Microsoft Security

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.[1]

Increase in number and sophistication of attacks

- In 2021, the average cost of a breach was **$4.24M**.[2]

Complexity managing multi-cloud environments

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

[1]Source: 451 Research
[2]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

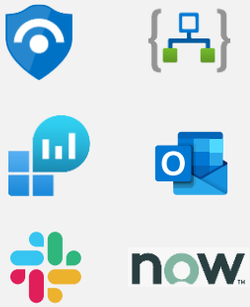
Vulnerability assessment & management

Respond & Automate

Assess and resolve security alerts and incidents

Automate response

Automate with the tools of your choice



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

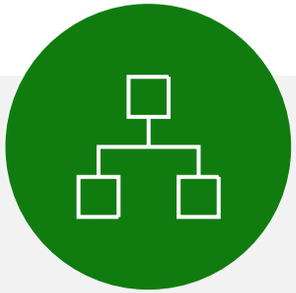
- Workload-specific signals and threat alerts
- Deterministic, AI, and anomaly-based detection mechanisms
- Leverages the power of Microsoft Threat Intelligence with 24 trillion signals daily

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

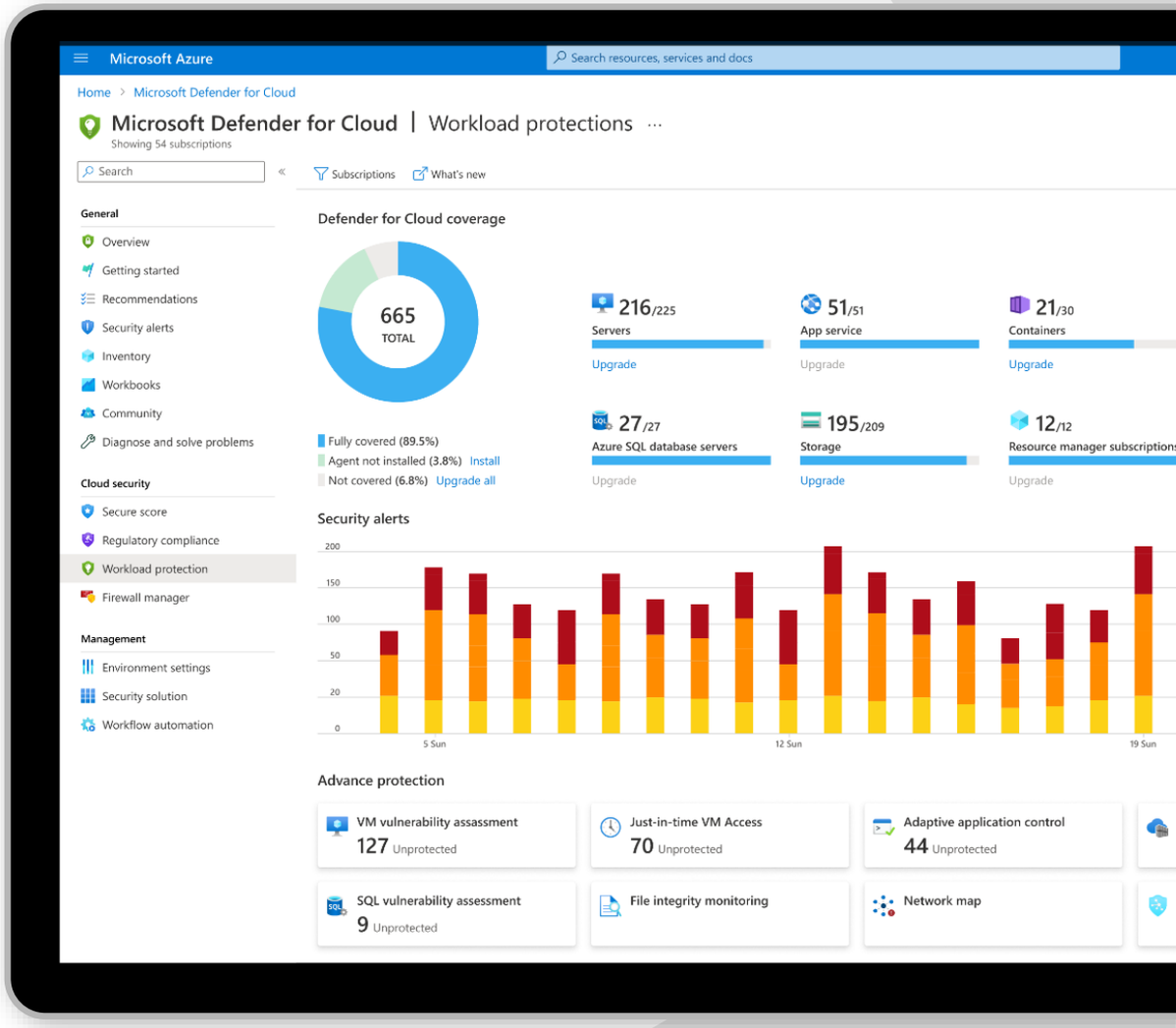
Identify and remediate vulnerabilities before they are exploited

Alert correlation

Prioritize more easily with connected alerts that are grouped into incidents

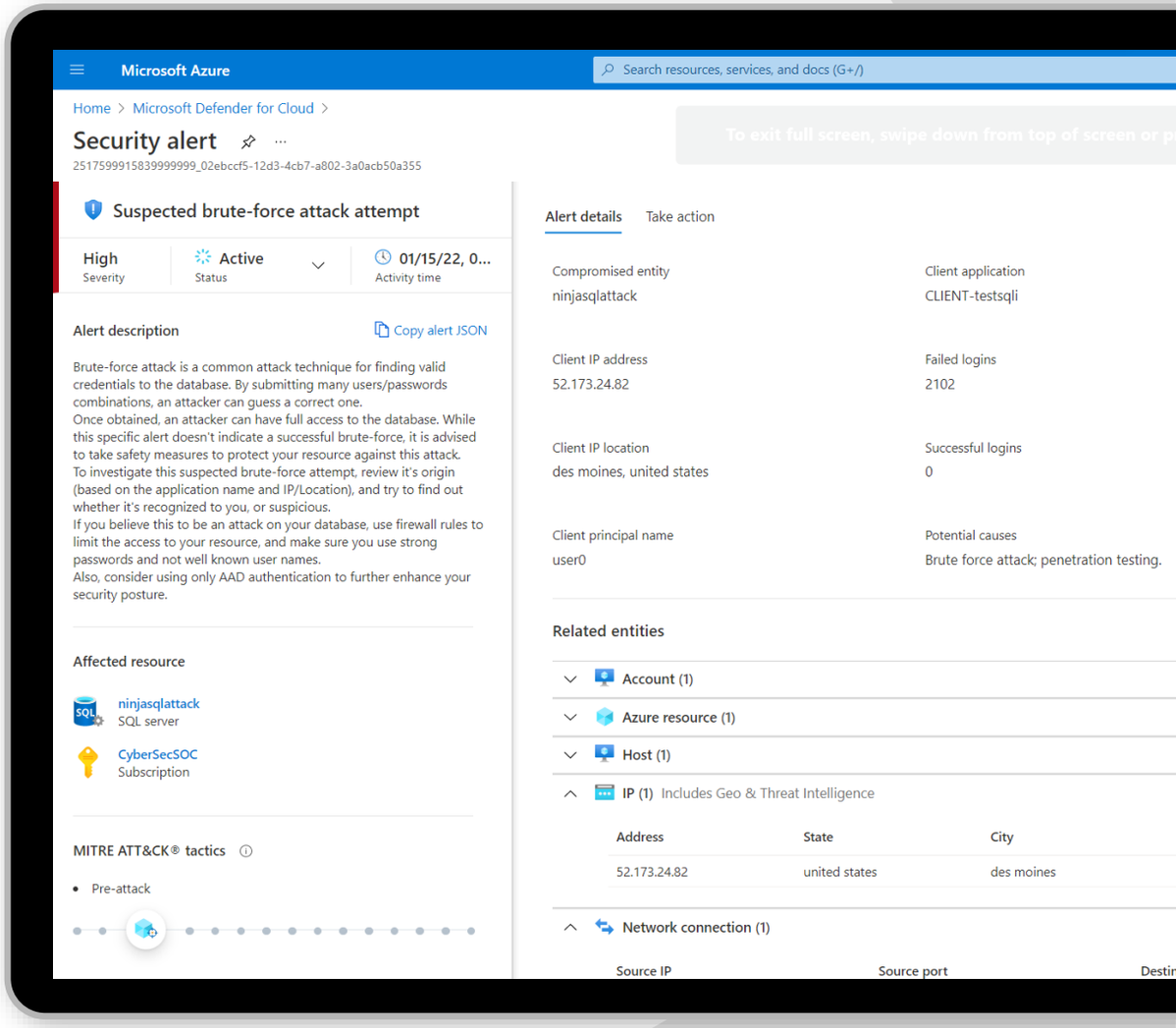
Protect your workloads in the cloud and on-premises

- 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.



Full-stack coverage with dedicated detections

Compute

- Any server
- Azure VMSS
- App Services
- Azure K8s
- Unmanaged K8s

Service Layer

- Azure DNS
- Key Vault
- Network Layer V1
- Resource Manager

Databases and Storage

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

AWS workloads

- Amazon EKS
- Amazon EC2
- Unmanaged Kubernetes
- Unmanaged SQL

GCP workloads

- GKE clusters
- Google Compute
- Unmanaged Kubernetes
- Unmanaged SQL

On-premise workloads

- Kubernetes
- SQL Servers
- Servers

On-premise

Protect your VMs

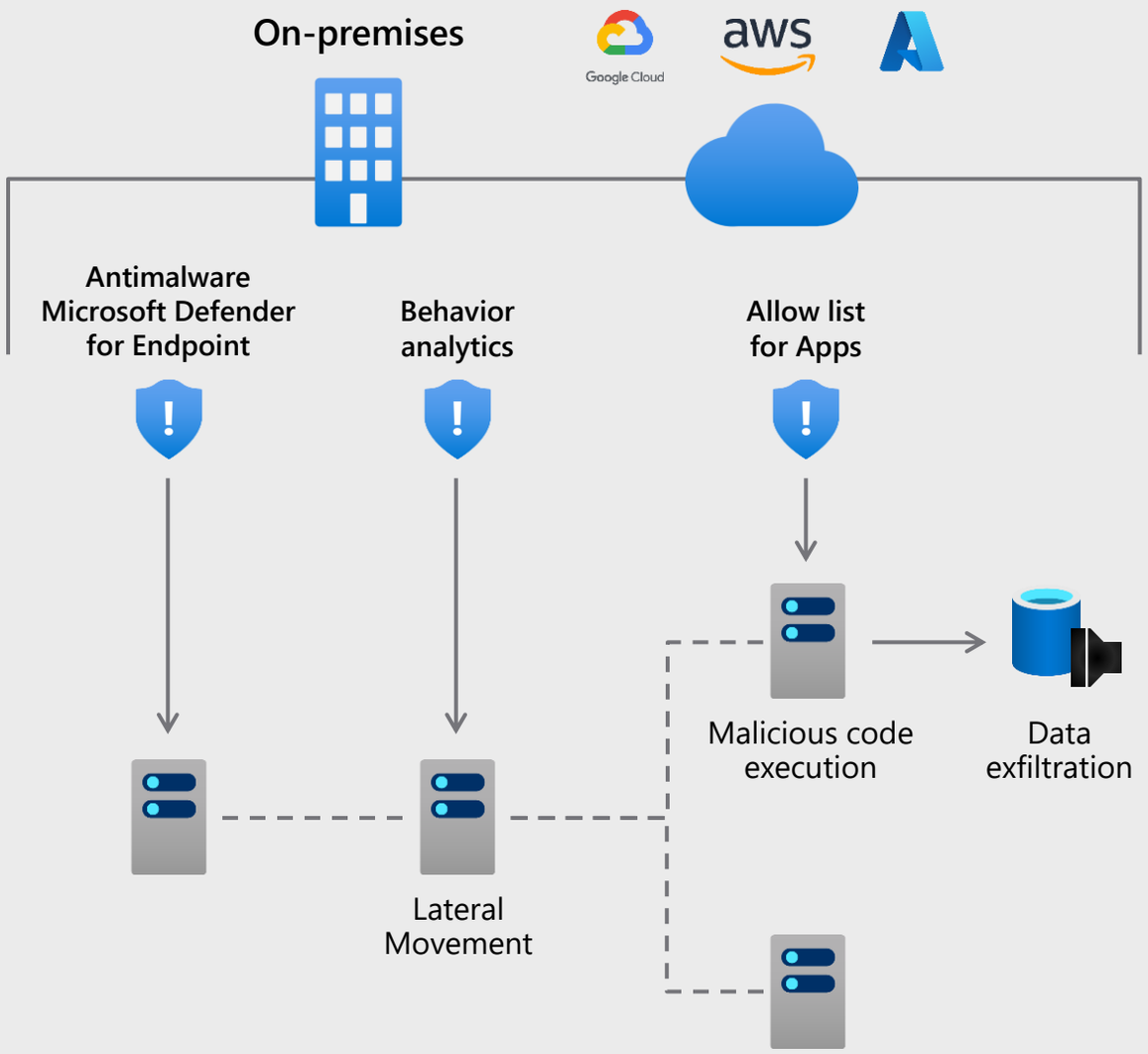
Server security in the cloud is different

- 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



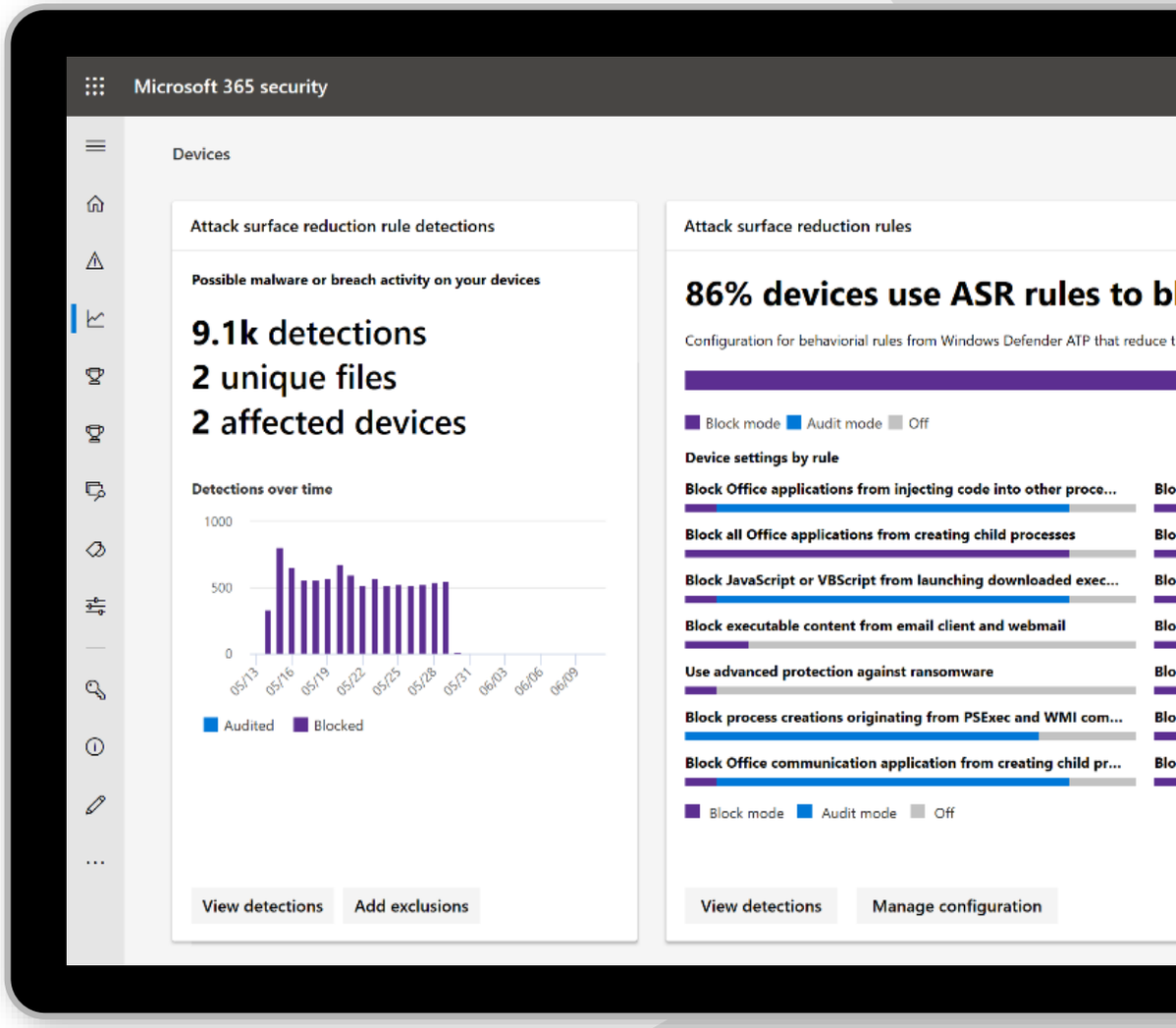


Attack surface reduction

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

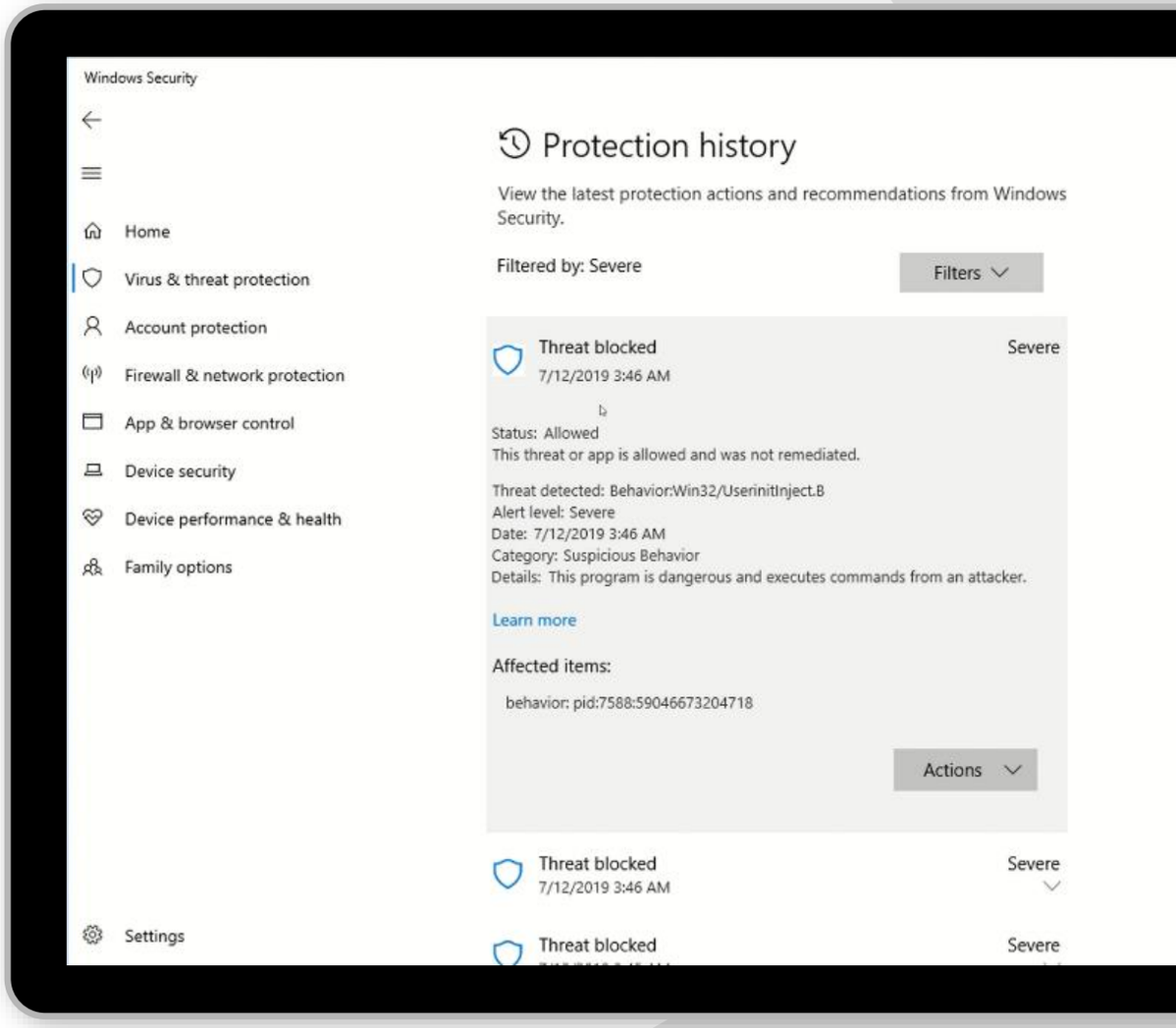


Next generation antivirus protection

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

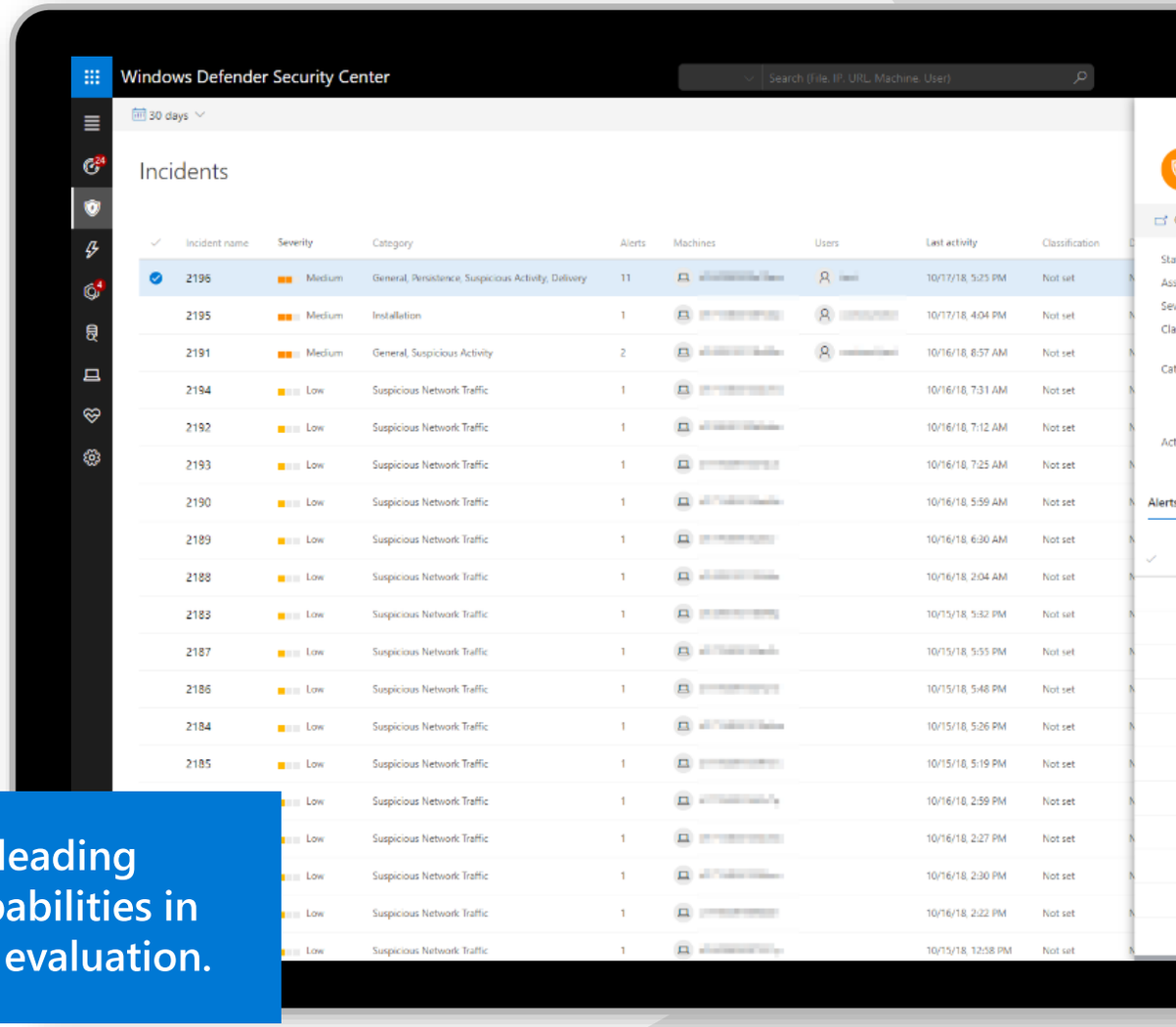


Endpoint detection & response

Powered by Microsoft Defender for Endpoint

Detect and investigate advanced persistent attacks

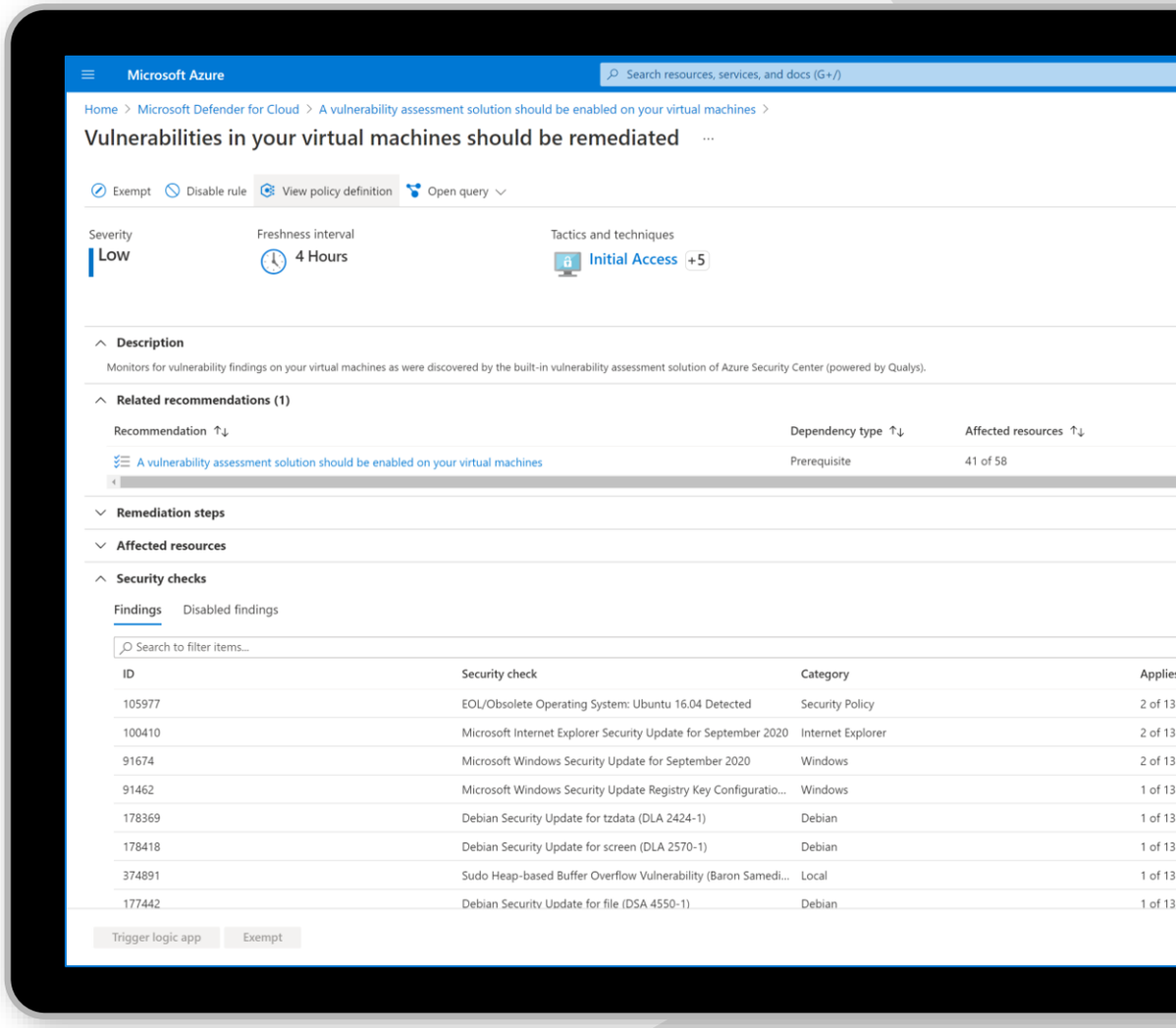
- Correlated behavioral alerts
- Investigation & hunting over six months of data
- Rich set of response actions



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

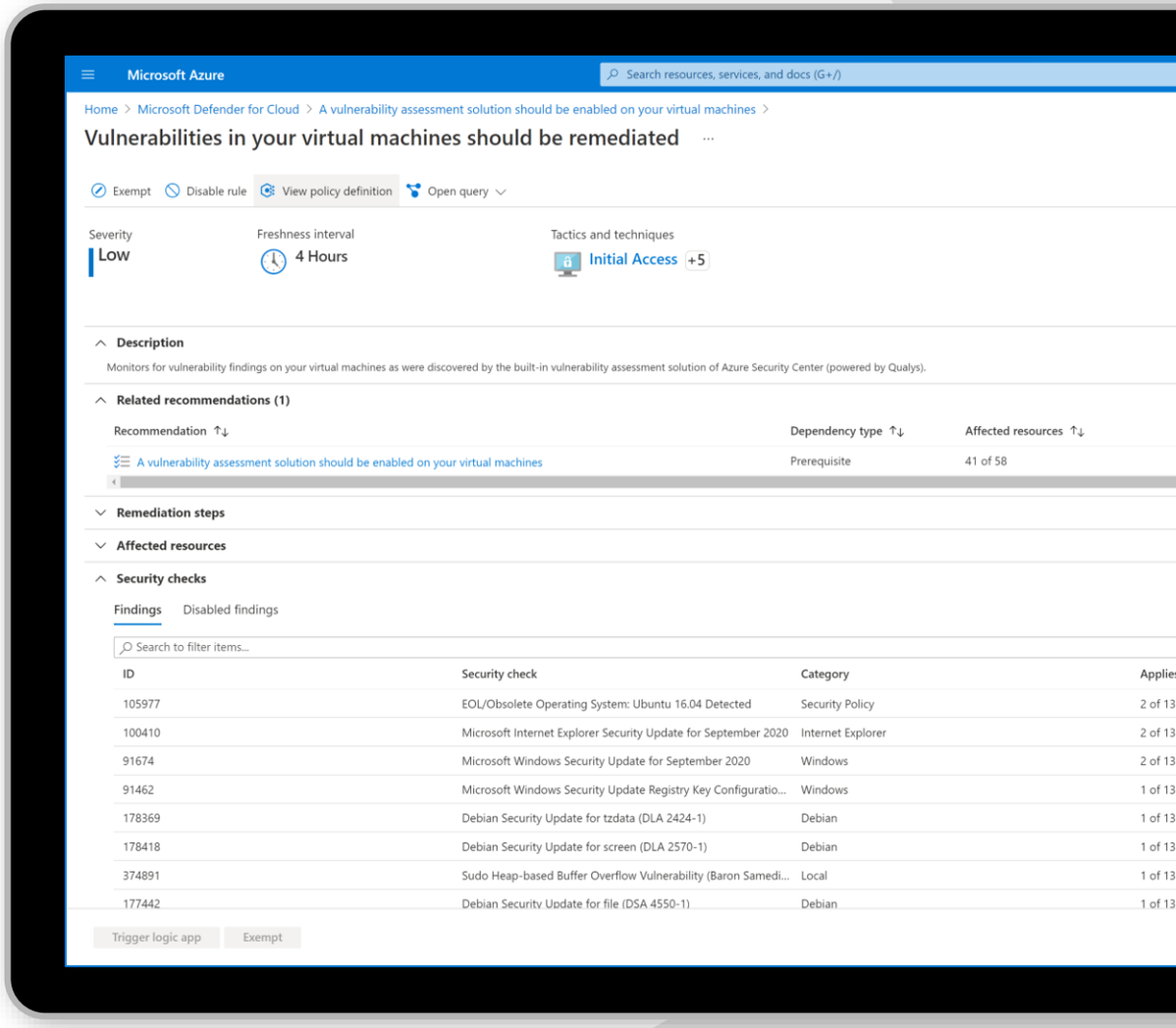
Adaptive application control

- 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



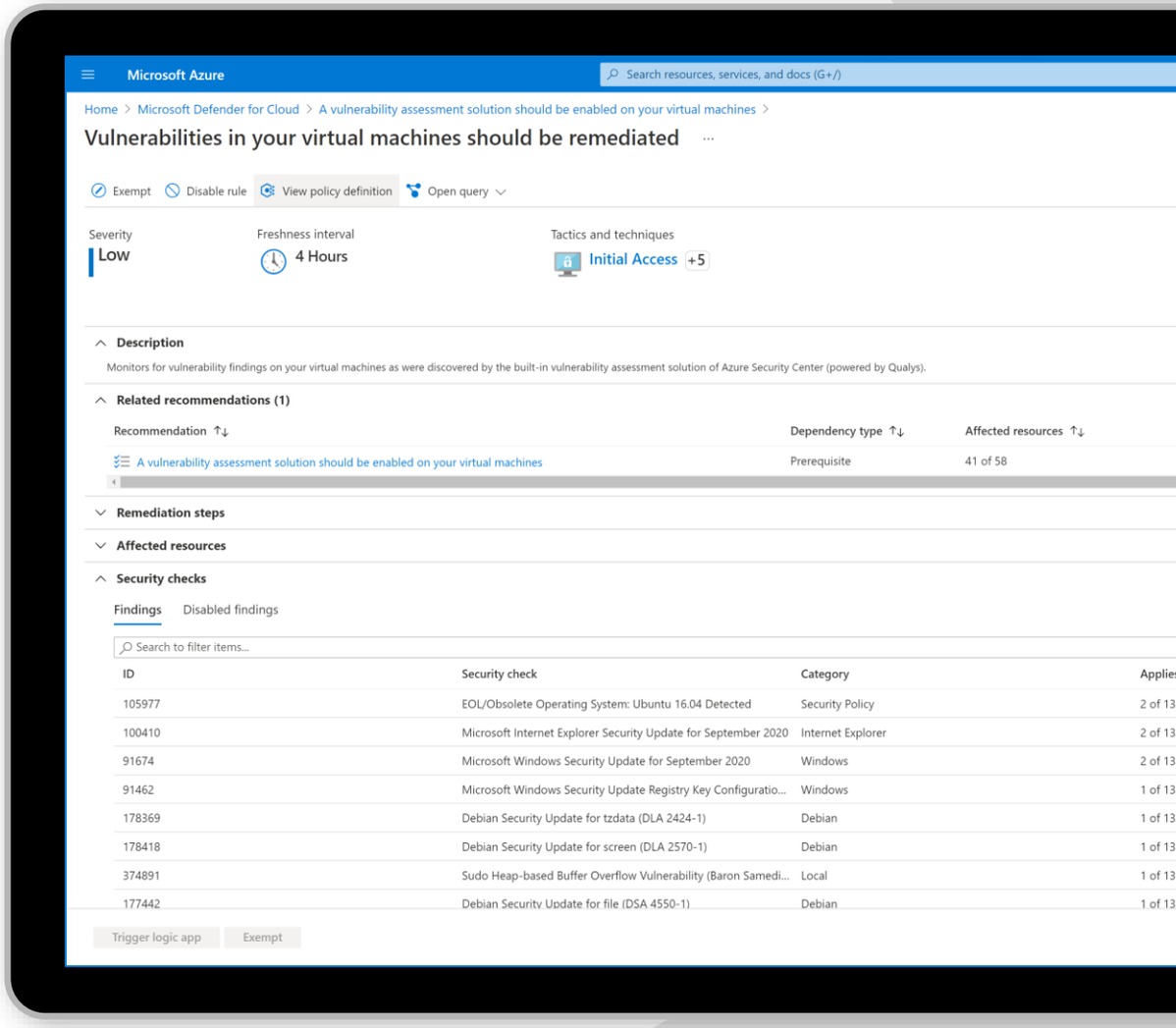
Asses your VMs and containers for vulnerabilities

- 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



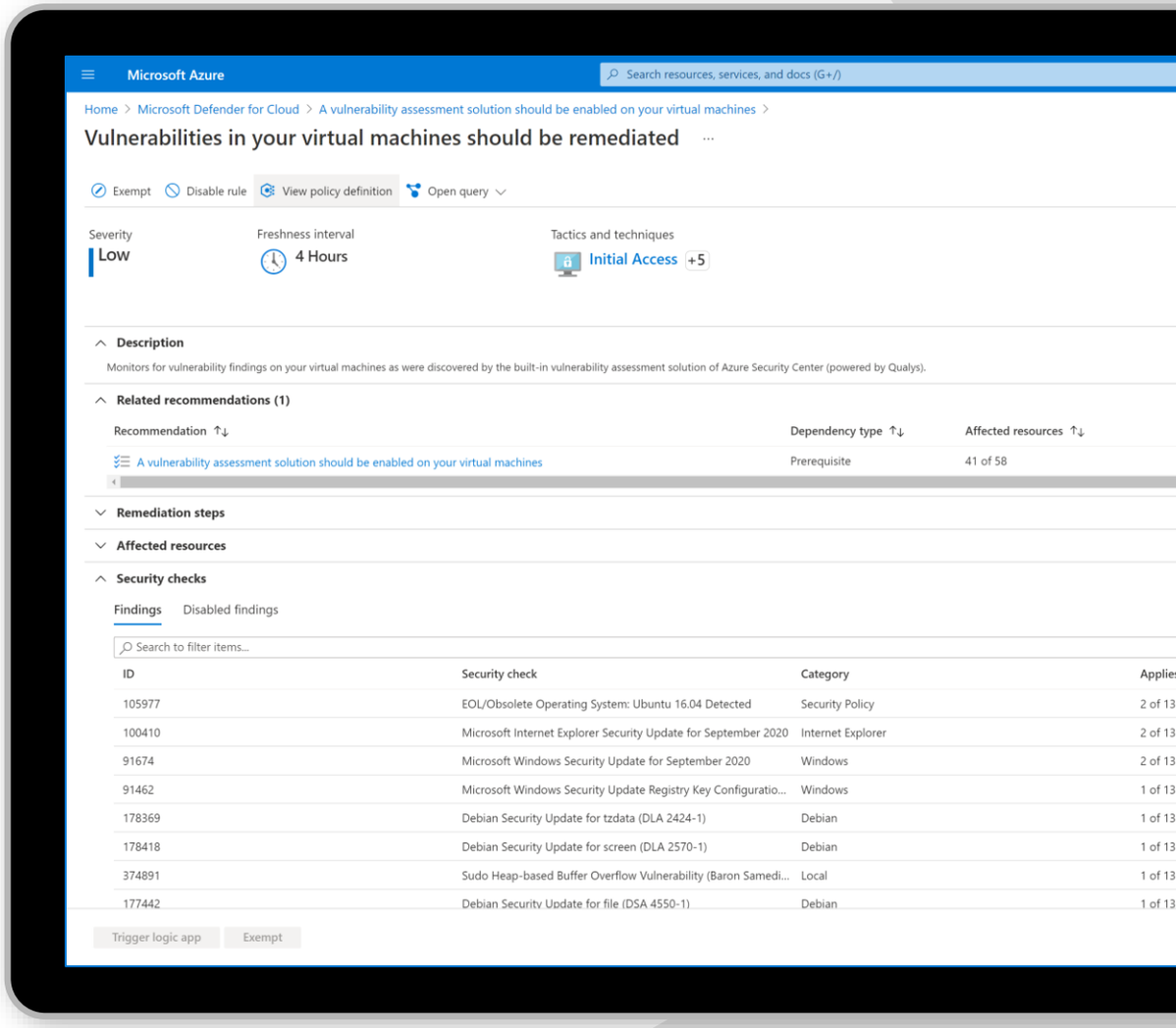
Just-in-time VM access

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



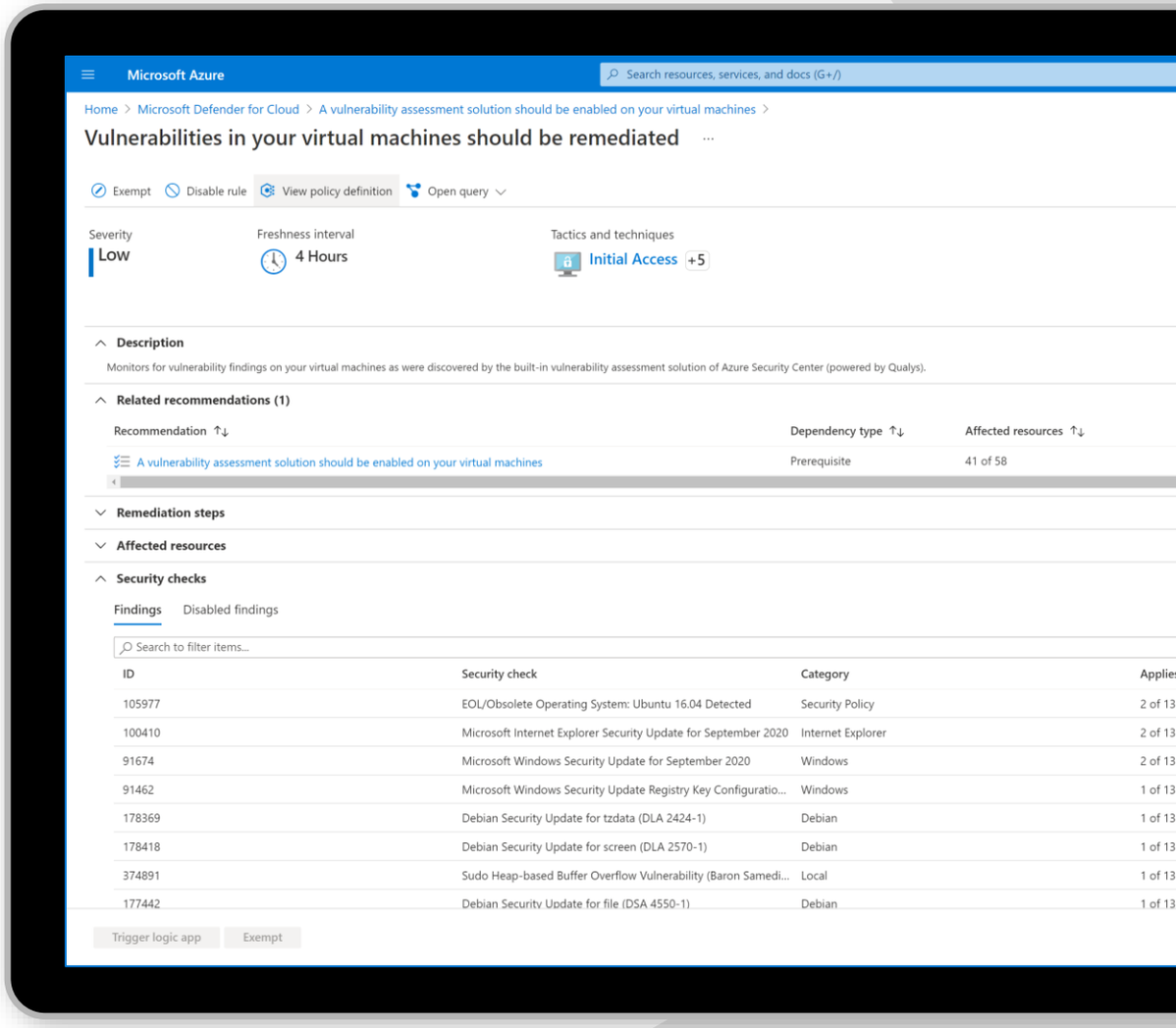
Adaptive network hardening

- 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



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

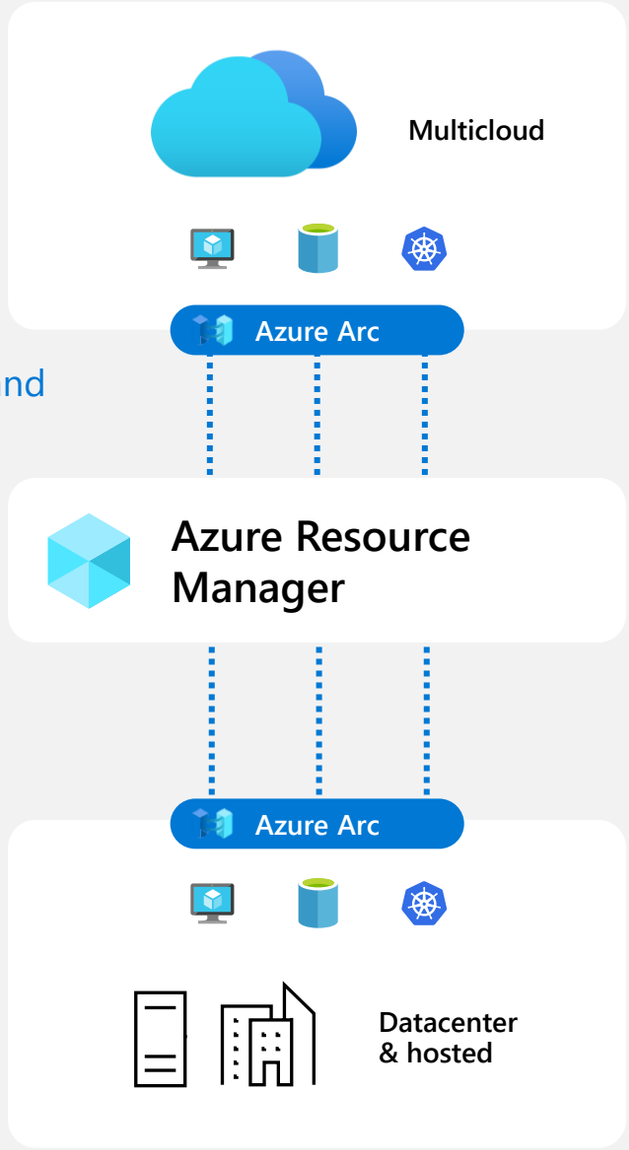
1. Server onboards to Azure Arc (the server is then discoverable by Defender for Servers)
2. Then Defender for Servers automatically provisions MDE to this server as an extension
3. Defender for Endpoint capabilities are now available on the server

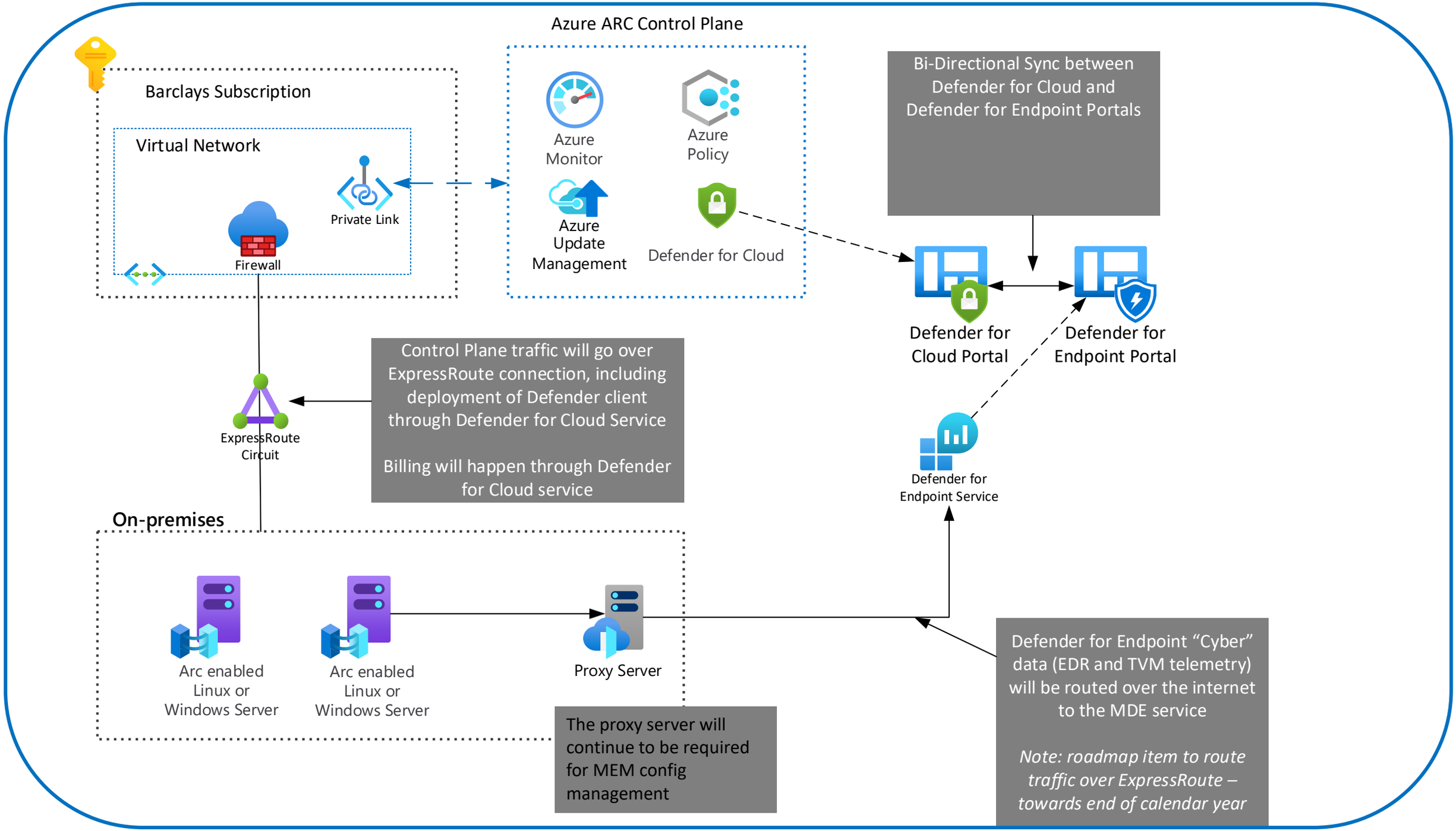
Use Azure Arc to connect workloads anywhere to Microsoft Defender for Cloud

- 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

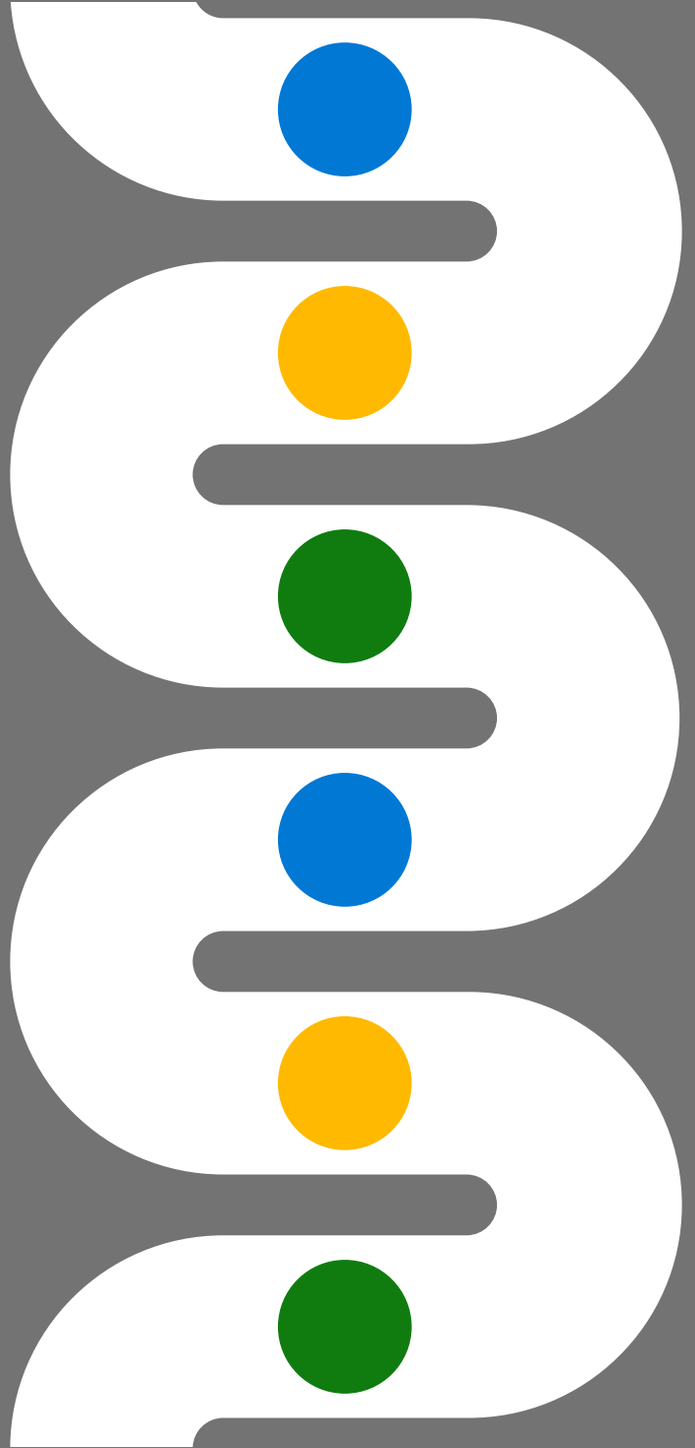
Azure Arc enables cloud management and security protections

Single control plane for any resource, anywhere




Azure ARC Control Plane
Barclays Subscription
Virtual Network
Private Link
Firewall
Azure Monitor
Azure Policy
Azure Update Management
Defender for Cloud
Bi-Directional Sync between Defender for Cloud and Defender for Endpoint Portals
Defender for Cloud Portal
Defender for Endpoint Portal
Defender for Endpoint Service
ExpressRoute Circuit
Control Plane traffic will go over ExpressRoute connection, including deployment of Defender client through Defender for Cloud Service
Billing will happen through Defender for Cloud service
On-premises
Arc enabled Linux or Windows Server
Arc enabled Linux or Windows Server
Proxy Server
The proxy server will continue to be required for MEM config management
Defender for Endpoint "Cyber" data (EDR and TVM telemetry) will be routed over the internet to the MDE service
Note: roadmap item to route traffic over ExpressRoute – towards end of calendar year

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[1]

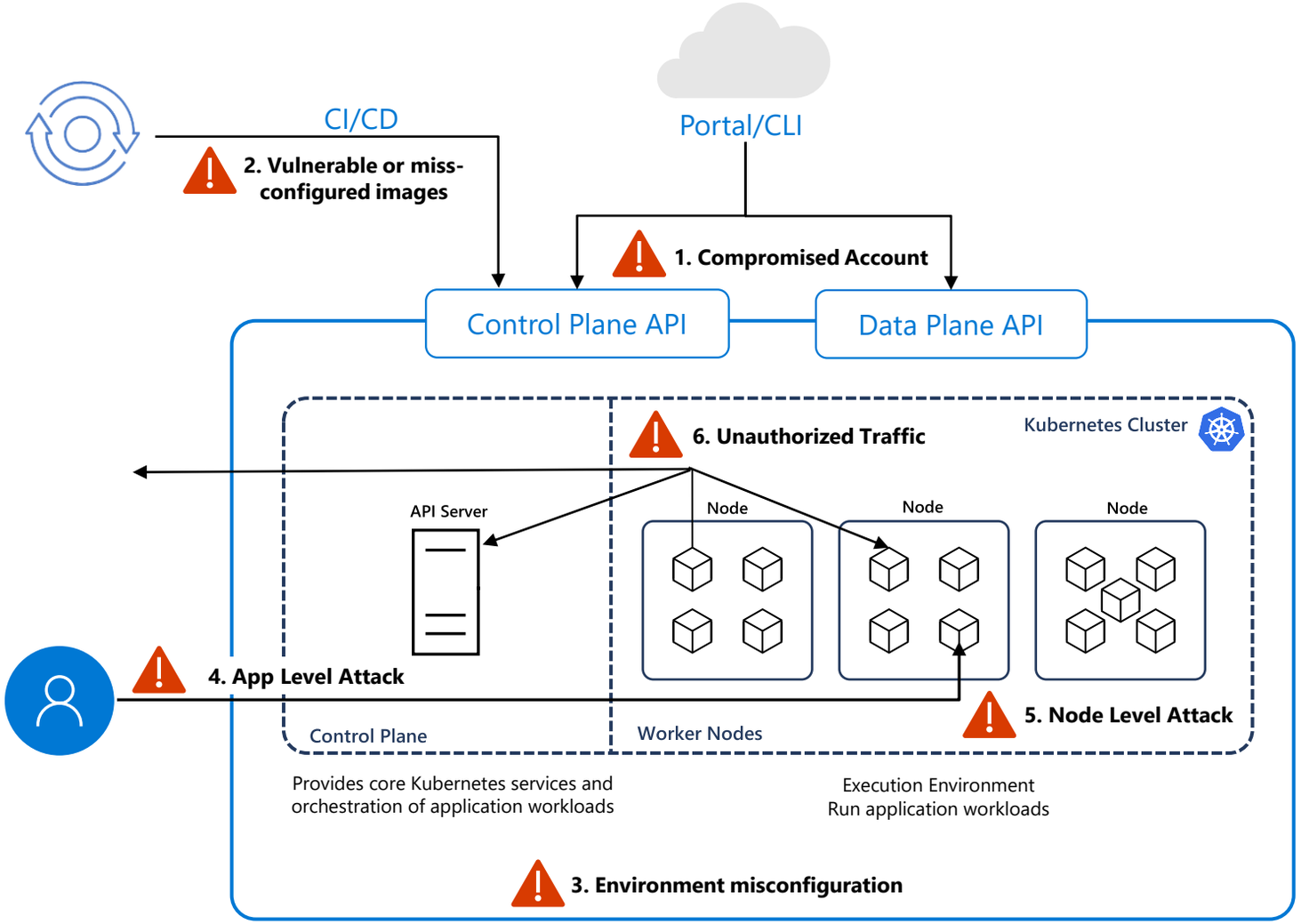
Visibility of containers traffic flows are difficult to track with traditional tools

Complex runtime environment, with different configuration layers and options

- **94%** orgs experienced at least one security incident in their Kubernetes environments during 2021[2]

[1] CNCF 2020 Container Adoption Survey
[2] 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

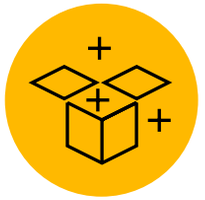
Reduce your attack surface by continuously scanning workloads to identify and manage container vulnerabilities

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

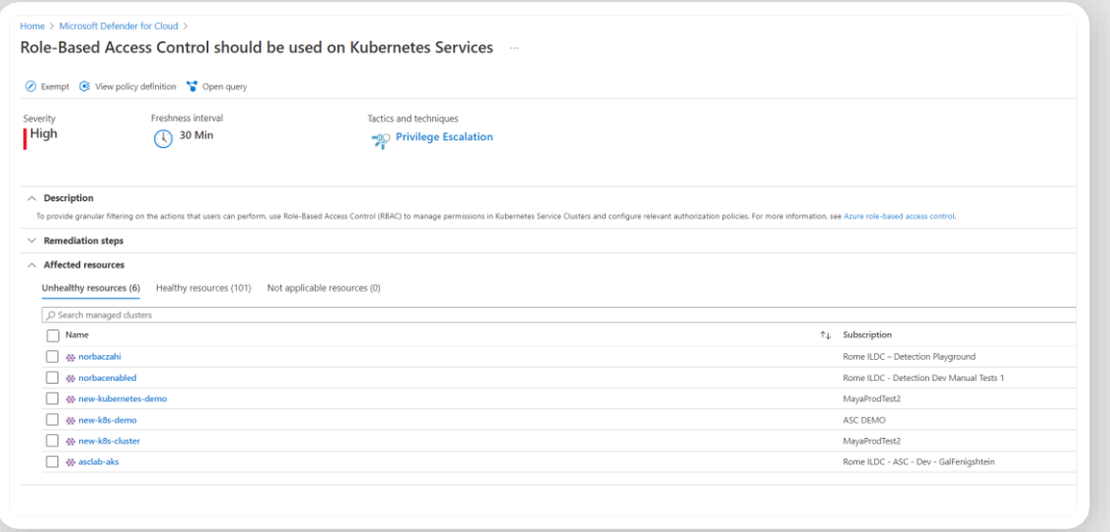
- Understand the bottom line of your security posture
- Prioritized view of containerized assets' security posture

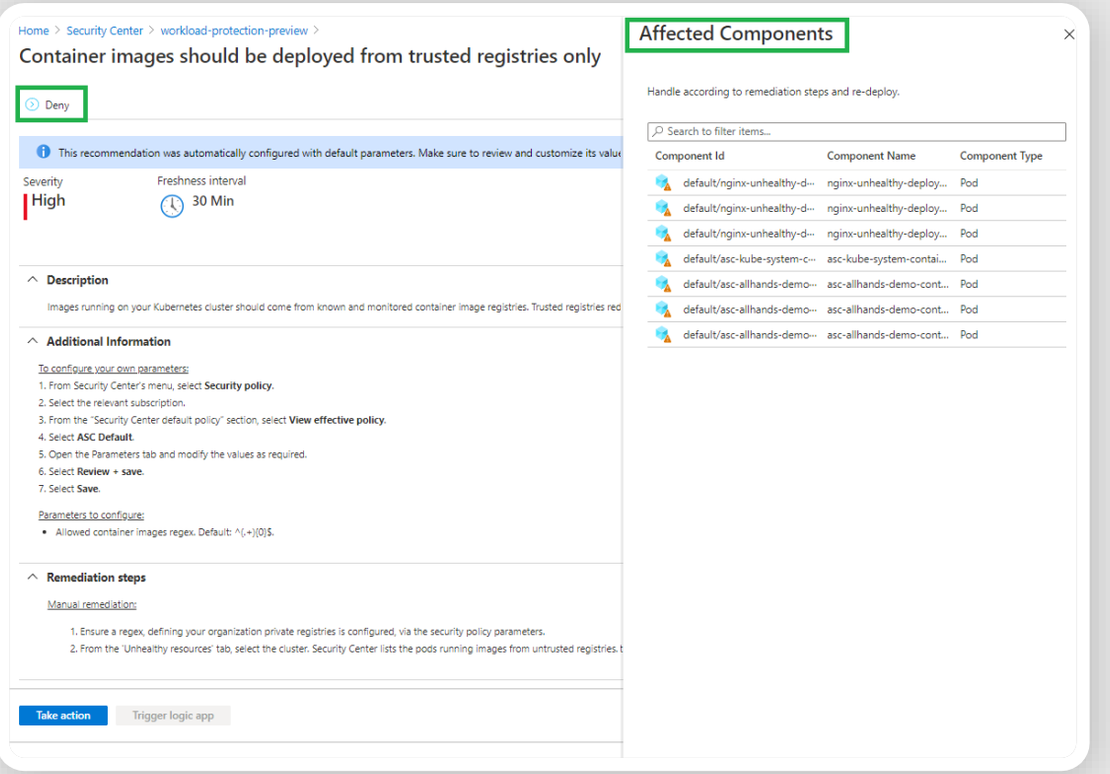
Control plane recommendations

- 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





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

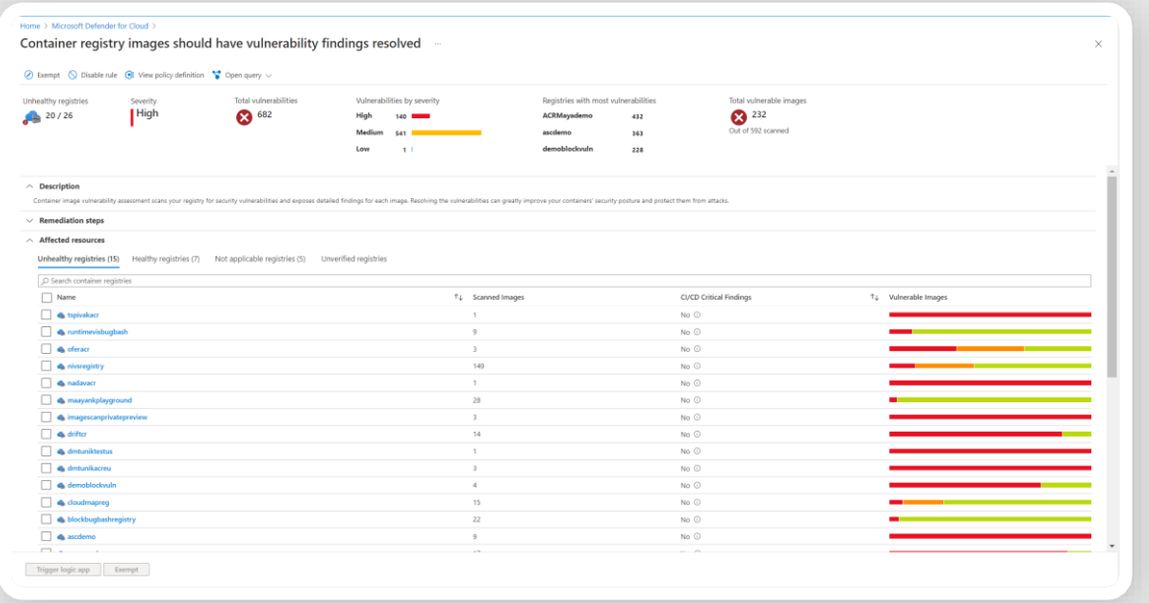
Runtime

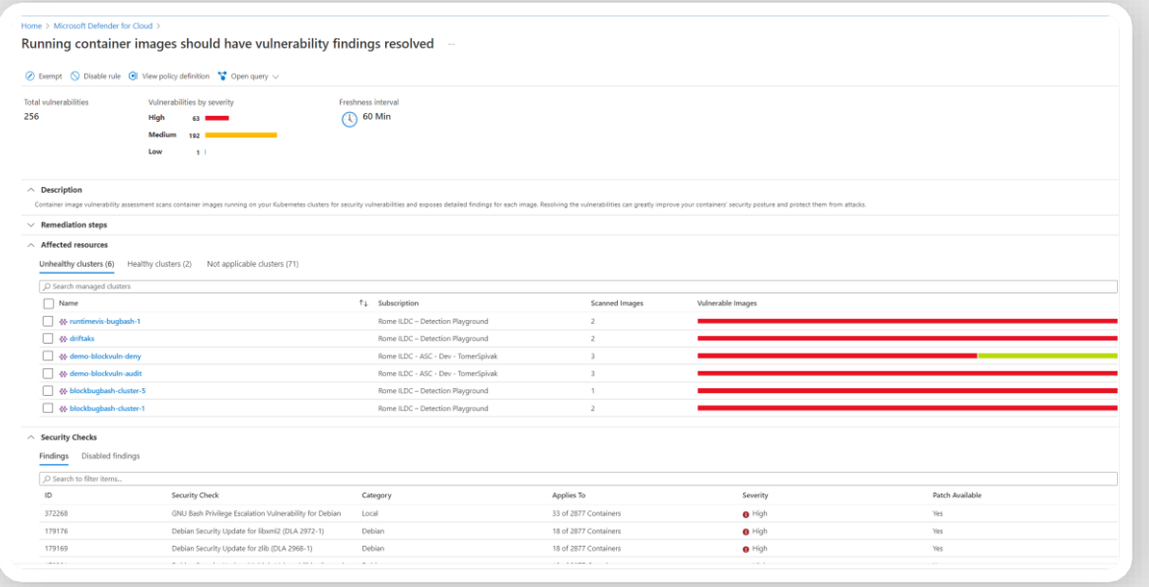
- Continuous scanning of running images
- Visibility of running images with vulnerabilities

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

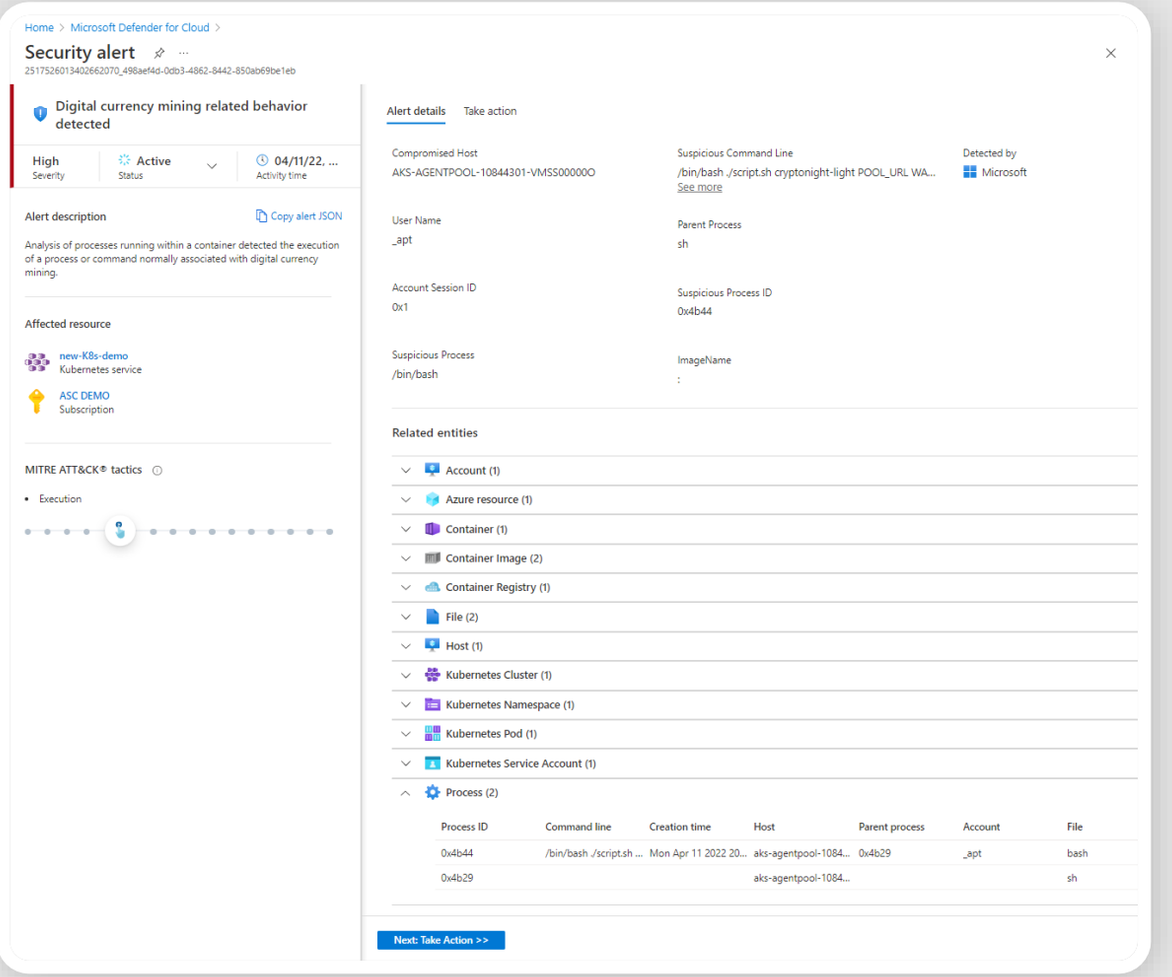
Understand risk and context

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

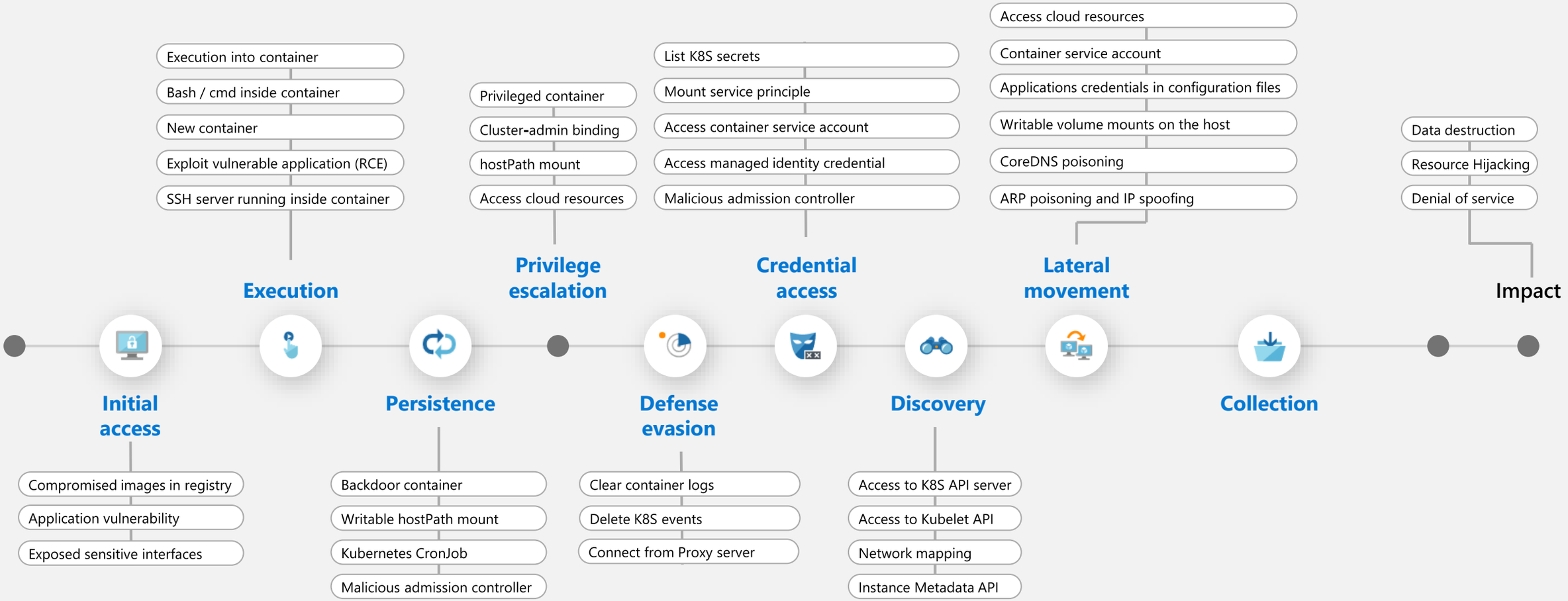
Automate response

New!

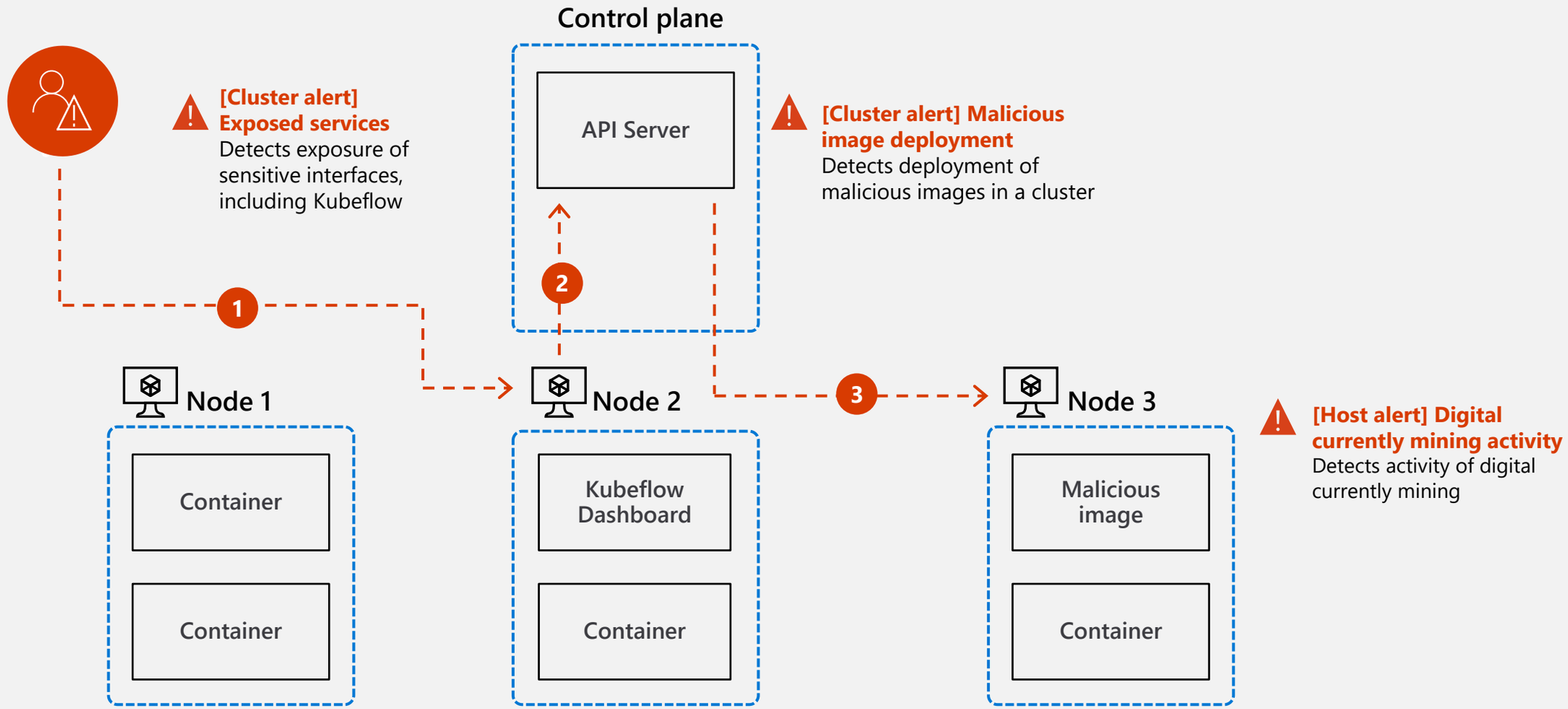
- Automate actions with tools of your choice: SIEM integration, email notifications, workflow automations and continues export



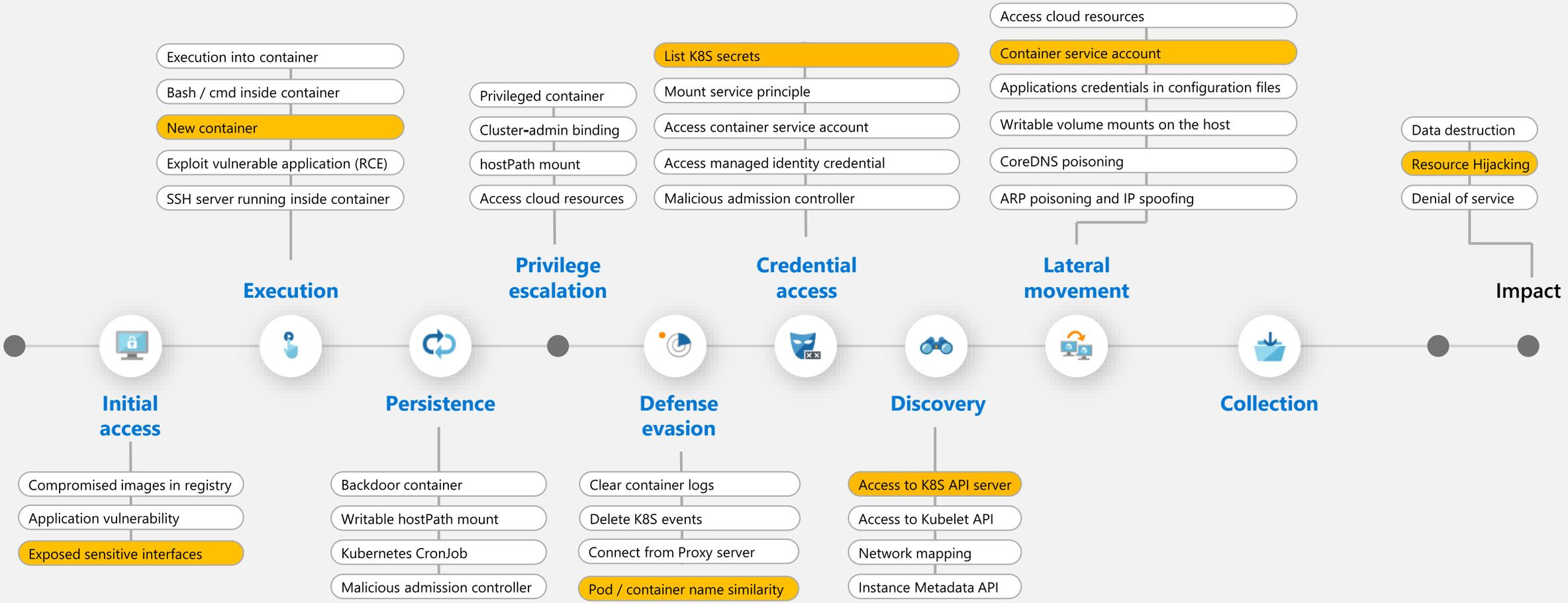
Threat detections aligned to the Kubernetes Attack Matrix



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

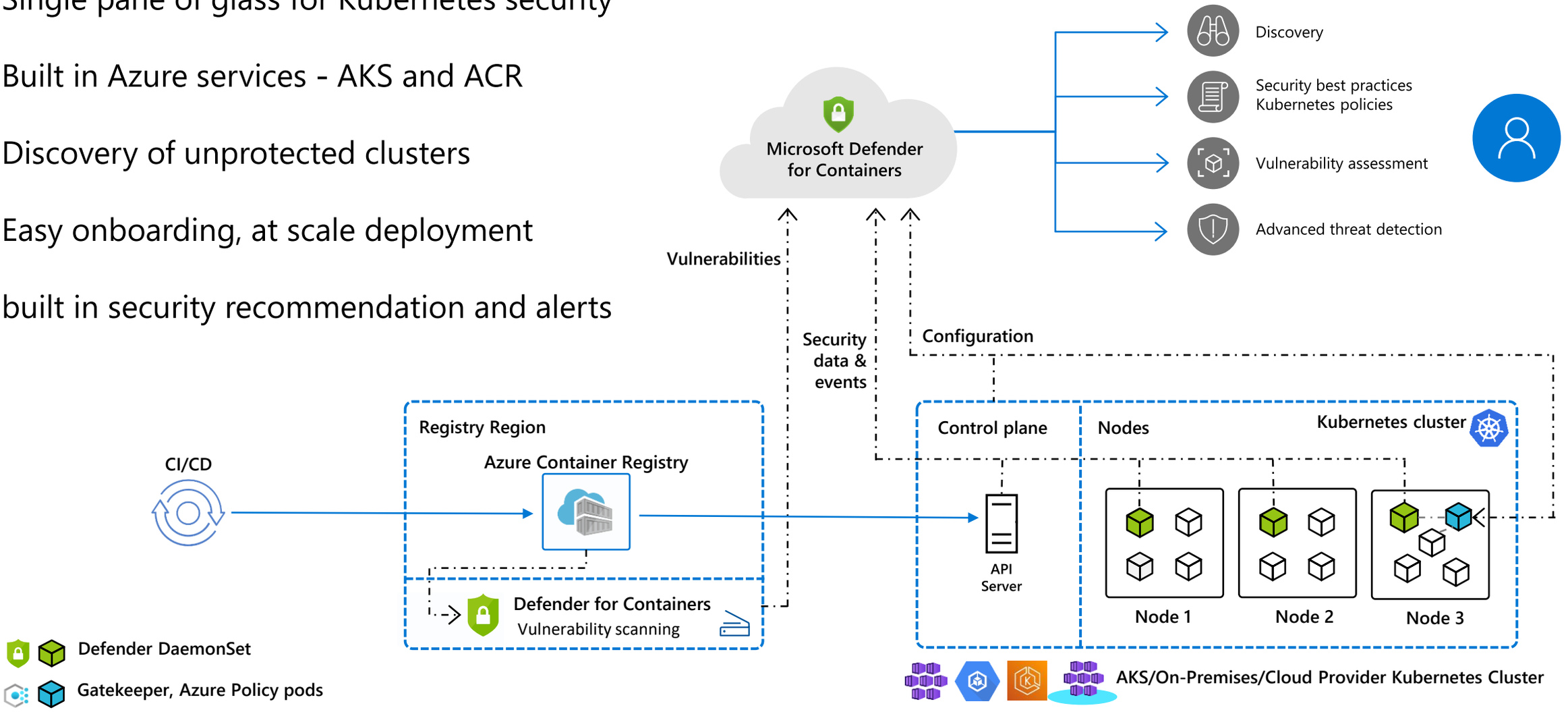


Threat detections aligned to the K8s Attack Matrix



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

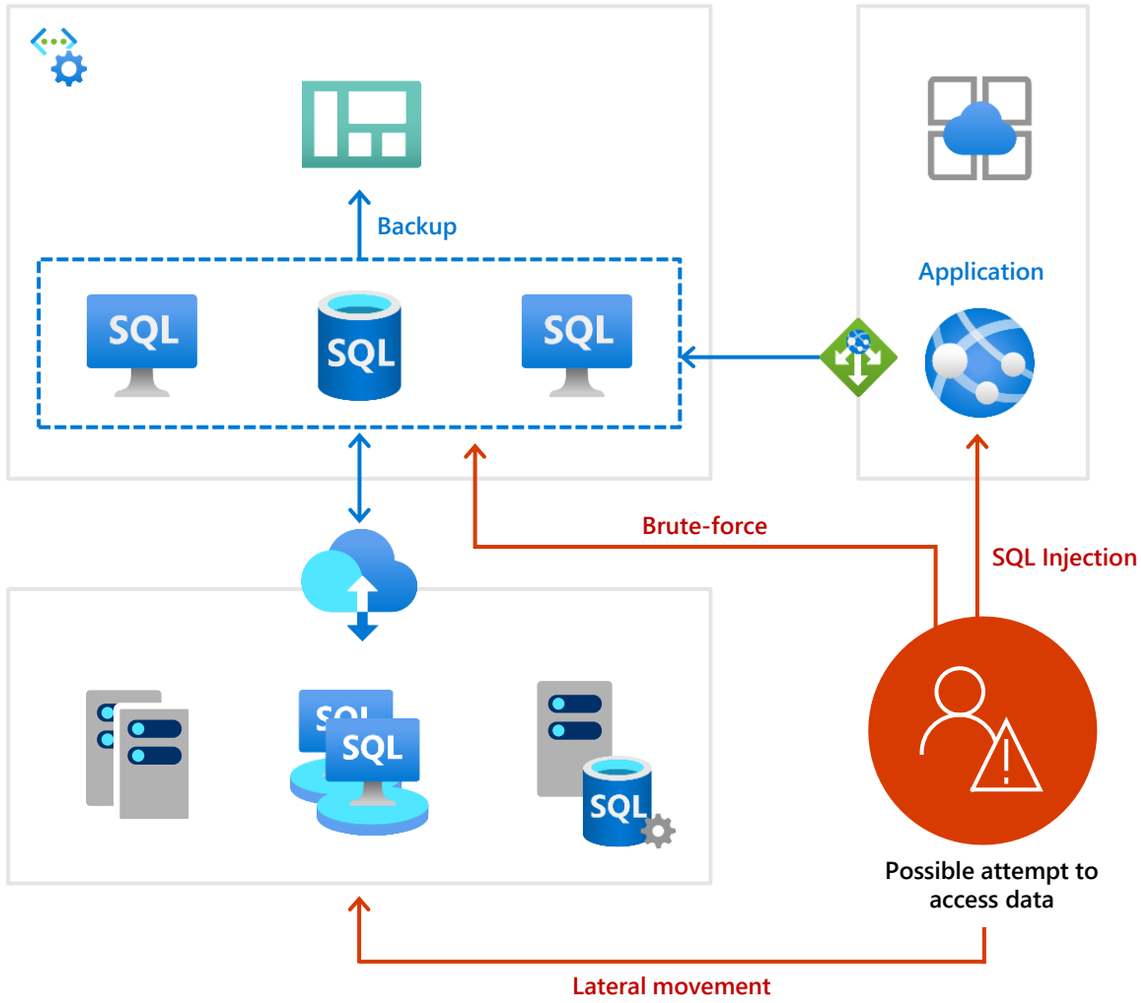
Azure Database for PostgreSQL

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

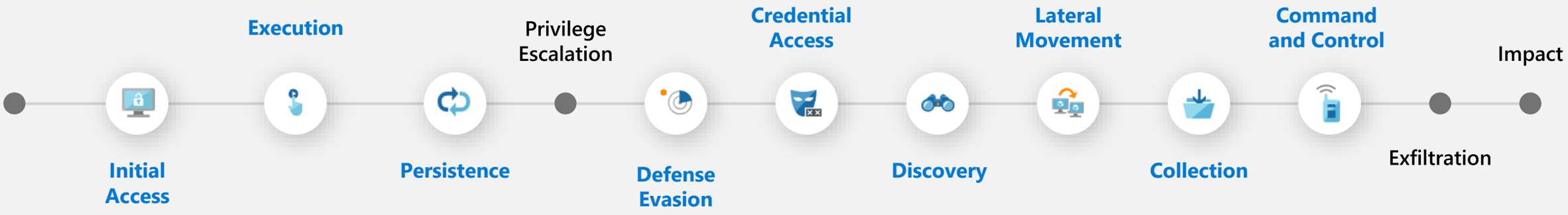
- Potential SQL Injection
- Vulnerability to SQL Injection
- Anomalous amount of data extraction
- Anomalous destination of data extraction

Threat intelligence

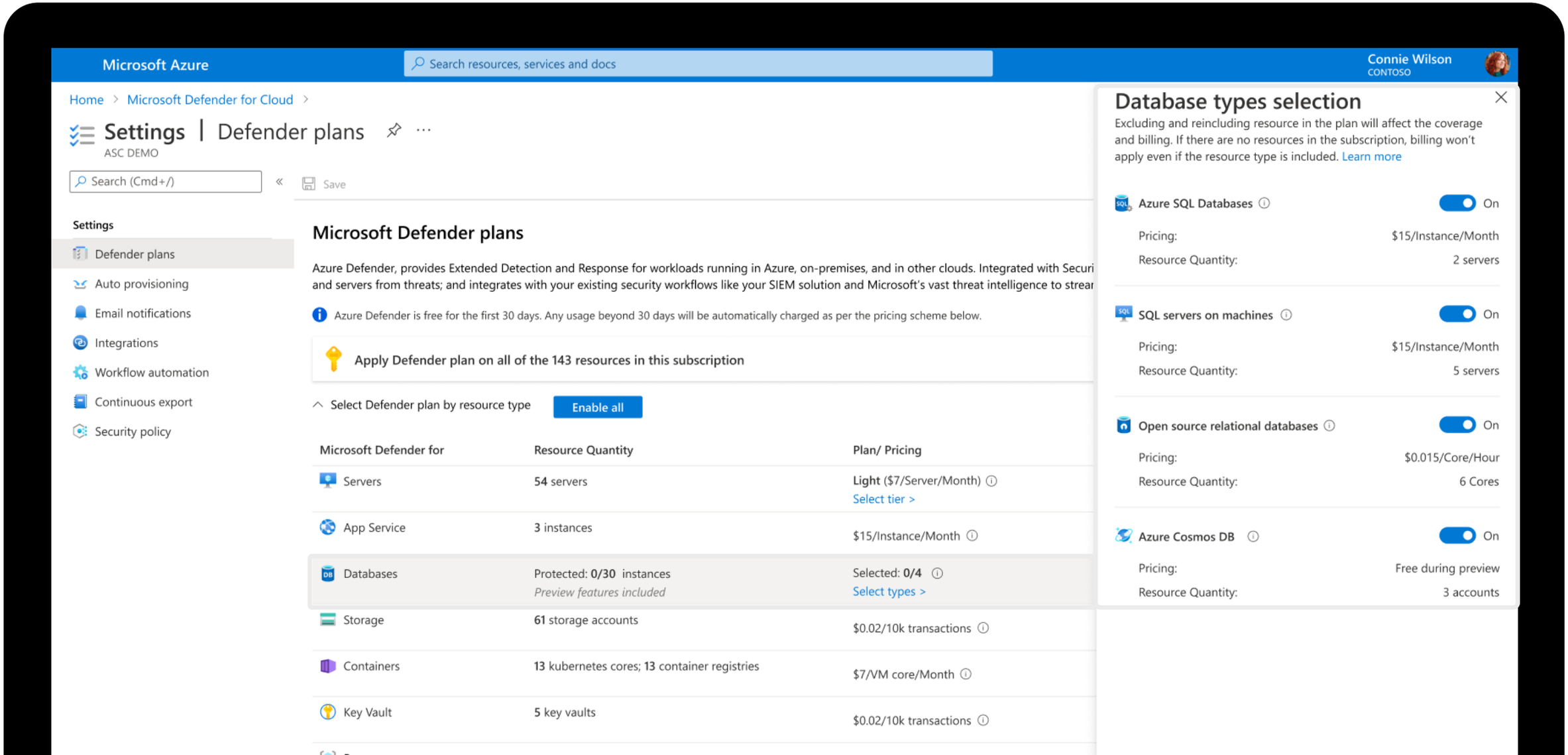
- Access from an unusual location
- Access from a suspicious IP
- Data center anomaly
- Principal anomaly
- Domain anomaly
- Suspicious app

Brute force

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

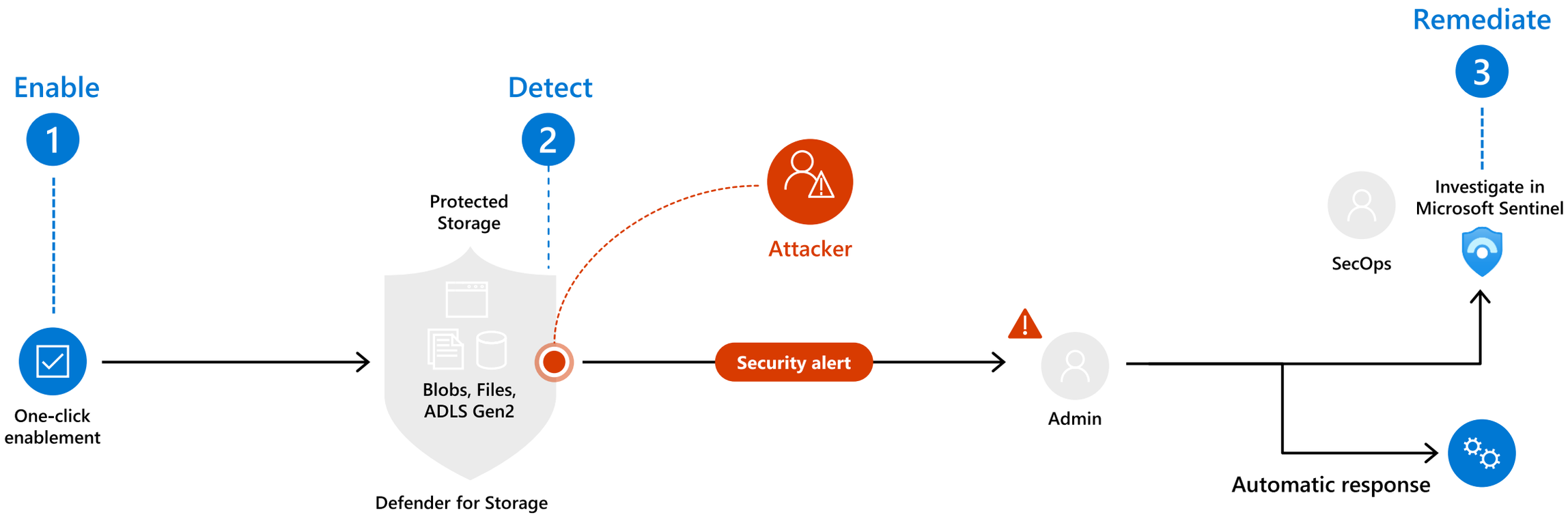


One-click enablement to protect your database estate



Microsoft Defender for Storage

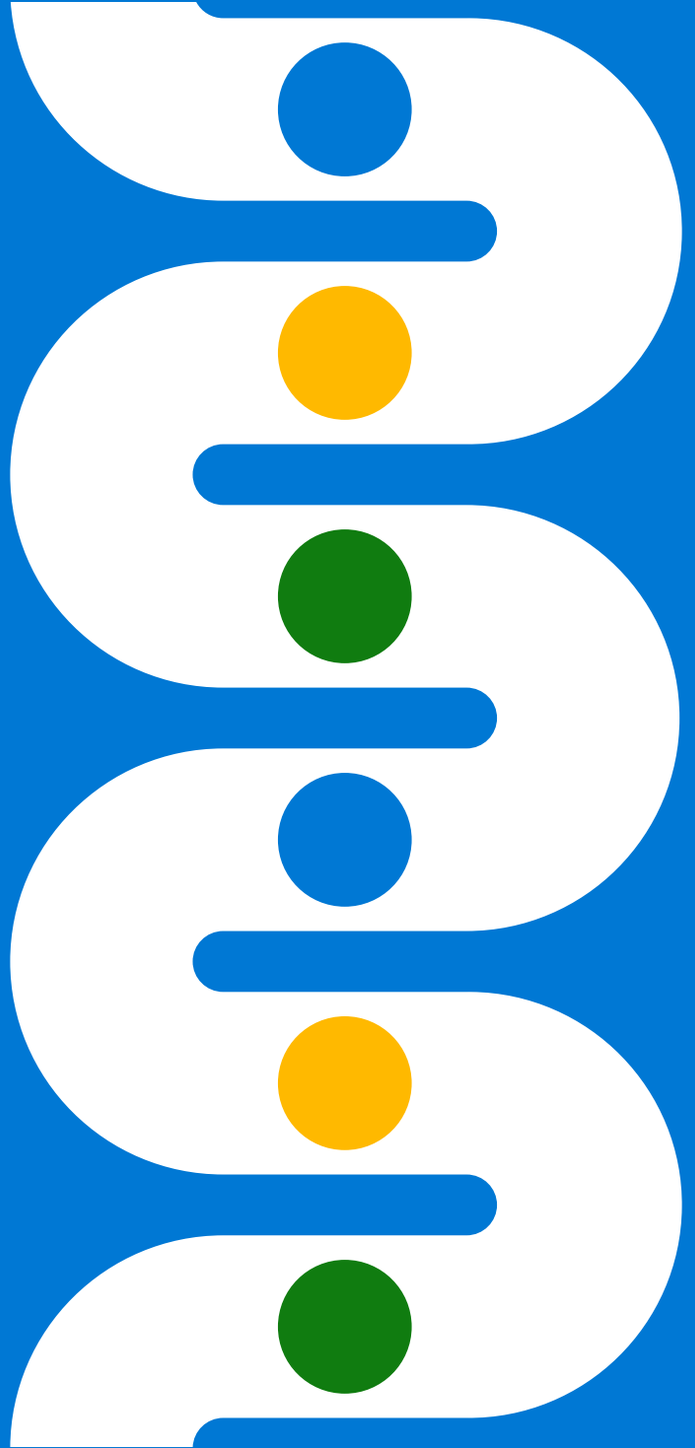
Protect blobs containers, file shares, and data lakes in Azure



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

Microsoft Defender for Resource Manager

Large attack vector due to high traffic and the central role it plays in Azure environments

Monitor all resource management operations performed in your organization

Detect suspicious Azure Resource Management activities and sends alerts

Microsoft Defender for DNS

Monitor all DNS queries from your Azure resources

Act on suspicious activity detected

Microsoft Defender for Key Vault

Detect unusual and potentially harmful attempts to exploit Azure Key Vault

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 you 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

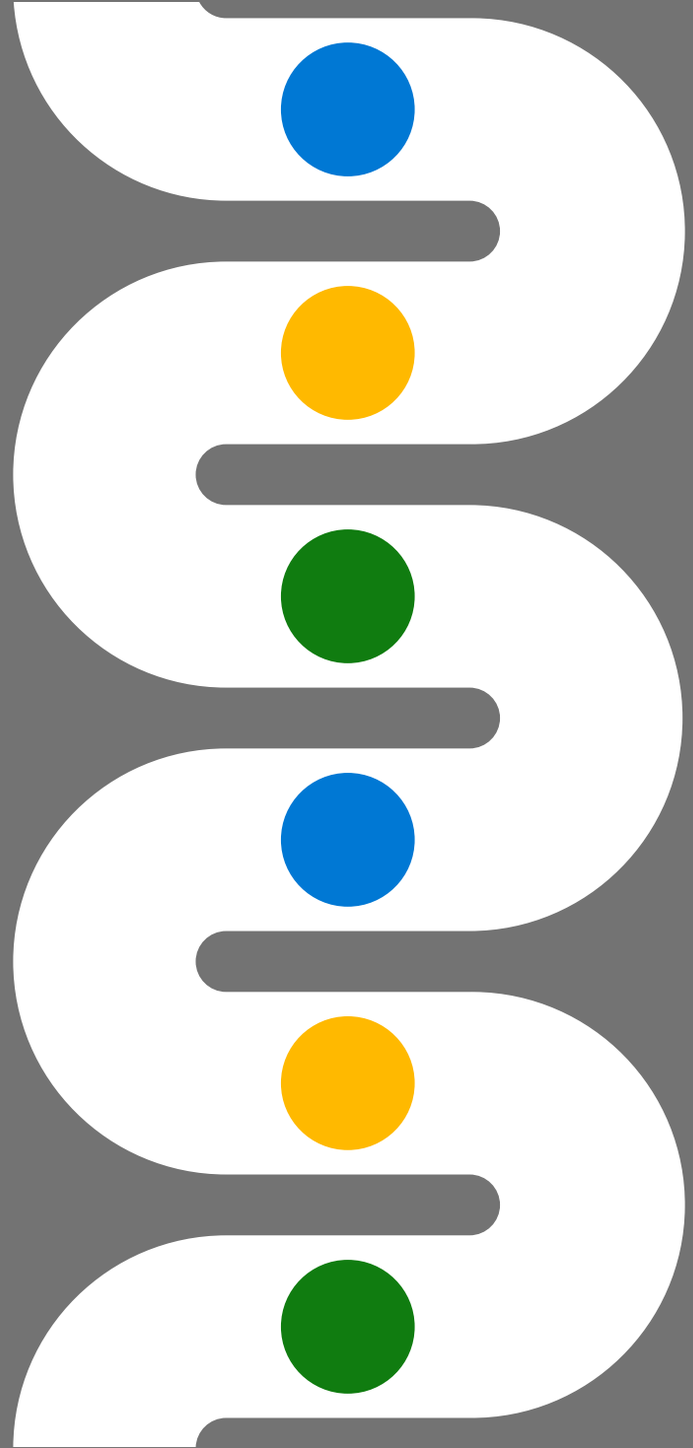
Onboard AWS, GCP and on-prem workloads with Azure Arc

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

Microsoft Security

Thank you

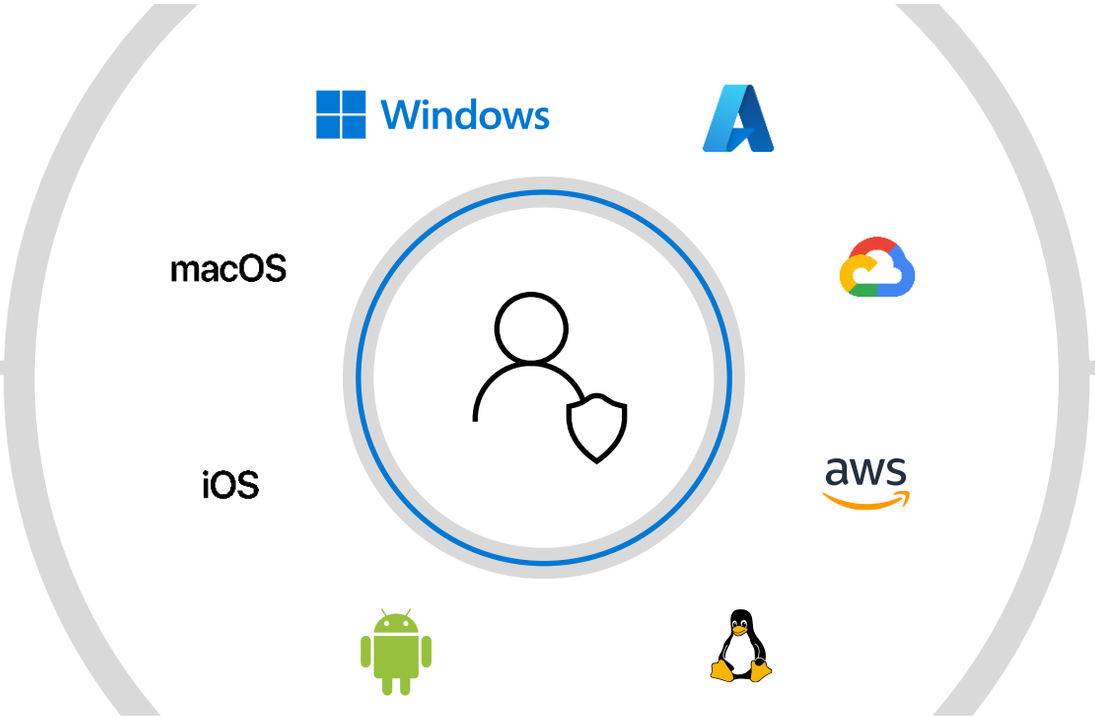
Most effective XDR to protect your users and cloud resources



SIEM

Microsoft Sentinel

Visibility across your entire organization



Existing security portfolio

Microsoft ecosystem

Microsoft 365 Defender

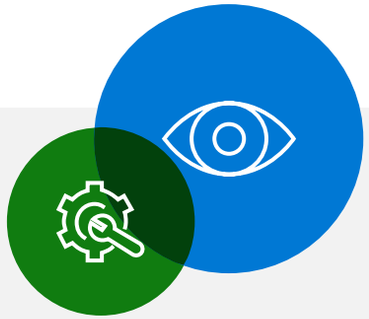
Secure your end users

Microsoft Defender for Cloud

Secure your infrastructure

XDR

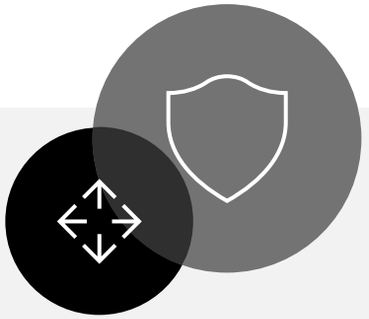
Microsoft XDR product vision



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**.