

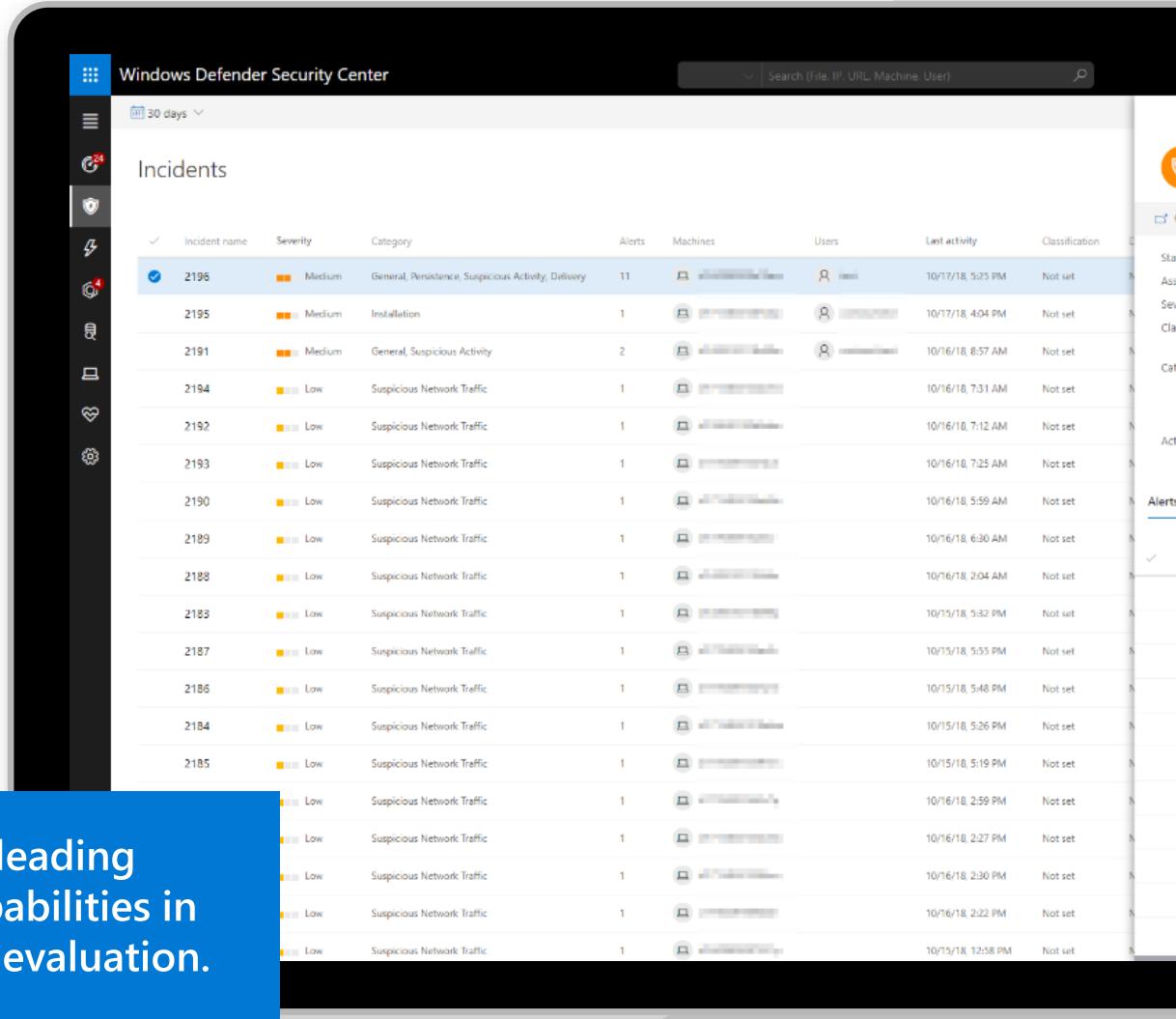


# Endpoint detection & response

Powered by Microsoft Defender for Endpoint

Detect and investigate advanced persistent attacks

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



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 detected events. The columns in the table are: Incident name, Severity, Category, Alerts, Machines, Users, Last activity, and Classification. The table lists multiple incidents, mostly categorized as "Suspicious Network Traffic" or "General, Suspicious Activity". Each row includes a checkbox, a severity color indicator (orange for Medium, yellow for Low), and a timestamp for the last activity.

Incident name	Severity	Category	Alerts	Machines	Users	Last activity	Classification
2196	Medium	General, Persistence, Suspicious Activity, Delivery	11	[redacted]	[redacted]	10/17/18, 5:25 PM	Not set
2195	Medium	Installation	1	[redacted]	[redacted]	10/17/18, 4:04 PM	Not set
2191	Medium	General, Suspicious Activity	2	[redacted]	[redacted]	10/16/18, 8:57 AM	Not set
2194	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 7:31 AM	Not set
2192	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 7:12 AM	Not set
2193	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 7:25 AM	Not set
2190	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 5:59 AM	Not set
2189	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 6:30 AM	Not set
2188	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 2:04 AM	Not set
2183	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 5:32 PM	Not set
2187	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 5:55 PM	Not set
2186	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 5:46 PM	Not set
2184	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 5:26 PM	Not set
2185	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 5:19 PM	Not set
	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 2:59 PM	Not set
	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 2:27 PM	Not set
	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 2:30 PM	Not set
	Low	Suspicious Network Traffic	1	[redacted]		10/16/18, 2:22 PM	Not set
	Low	Suspicious Network Traffic	1	[redacted]		10/15/18, 12:58 PM	Not set



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 organizational policies, and increase oversight of apps that access sensitive data

The screenshot shows a Microsoft Azure dashboard titled "Vulnerabilities in your virtual machines should be remediated". Key details include:

- Severity: Low
- Freshness interval: 4 Hours
- Tactics and techniques: Initial Access +5

Under "Description", it states: "Monitors for vulnerability findings on your virtual machines as were discovered by the built-in vulnerability assessment solution of Azure Security Center (powered by Qualys)."

Under "Related recommendations (1)", there is one item: "A vulnerability assessment solution should be enabled on your virtual machines". It includes columns for "Prerequisite" and "Affected resources", with "41 of 58" listed.

Under "Remediation steps", there is a link to "A vulnerability assessment solution should be enabled on your virtual machines".

Under "Affected resources", there is a table with columns: ID, Security check, Category, and Application. The table lists several items, such as "EOL/Obsolete Operating System: Ubuntu 16.04 Detected" under "Security Policy" and "Microsoft Internet Explorer Security Update for September 2020" under "Internet Explorer".

Under "Security checks", there are tabs for "Findings" and "Disabled findings". A search bar is present above the table.

At the bottom, there are buttons for "Trigger logic app" and "Exempt".

# Asses 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, including severity (Low), freshness interval (4 Hours), and tactics and techniques (Initial Access +5). It includes sections for Description, Related recommendations, Remediation steps, Affected resources, and Security checks. A detailed table of findings is shown, with the first few rows listed below:

ID	Security check	Category	Applied
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 Microsoft Azure Defender for Cloud interface. The top navigation bar includes 'Microsoft Azure', a search bar, and a 'Home' link. Below the navigation, a breadcrumb trail shows 'Home > Microsoft Defender for Cloud > A vulnerability assessment solution should be enabled on your virtual machines'. The main title is 'Vulnerabilities in your virtual machines should be remediated'. Key metrics displayed are 'Severity: Low', 'Freshness interval: 4 Hours', and 'Tactics and techniques: Initial Access +5'. The page content includes sections for 'Description', 'Related recommendations (1)', 'Remediation steps', 'Affected resources', and 'Security checks'. Under 'Security checks', there is a table with columns 'ID', 'Security check', 'Category', and 'Applies to'. The table lists several findings, such as 'EOL/Obsolete Operating System: Ubuntu 16.04 Detected' (Security Policy, 2 of 13), 'Microsoft Internet Explorer Security Update for September 2020' (Internet Explorer, 2 of 13), and various Windows and Debian security updates.

ID	Security check	Category	Applies to
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

# 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 Microsoft Azure Defender for Cloud interface. The top navigation bar includes 'Microsoft Azure', a search bar, and a policy definition link. The main title is 'Vulnerabilities in your virtual machines should be remediated'. Below this, it displays 'Severity: Low', 'Freshness interval: 4 Hours', and 'Tactics and techniques: Initial Access +5'. The page is divided into sections: 'Description' (Monitors for vulnerability findings on your virtual machines as were discovered by the built-in vulnerability assessment solution of Azure Security Center (powered by Qualys)), 'Related recommendations (1)' (a single recommendation titled 'A vulnerability assessment solution should be enabled on your virtual machines'), 'Remediation steps' (a collapsed section), 'Affected resources' (a collapsed section), and 'Security checks' (a section with tabs for 'Findings' and 'Disabled findings'). Under 'Findings', there is a table with columns: ID, Security check, Category, and Applied. The table lists several items, such as 'EOL/Obsolete Operating System: Ubuntu 16.04 Detected' under 'Security Policy' and 'Microsoft Internet Explorer Security Update for September 2020' under 'Internet Explorer'. At the bottom, there are buttons for 'Trigger logic app' and 'Exempt'.

ID	Security check	Category	Applied
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

# 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 a Microsoft Azure interface for Microsoft Defender for Cloud. The main title is "Vulnerabilities in your virtual machines should be remediated". Key details include:

- Severity: Low
- Freshness interval: 4 Hours
- Tactics and techniques: Initial Access +5

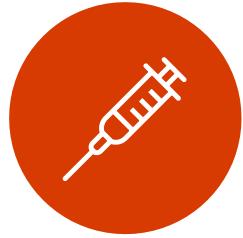
Below this, there are sections for:

- Description: Monitors for vulnerability findings on your virtual machines as were discovered by the built-in vulnerability assessment solution of Azure Security Center (powered by Qualys).
- Related recommendations (1): A vulnerability assessment solution should be enabled on your virtual machines.
- Remediation steps: A link to the recommendation.
- Affected resources: A table showing 41 of 58 affected resources.
- Security checks: A table showing findings and disabled findings.

ID	Security check	Category	Applied
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

At the bottom, there are buttons for "Trigger logic app" and "Exempt".

# VM threat detection categories



Ransomware

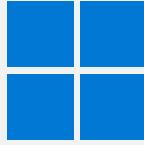


Threat intelligence



Brute force

# Supported operating systems



Windows Server 2012 R2

Windows Server 2016

Windows Server, version 1803 or later

Windows Server 2019

Windows Server 2022



Red Hat Enterprise Linux 7.2+

Red Hat Enterprise Linux 8.x

CentOS 7.2+, 8

Ubuntu 16.04, 18.04, 20.04

SUSE Linux Enterprise Server 12, 15

Oracle Linux 7.2 or higher

Oracle Linux 8.x

Amazon Linux 2

# Feature comparison

Feature	Defender for Servers P1 (\$5)*	Defender for Servers P2 (\$15)*
Hardening recommendations	✓	✓
Asset discovery	✓	✓
Vulnerability assessment using Microsoft Threat & Vulnerability Management	✓	✓
Attack surface reduction	✓	✓
Next generation antivirus protection	✓	✓
Endpoint detection & response	✓	✓
Automated self-healing	✓	✓
Log-analytics (500MB free)		✓
Regulatory compliance assessment		✓
Vulnerability assessment using Qualys		✓
Network layer threat detection		✓ *
Adaptive application controls		✓
File integrity monitoring		✓ *
Just-in-time VM access for management ports		✓ *
Adaptive network hardening		✓

\* Currently Azure-only

# Onboarding

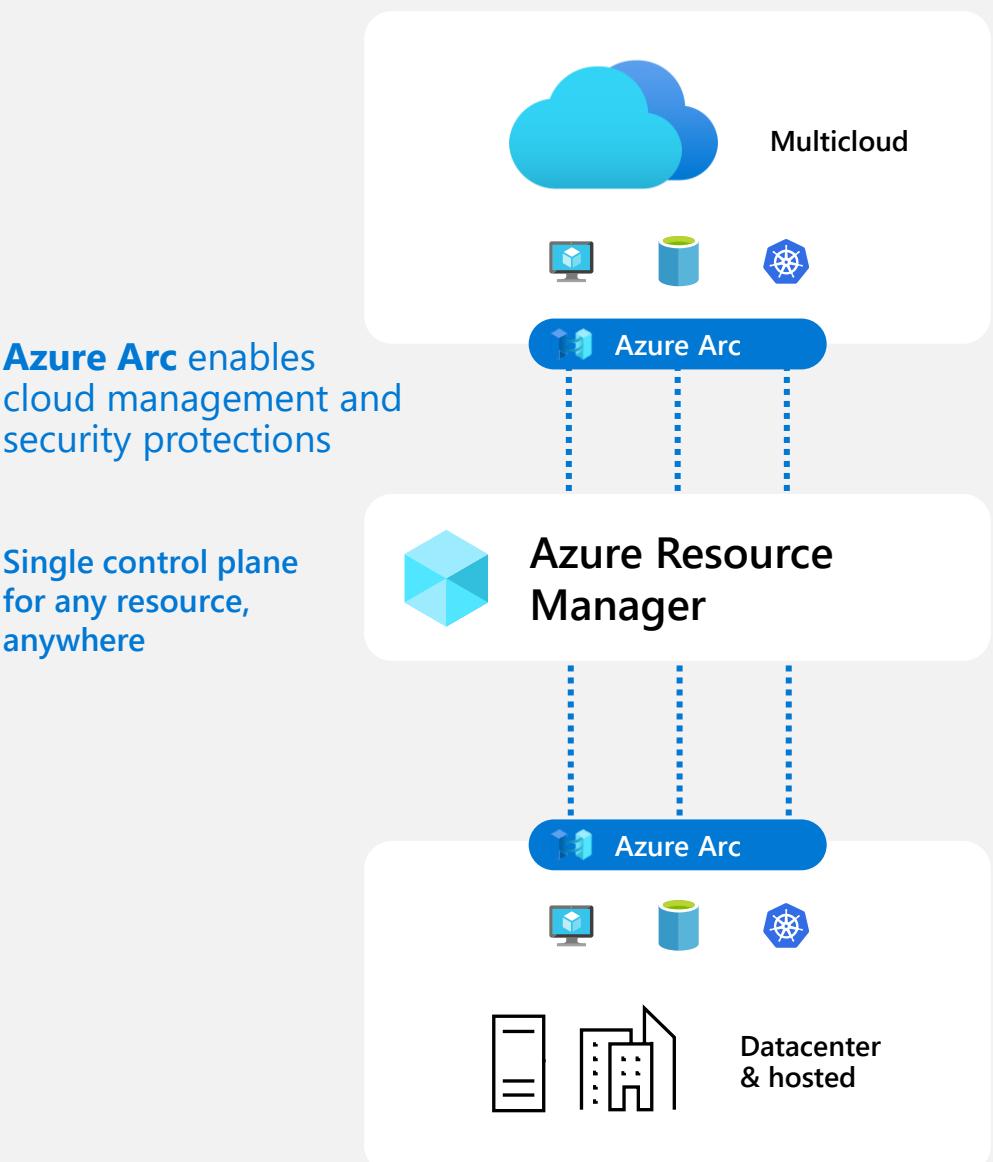
- Enable Defender for Servers P1 or P2 in the Azure Portal (one-click)
- Install the Azure Arc agent to on-prem and non-Azure cloud servers
- MDE will be automatically provisioned- via the MDE.Windows & MDE.Linux extensions
- On-premise servers are now onboarded to Defender for Cloud and Defender for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

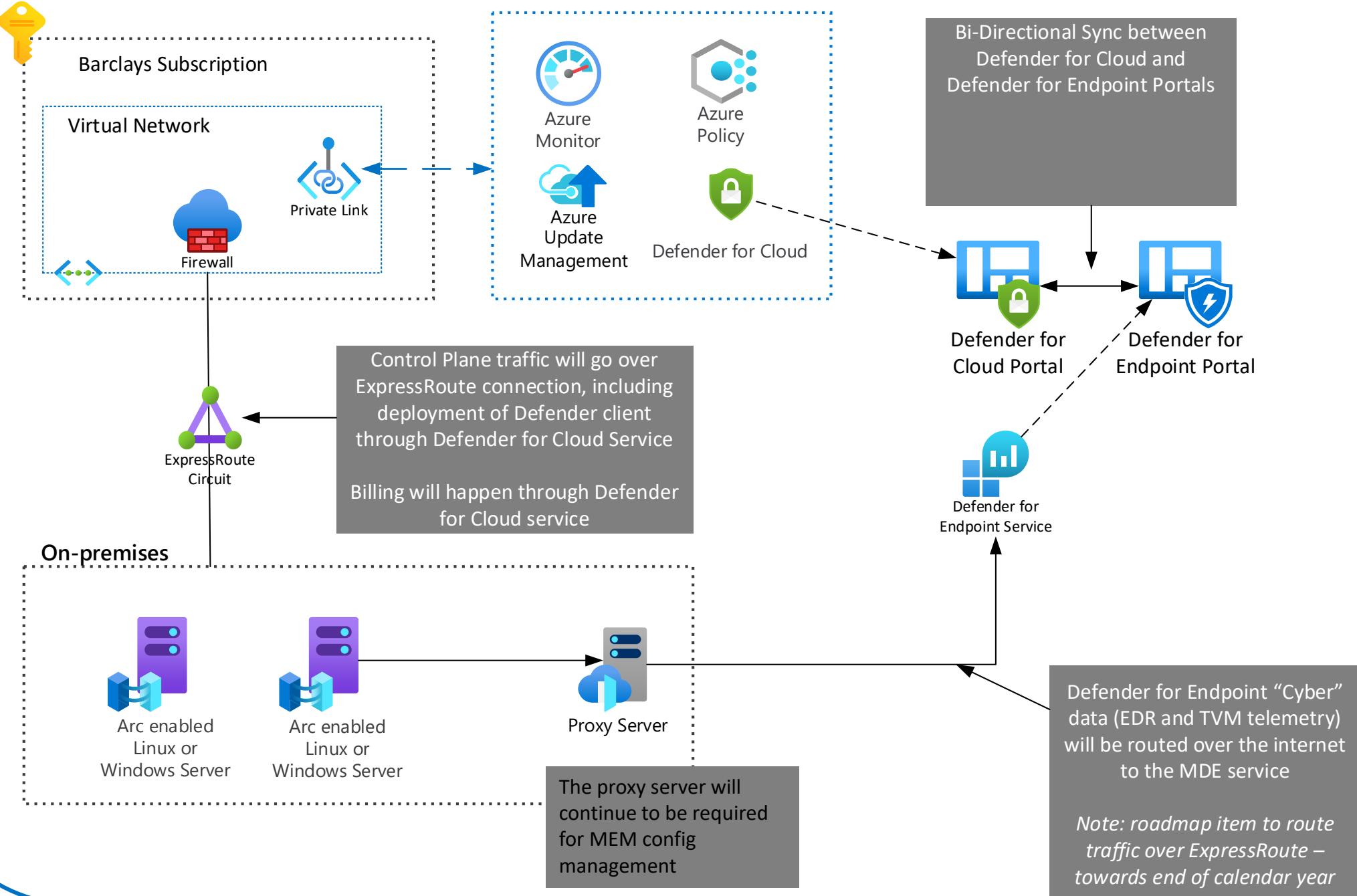
1. Server onboards to Azure Arc (the server is then discoverable by Defender for Servers)
2. Then Defender for Servers automatically provisions MDE to this server as an extension
3. Defender for Endpoint capabilities are now available on the server



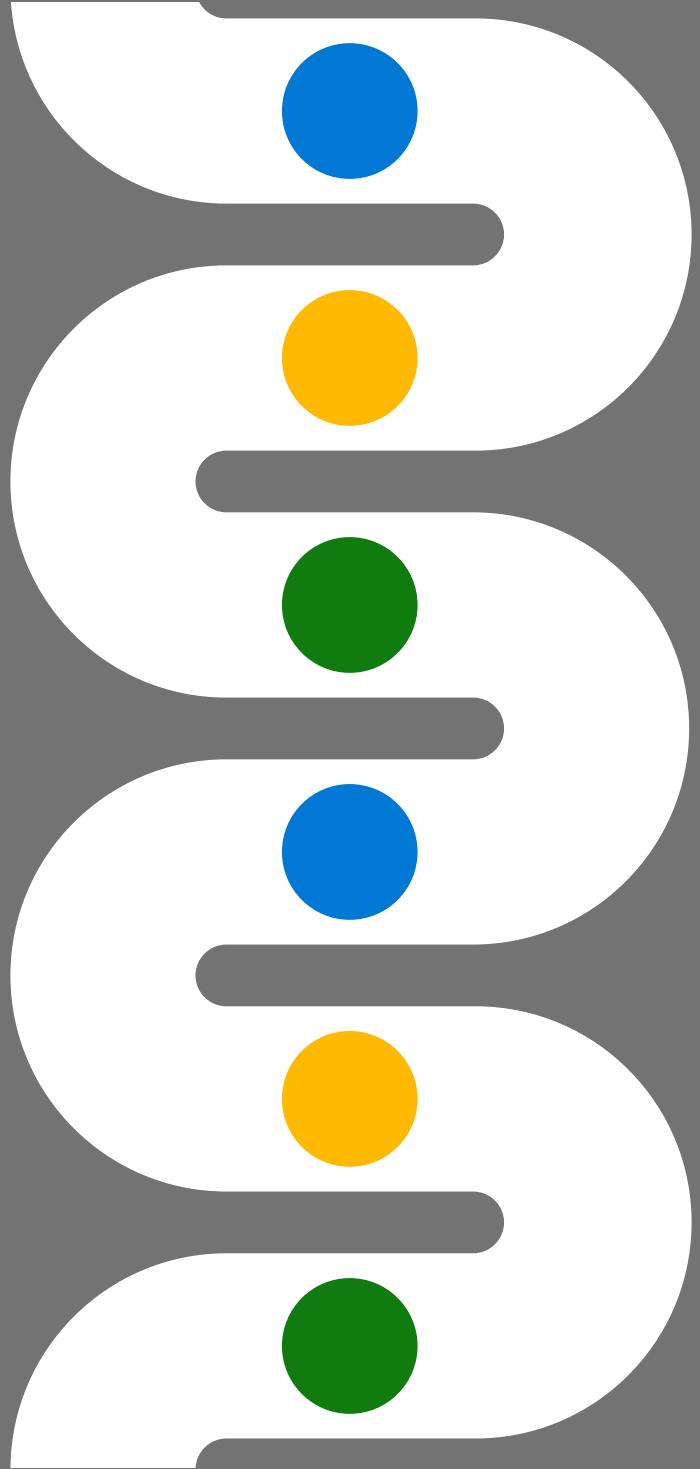
# Use Azure Arc to connect workloads anywhere to Microsoft Defender for Cloud

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





Protect your  
containers



# Container security challenges



Containerized applications are elastic,  
spawn and re-size rapidly

Images are immutable, containers  
are short lived

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



Visibility of containers traffic flows are  
difficult to track with traditional tools

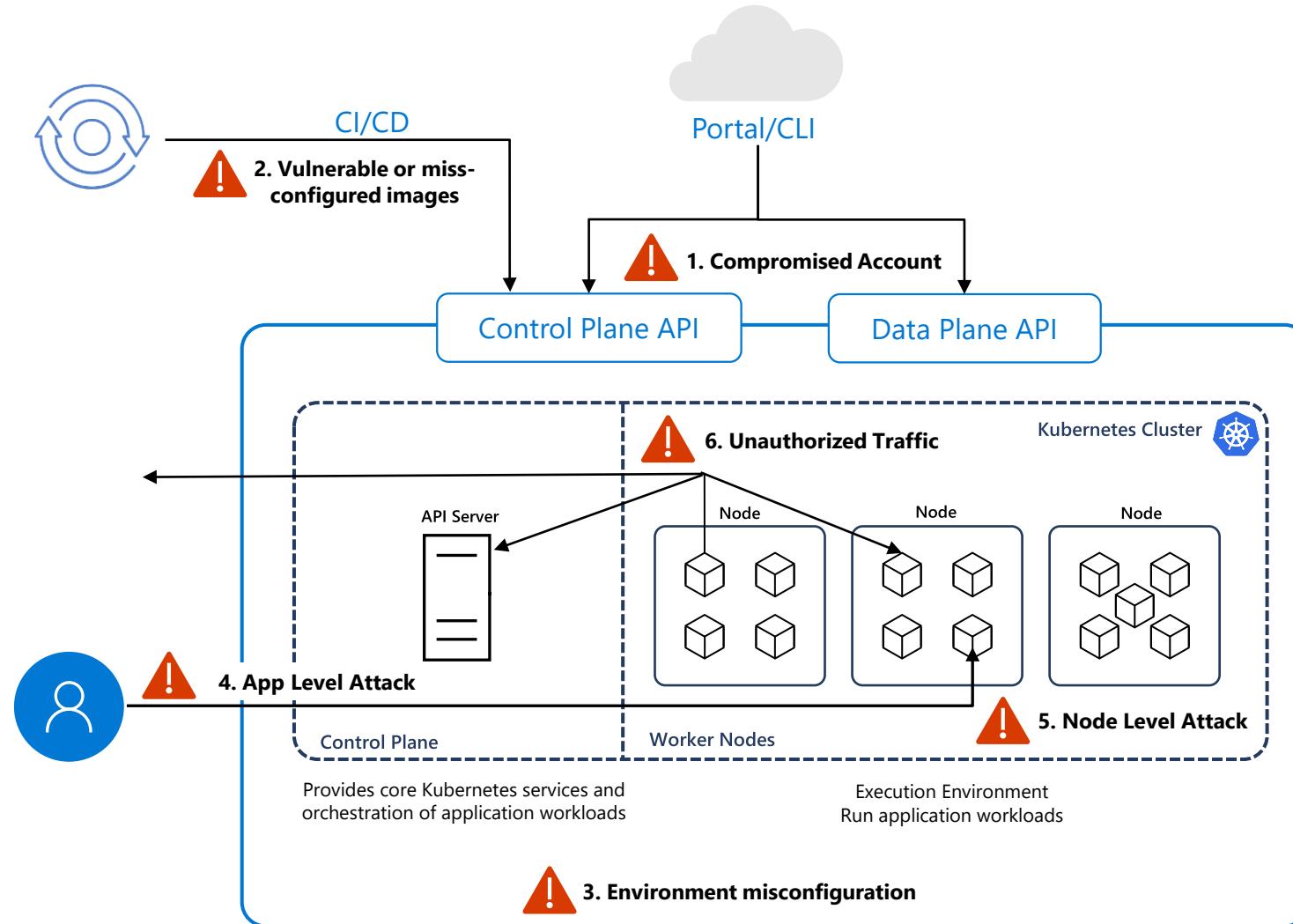
Complex runtime environment, with different  
configuration layers and options

» **94%** orgs experienced at least one security  
incident in their Kubernetes environments  
during 2021<sup>2</sup>

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

<sup>2</sup> State of Kubernetes Security Report 2021

# Threat Landscape for managed Kubernetes



## Common attack techniques

- Abuse over permissive roles\SA
- Exploit vulnerable images
- Deploy backdoor containers
- Access exposed applications
- Escape to the host

# Microsoft Defender for Containers

Protect multi-cloud and hybrid container deployments



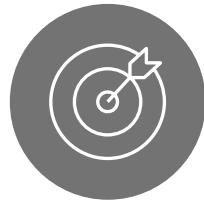
## Hardening

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



## Vulnerability management

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



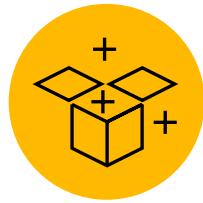
## Advanced threat detection

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



# Hardening

## Secure Score

- Understand the bottom line of your security posture
- Prioritized view of containerized assets' security posture

## Control plane recommendations

- Harden and audit according to Azure Security Benchmarks
- Follow Docker CIS benchmark on container nodes

## Date plane recommendations

- Audit or enforce K8s workloads security best practices

The screenshot shows a policy detail page for 'Role-Based Access Control should be used on Kubernetes Services'. It includes sections for Severity (High), Freshness interval (30 Min), Tactics and techniques (Privilege Escalation), and Affected resources (listing multiple clusters like norbcazahi, norbacenabled, new-kubernetes-demo, new-k8s-demo, new-k8s-cluster, and asclab-aks). A search bar at the top allows filtering by cluster name.

The screenshot shows a recommendation titled 'Container images should be deployed from trusted registries only'. It has a 'Deny' status button. The 'Affected Components' section lists various pods across different clusters. The main body of the card provides a description about running images from known registries and includes an 'Additional Information' section with configuration steps and a 'Remediation steps' section with manual remediation instructions. Buttons at the bottom allow taking action or triggering a logic app.

# Vulnerability management

## Zero configuration

- Automatic discovery and onboarding of ACR

## Ship

- Scan triggered on image push, pull, and import
- Birdseye view for all registry vulnerabilities

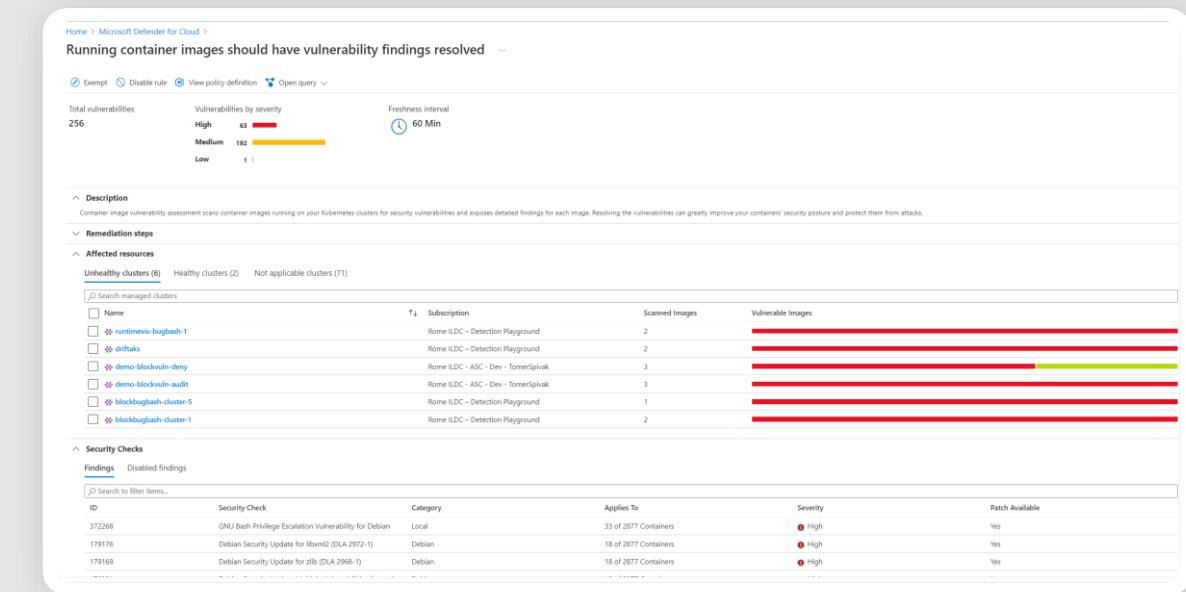
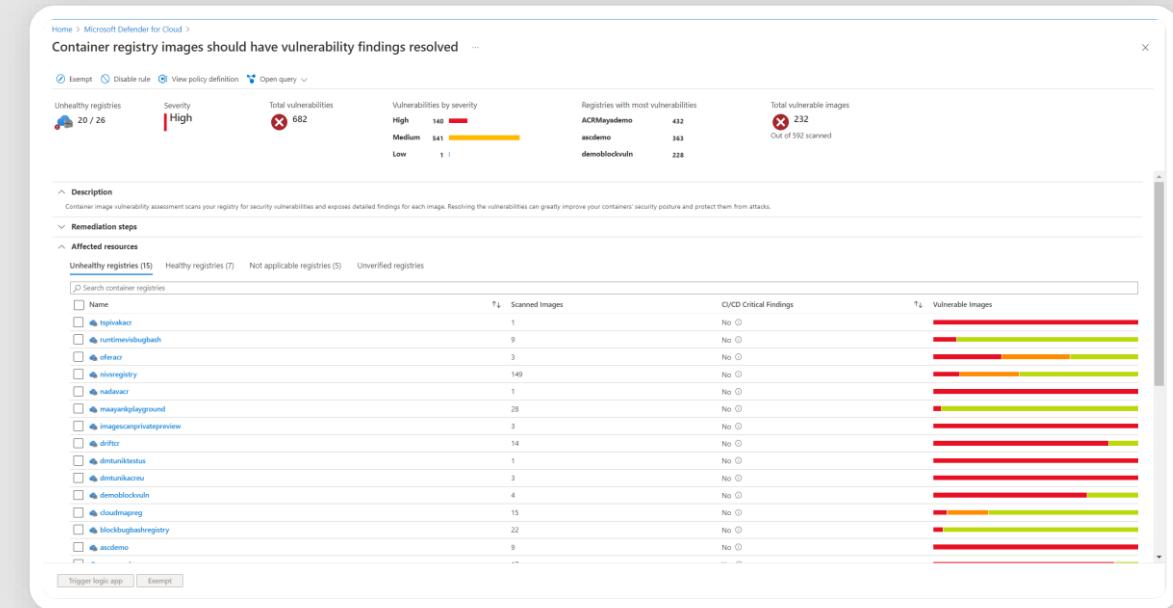
## Runtime

- Continuous scanning of running images
- Visibility of running images with vulnerabilities

## Build

Coming soon

- Scan your images as part of your CI/CD pipeline



# Advanced threat detection

## Rich detection suite

- Control plane and workload level detections
- Deterministic, AI, and anomaly-based alerts to identify threats

## Leading threat intelligence

- Microsoft's global threat intelligence with honeypot networks, research malware feeds, in addition to memory forensic techniques to identify fileless attacks

## Understand risk and context

- Prioritized alerts mapped to MITRE ATT&CK® tactics to easily understand the Kubernetes context, effect across the attack lifecycle and to identify response action

## Automate response

New!

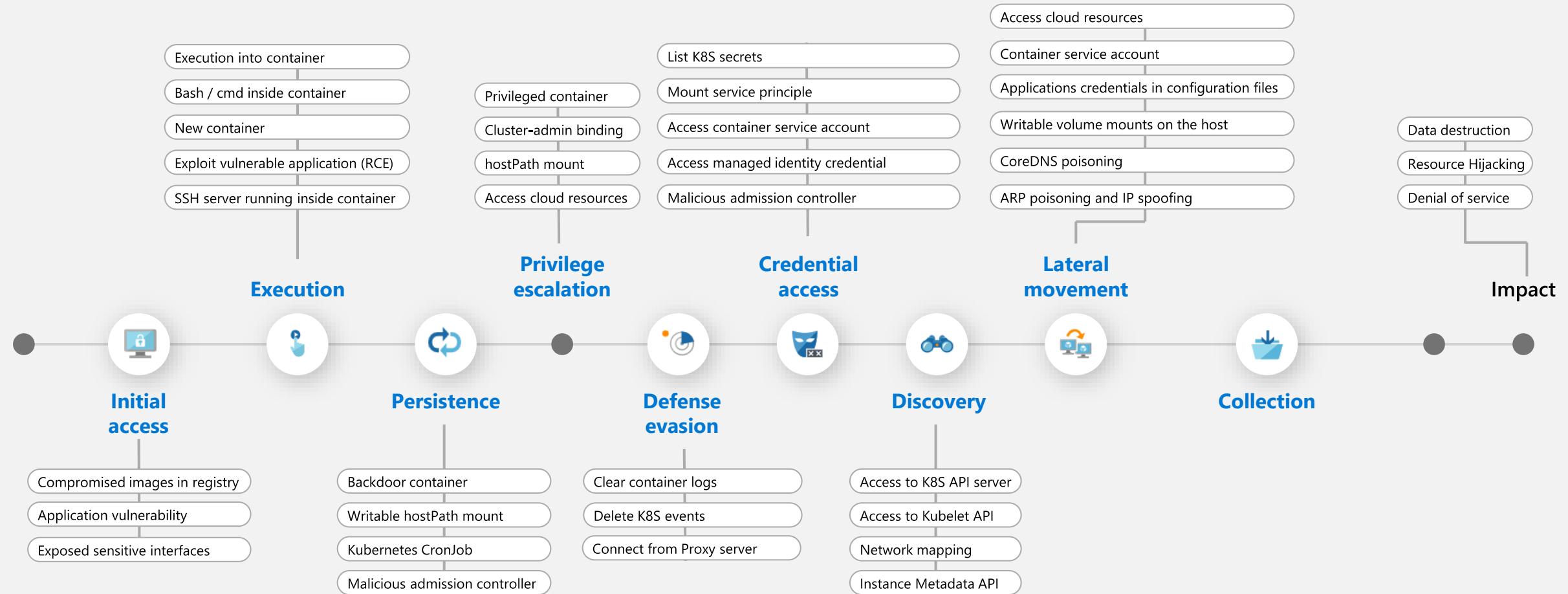
- Automate actions with tools of your choice: SIEM integration, email notifications, workflow automations and continues export

The screenshot shows a detailed view of a security alert in Microsoft Defender for Cloud. The alert is titled "Security alert" and describes "Digital currency mining related behavior detected". It is categorized as "High Severity" and "Active". The activity time is listed as "04/11/22, ...". The alert description states: "Analysis of processes running within a container detected the execution of a process or command normally associated with digital currency mining." Below this, the "Affected resource" section lists "new-K8s-demo" (Kubernetes service) and "ASC DEMO" (Subscription). The "MITRE ATT&CK® tactics" section shows "Execution" as the current tactic. The "Alert details" tab is selected, displaying information such as the Compromised Host (AKS-AGENTPOOL-10844301-VMSS00000), Suspicious Command Line (/bin/bash ./script.sh cryptonight-light POOL\_URL WA...), User Name (\_apt), Parent Process (sh), Account Session ID (0x1), Suspicious Process ID (0x4b44), Suspicious Process (/bin/bash), and ImageName (:). The "Related entities" section lists various Azure resources like Account, Azure resource, Container, Container Image, Container Registry, File, Host, Kubernetes Cluster, Kubernetes Namespace, Kubernetes Pod, Kubernetes Service Account, and Process. A table at the bottom provides a detailed list of processes with columns for Process ID, Command line, Creation time, Host, Parent process, Account, and File. The table shows two entries: 0x4b44 (command /bin/bash ./script.sh...) and 0x4b29 (command aks-agentpool-1084...).

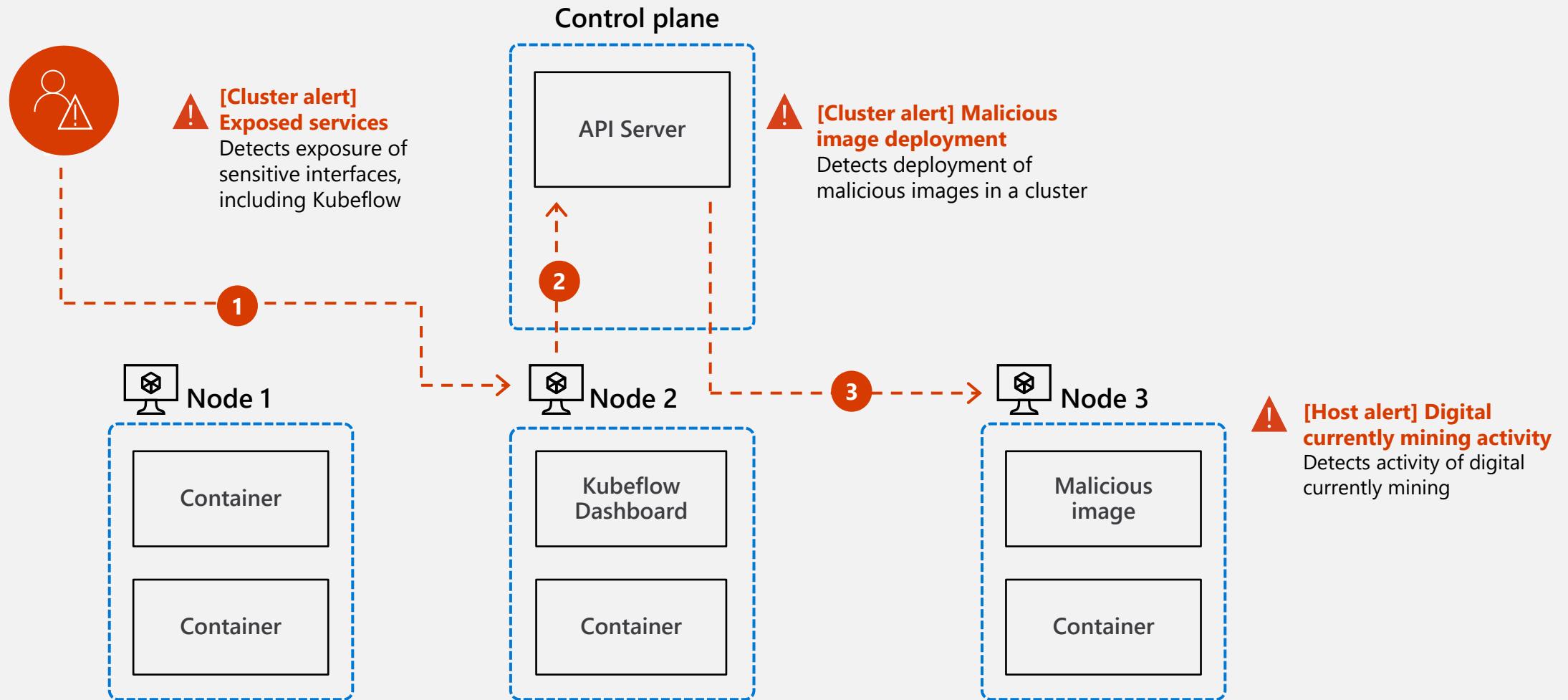
Process ID	Command line	Creation time	Host	Parent process	Account	File
0x4b44	/bin/bash ./script.sh...	Mon Apr 11 2022 20...	aks-agentpool-1084...	0x4b29	_apt	bash
0x4b29			aks-agentpool-1084...		sh	

Next: Take Action >>

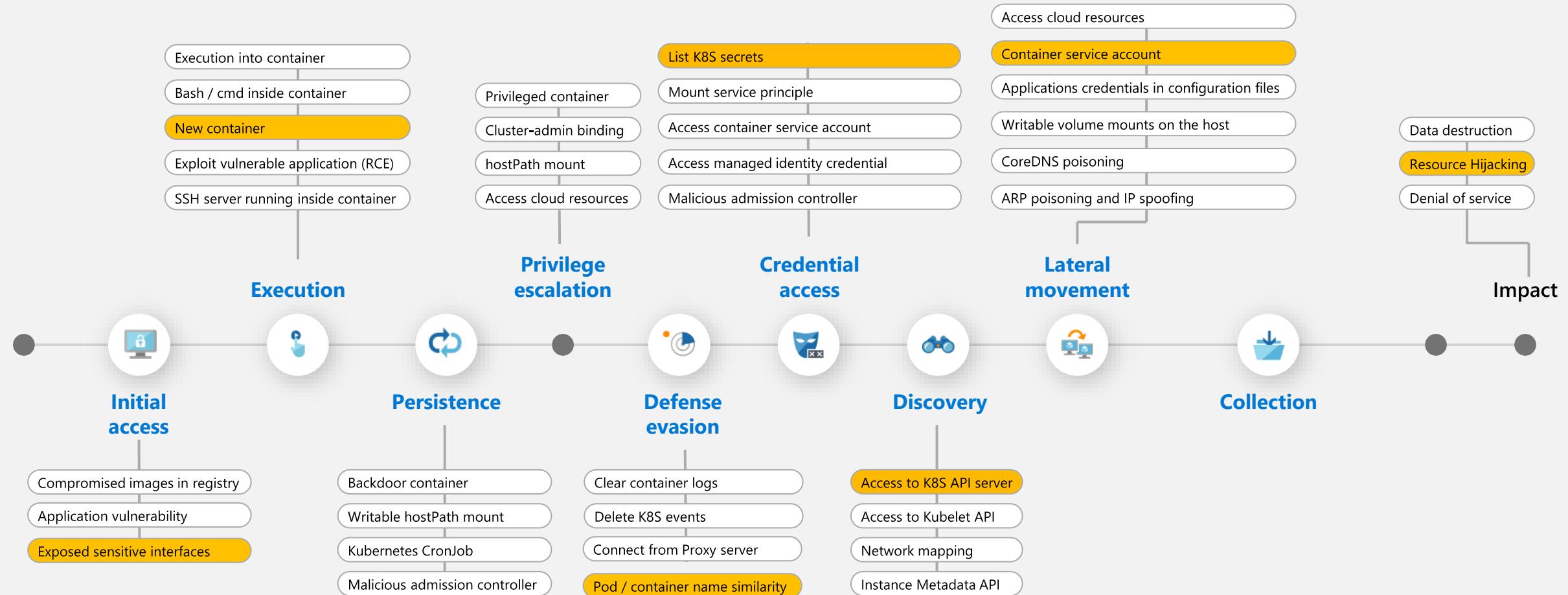
# Threat detections aligned to the Kubernetes Attack Matrix



# The attack flow: End-to-end container and host visibility

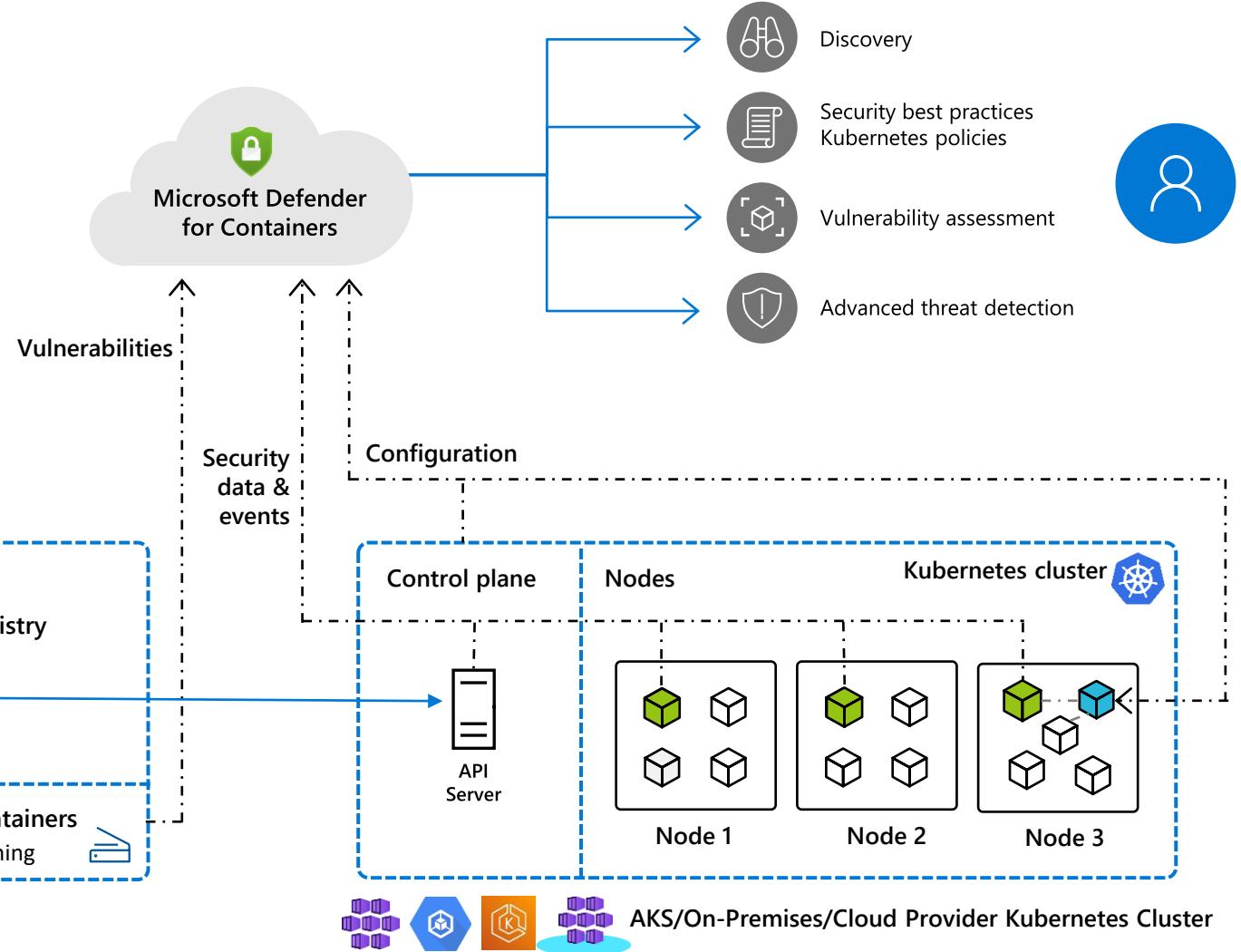


# Threat detections aligned to the K8s Attack Matrix



# Microsoft Defender for Containers

- Single pane of glass for Kubernetes security
- Built in Azure services - AKS and ACR
- Discovery of unprotected clusters
- Easy onboarding, at scale deployment
- built in security recommendation and alerts



**Protect your  
database  
workloads and  
storage instances**



# Protect databases and storage accounts



## Azure native security

Built into Azure with one-click enablement.



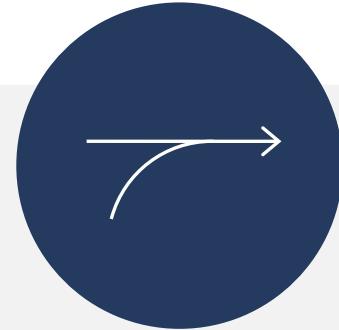
## Rich detection suite

Alerts specifically designed for threats targeted at databases and storage accounts



## Respond at scale

Reduce friction by preventing and responding to top threats first



## Centralized and integrated

Centralize security across all data assets and use the build in integration with Microsoft Sentinel & Azure Purview

# Protect your 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

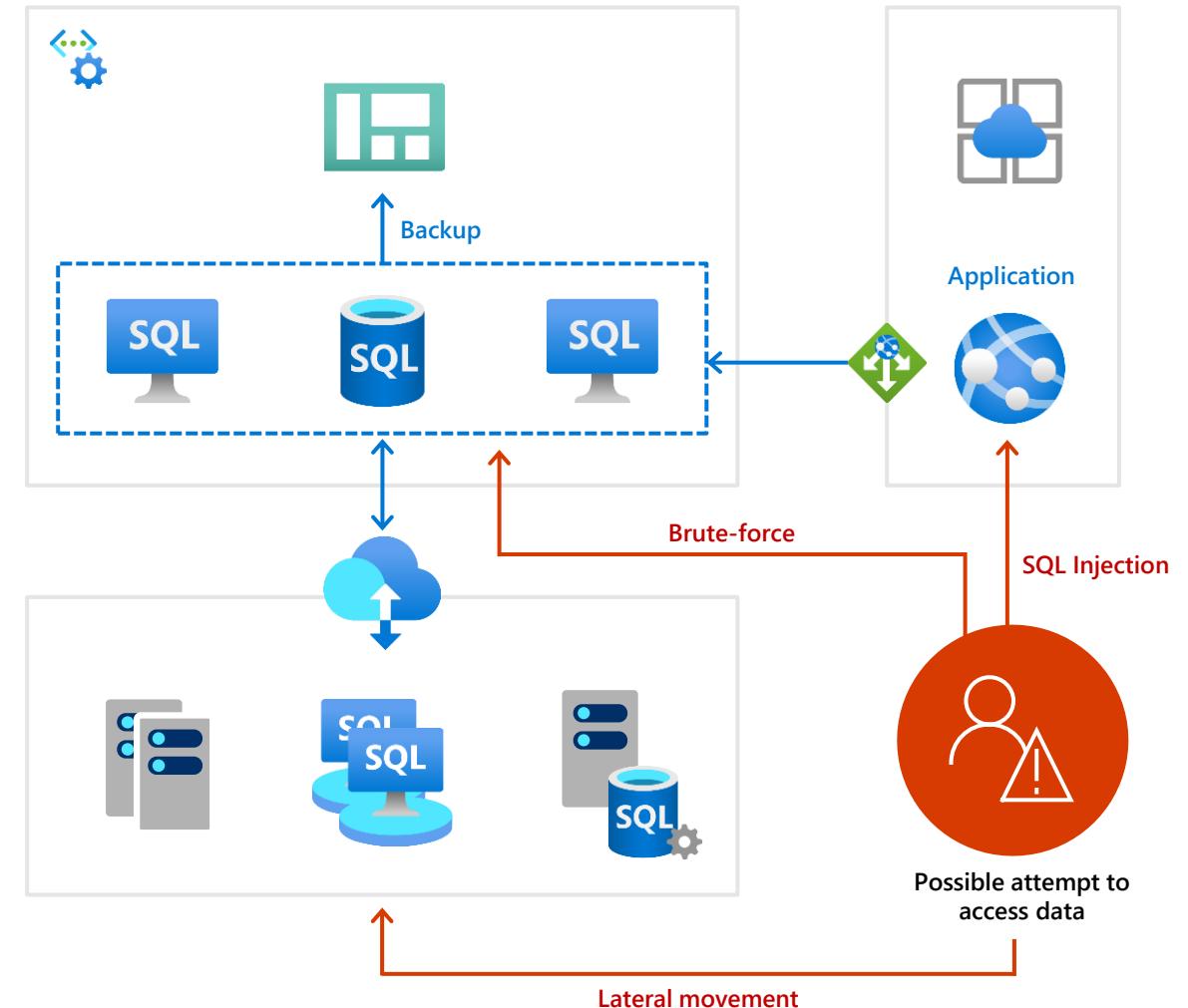
## Defender for Azure Cosmos DB



Azure Cosmos DB

# Common database threats

- ⚠️ SQL injection attacks
- ⚠️ Brute-force attacks
- ⚠️ Unusual data exfiltration
- ⚠️ Suspicious access or queries



# Database 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



# One-click enablement to protect your database estate

Microsoft Azure Search resources, services and docs Connie Wilson  
Home > Microsoft Defender for Cloud > 

**Settings | Defender plans**  ...  
ASC DEMO

Search (Cmd+ /) Save

**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) 
App Service	3 instances	\$15/Instance/Month 
Databases	Protected: 0/30 instances Preview features included	Selected: 0/4 
Storage	61 storage accounts	\$0.02/10k transactions 
Containers	13 kubernetes cores; 13 container registries	\$7/VM core/Month 
Key Vault	5 key vaults	\$0.02/10k transactions 

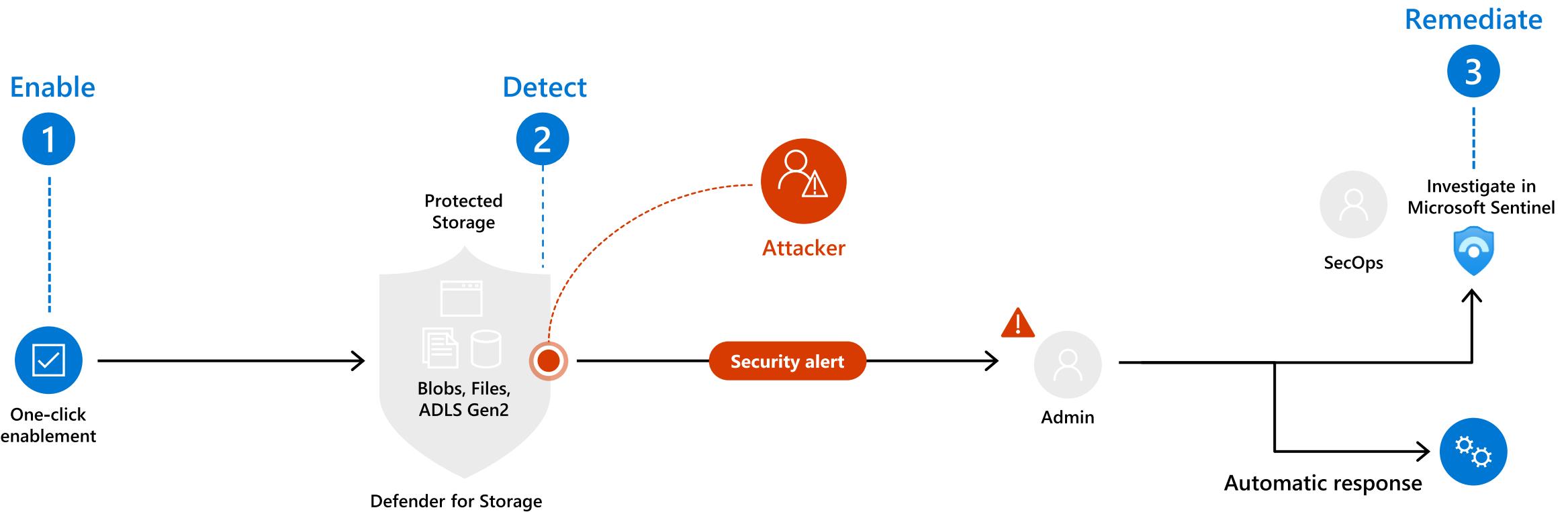
**Database types selection**

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](#)

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

# Microsoft Defender for Storage

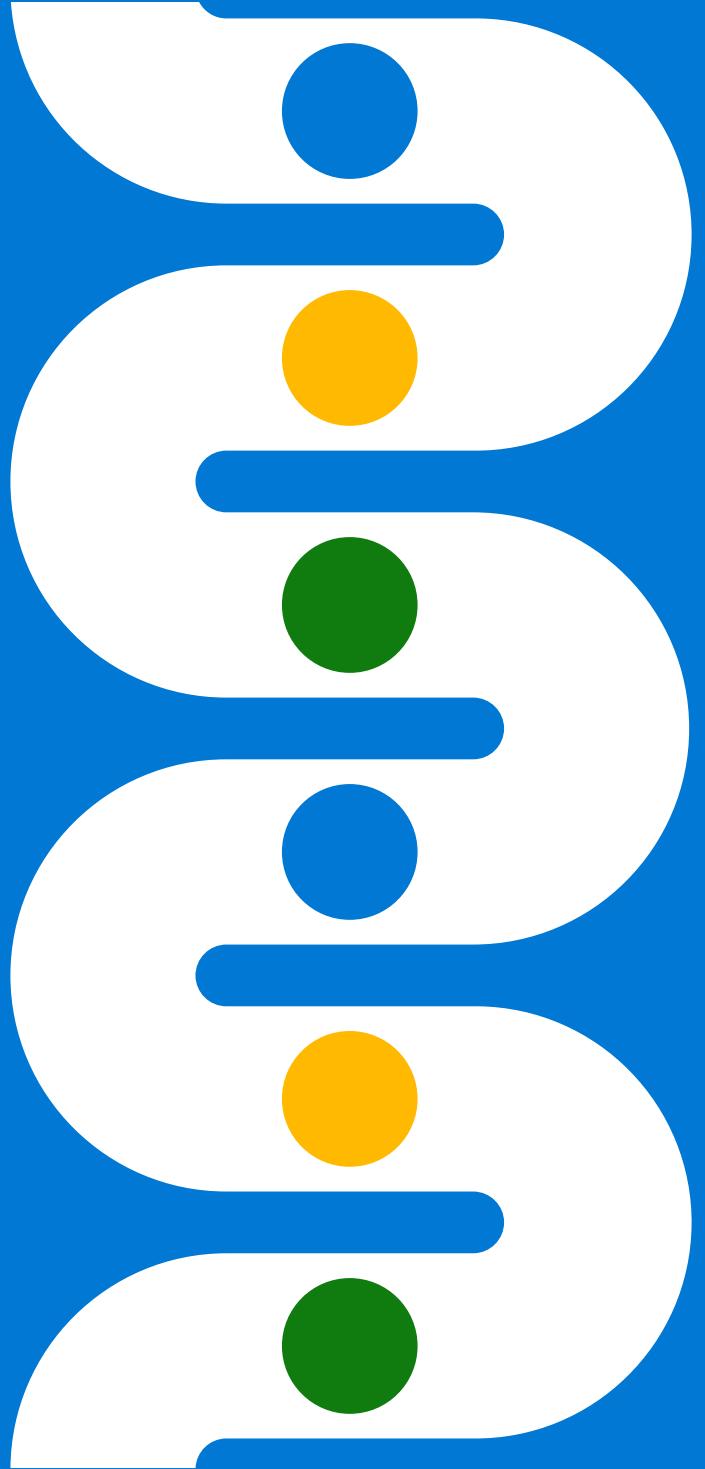
Protect blobs containers, file shares, and data lakes in Azure



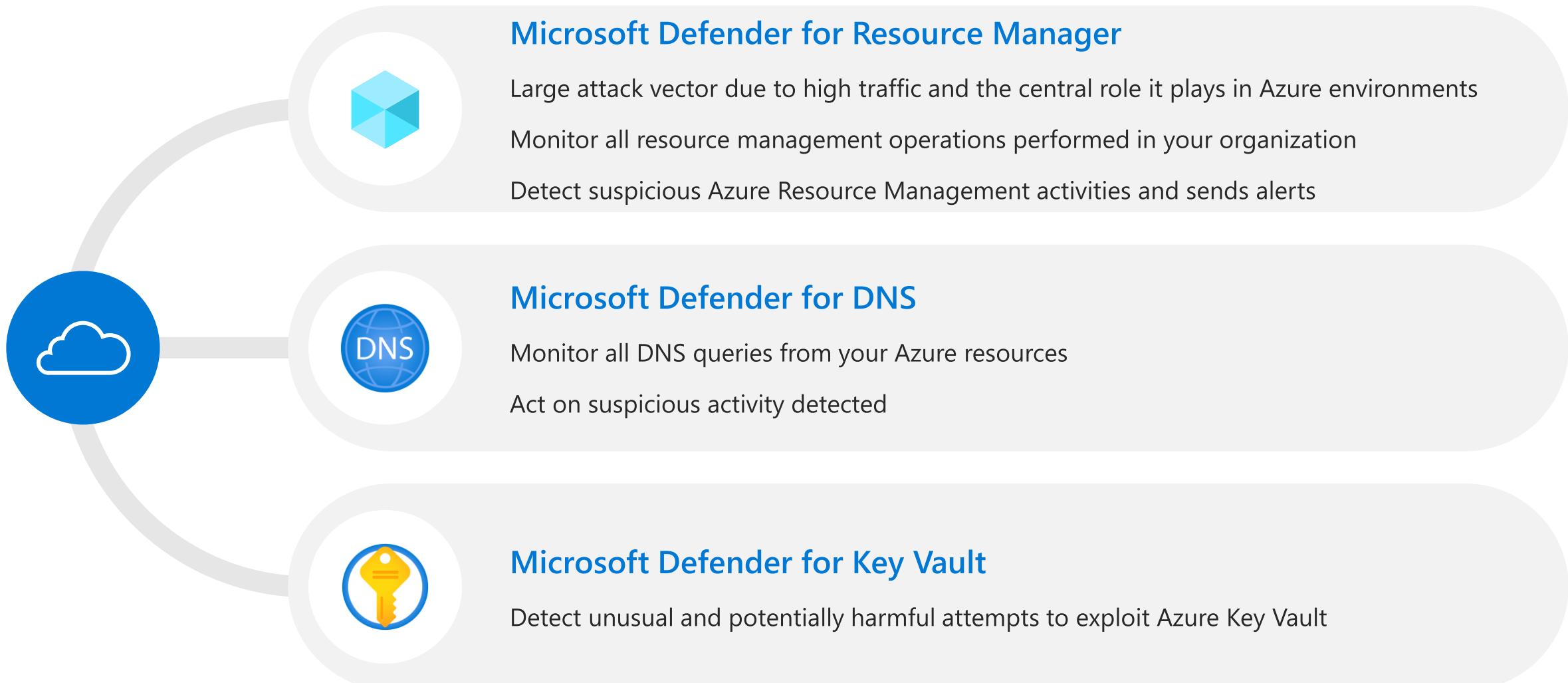
## Threat alerts for storage accounts

- Unusual access to an account
- Unusual behavior in an account
- Hash reputation-based Malware detection
- Unusual file uploads
- Public visibility
- Phishing campaigns

Protect the cloud  
service layer



# Cloud service layer protection



# Wrap-up



# Microsoft Defender for Cloud

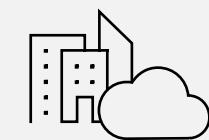
- Secure and protect resources across the three major cloud providers and hybrid environments in one place

---

- Ensure secure and compliant configuration of cloud resources

---

- Detect vulnerabilities and threats to protect against malicious attacks



# Strengthen your cloud security posture today



Enable Defender  
for Cloud  
to assess your  
security posture



Fix your top 5  
Secure Score  
recommendations  
today



Start a free trial  
to protect your  
workloads



Onboard AWS,  
GCP and on-prem  
workloads with  
Azure Arc

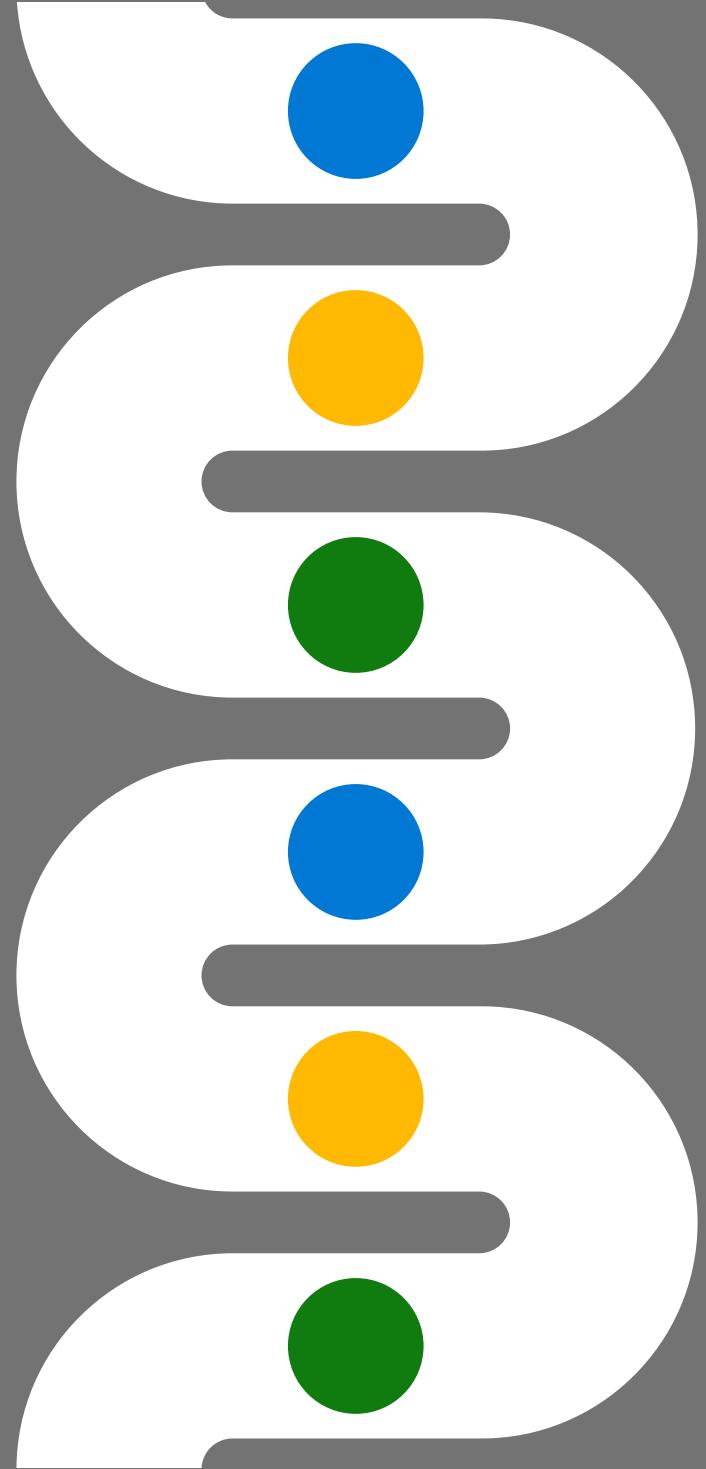
To learn more, visit:

[aka.ms/DefenderForCloud >>](https://aka.ms/DefenderForCloud)



# Thank you

**Most effective XDR to  
protect your users and  
cloud resources**



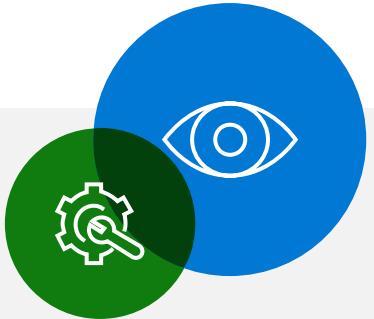
SIEM

## Microsoft Sentinel

Visibility across your entire organization



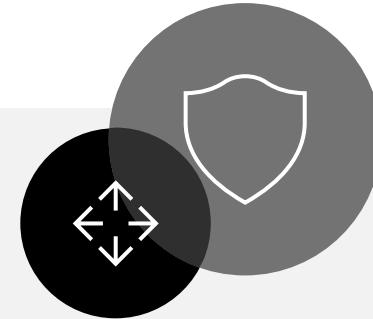
# Microsoft XDR product vision



**Microsoft's vision for SIEM+XDR** is to deliver a **single, integrated solution** to help SOC's stop attacks and keep their organization safe.

Our SIEM+XDR vision **extends beyond native and hybrid** models to provide the depth of automated correlation from XDR, integrated with the power of a cloud-native SIEM.

Third-party data and breadth of signal is critical. That's why a **multi-cloud, multi-platform** solution is integral to our SIEM+XDR vision.



## Our three principles for XDR:

1. Expand beyond the endpoint and EDR to a truly **unified** cross-workload, multi-cloud security solution.
2. Provide **built-in** prevention and protection across all Microsoft owned security assets, extending to multi-platform (iOS, Android, Linux, MacOS) and multi-cloud (GCP, AWS).
3. Drive shift from detection to **prevention** via real-time blocking of threats and reduce time to response through incident correlation and automated **self-healing**.