Microsoft Security

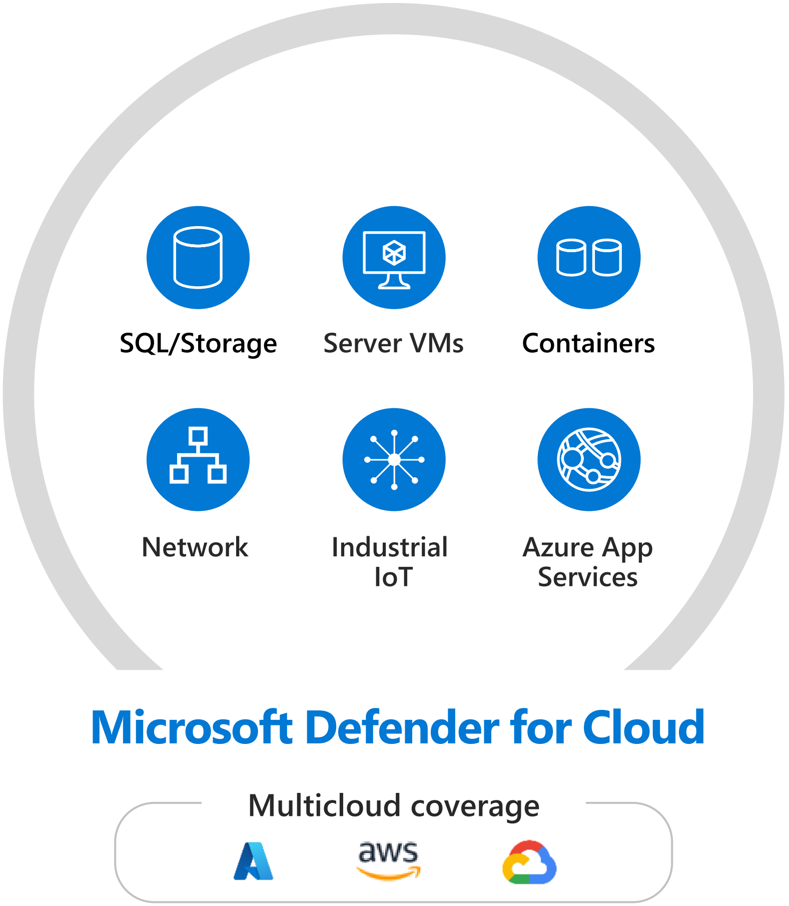
Microsoft Defender for Cloud

Protect your multicloud and hybrid environments
Cloud Workload Protection

Angelica Faber

Microsoft Defender for Cloud

Secure your critical cloud workloads running in AWS, Azure, and Google Cloud



SQL/Storage

Server VMs

Containers

Network

Industrial IoT

Azure App Services

Microsoft Defender for Cloud

Multicloud coverage

- Easy onboarding of AWS and GCP accounts and native support for Azure
- Get a bird's-eye view of your security posture and vulnerabilities across clouds with secure score
- Assess and implement best practices for compliance and security in the cloud
- Protect Amazon EKS clusters and AWS EC2 workloads
- Detect and block advanced malware and threats for Linux and Windows servers running in the cloud or on-premises

Cloud Workload Protection

Strengthen multi cloud security posture

Secure Score | Policies and compliance | Automation

Leveraging Azure Arc

Protect your multicloud and hybrid workloads

Servers | Cloud native workloads | Databases and storage

Azure service layers | IoT devices

Streamline security management

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

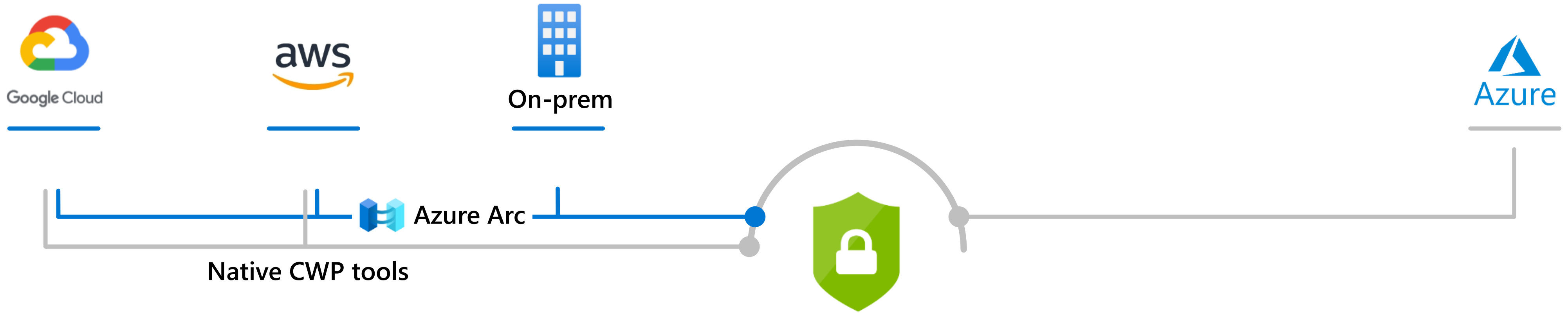
- GKE clusters
- Google Compute
- Unmanaged Kubernetes
- Unmanaged SQL

On-premise workloads

- Kubernetes
- SQL Servers
- Servers

On-premise

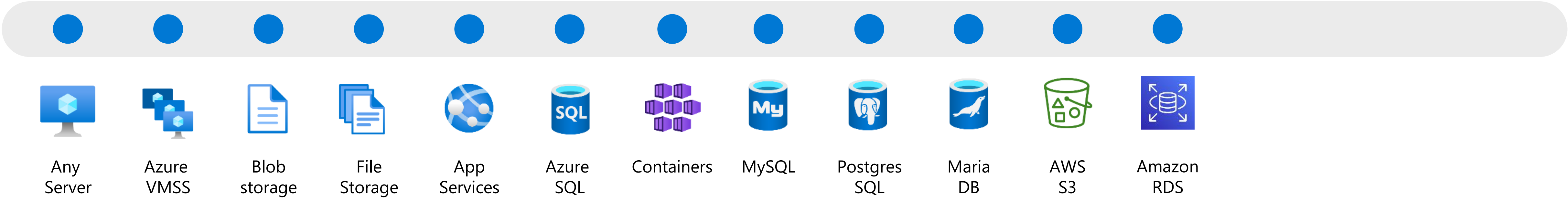
Multicloud & hybrid protection



Security posture & compliance	Secure score	Asset management	Regulatory compliance
Server protection	Threat detection	Vulnerability Assessment	
Automation & management at scale	Automation	SIEM integration	Export

Threat protection for cloud and hybrid workloads

Threat protection for common cloud resources



Any Server

Azure VMSS

Blob storage

File Storage

App Services

Azure SQL

Containers

MySQL

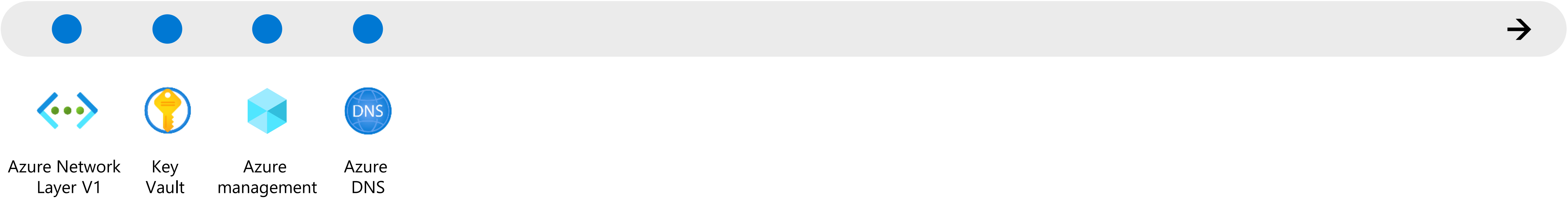
Postgres SQL

Maria DB

AWS S3

Amazon RDS

Threat protection for Azure service layer



Azure Network Layer V1

Key Vault

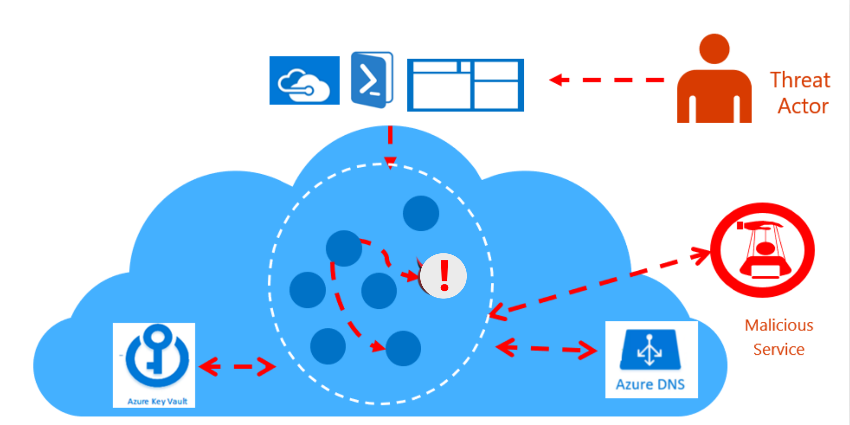
Azure management

Azure DNS

Defender for Azure Service Layers

Detect suspicious activities in Azure Management, Azure DNS and Azure Key Vault

- Just turn it **ON** (aka agentless solution)
- Protect **different** workloads **across** Azure services
- Detect threats that exploit **Azure service layers** attack surface



Defender for Resource Manager

Detects suspicious **Azure Resource Management activities** that indicate some workloads were potentially compromised

Defender for DNS

Detects suspicious **Azure DNS communication** that indicate some workloads were potentially compromised.

Defender for Key Vault

Detects suspicious or unusual **Azure Key Vault activities** that indicate some workloads certificates, keys and secrets were potentially compromised.

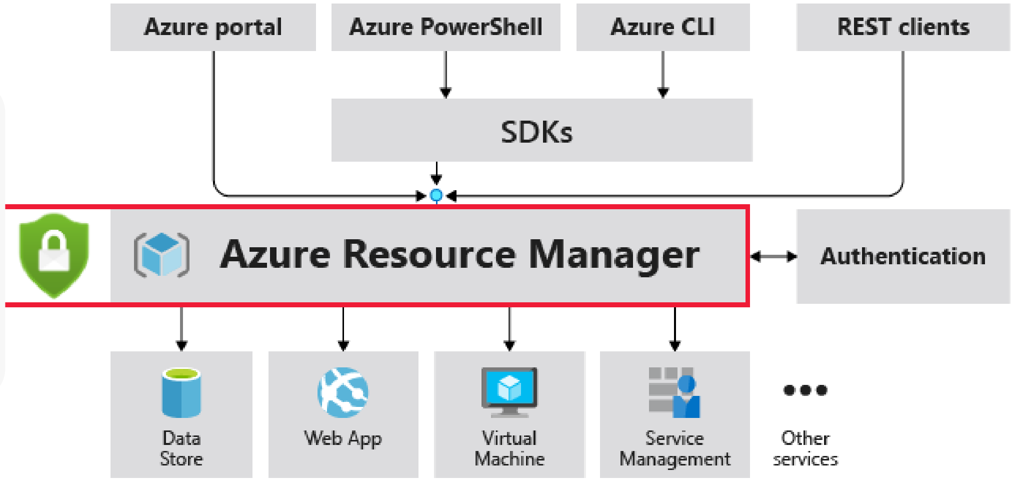
Defender for Resource Manager

Detection Examples

Suspicious resource management operations, such as operations from malicious IP addresses, disabling antimalware and suspicious scripts running in VM extensions

Use of exploitation toolkits like Microburst or PowerZure

Lateral movement from the Azure management layer to the Azure resources data plane

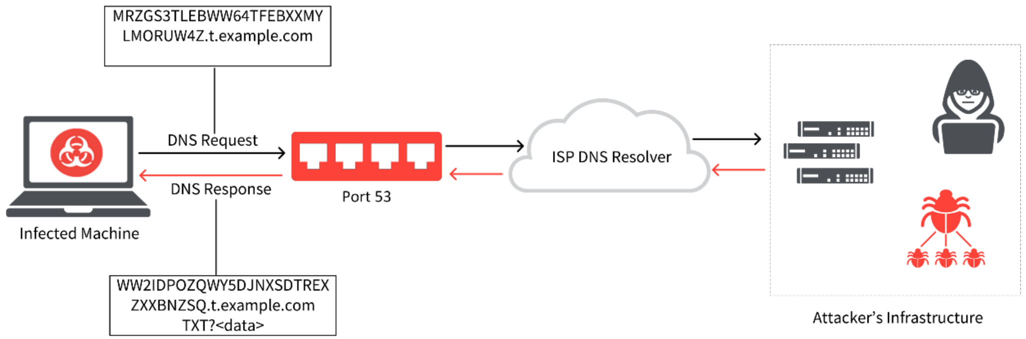


Defender for DNS

Detection Examples

Communication with malicious domains from your Azure resources

- **Communication with suspicious domains, C&C servers -** domain name associated with known command and control server
- **Bitcoin mining activity -** domain name associated with Bitcoin mining
- **Phishing activity -** domain name associated with Phishing
- **Dark web -** domain name associated with dark web



Sophisticated attacks through the DNS infra

- **DNS Tunneling -** exfiltrating data through DNS queries.
- **Network intrusion signature** - detecting signatures of botnets, malwares, trojans.
- **DNS cache poisoning -** Change DNS response to redirect users to attacker’s domain.
- **Sinkhole DNS -** DNS server that answer false results, allowing an attacker to redirect a system to a malicious destination.

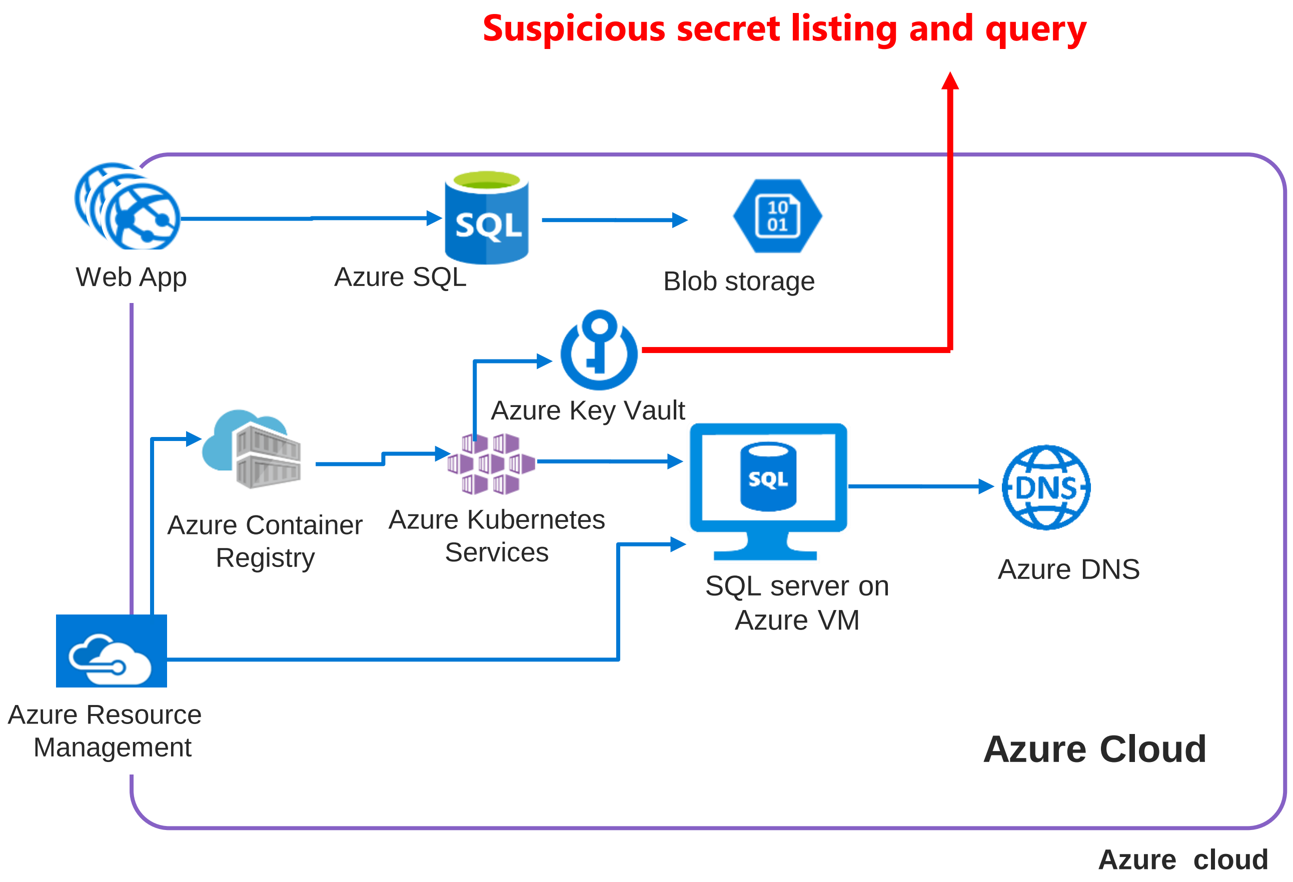
Defender for Key Vault

Detection Examples

Defender for Cloud

Defender for Key Vault

- 🔒 Recommends for Key Vault should be enabled
- 🔒 Recommends configuring private endpoint
- 🚨 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 ir key vault
- 🚨 Detects unusual user accessed a key vault



Microsoft Defender for Servers

Complement EDR with increased visibility, detection, and prevention

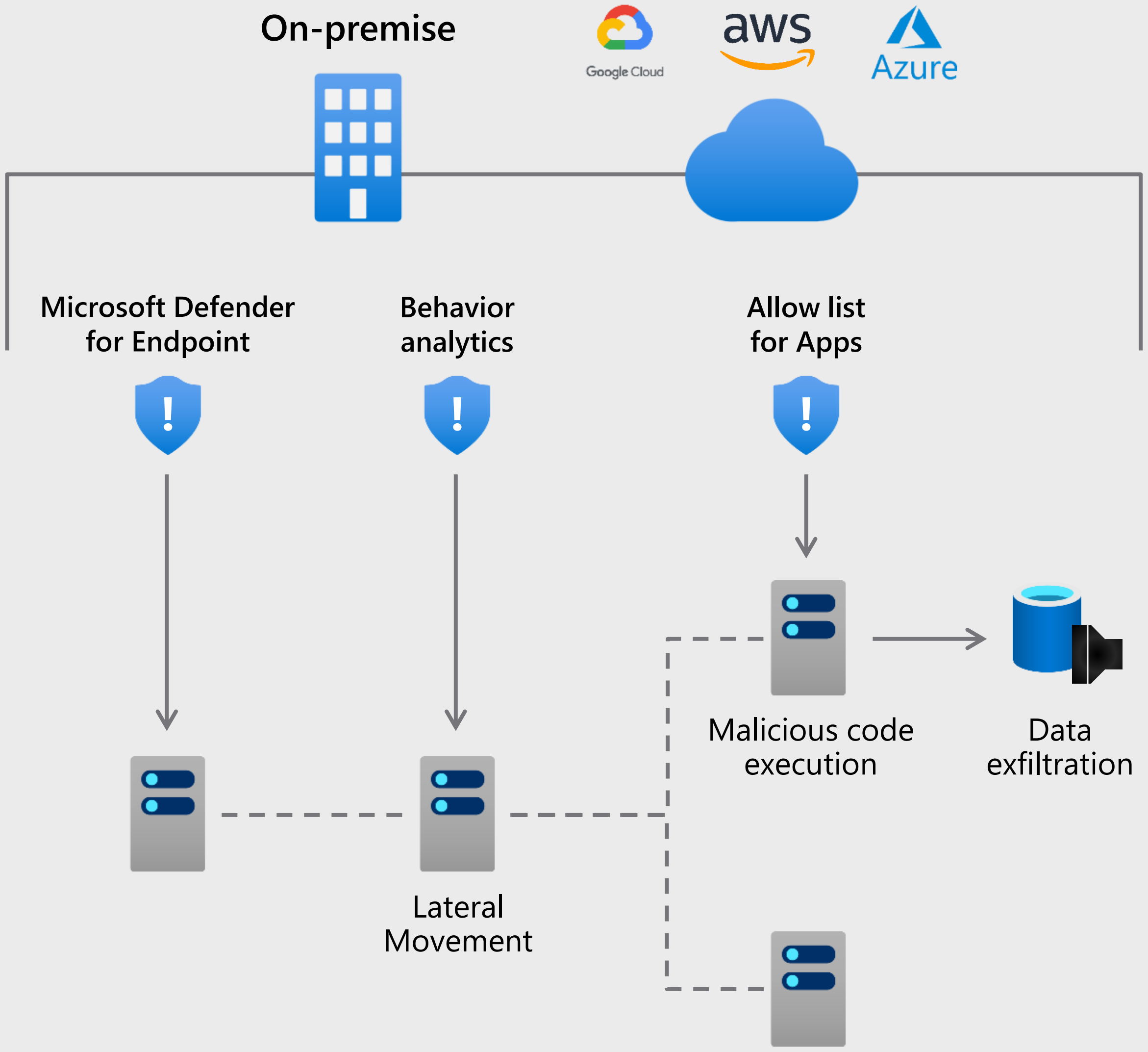
Extend Visbility and Protection to On-Premise and Multi-Cloud Workloads

Advanced Protection and Detection Capabilities leveraging ML

Harden machines against malware and comply with regulatory frameworks

Mitigate network exposure of management ports

Integration with Microsoft Defender for Endpoint



Feature Comparison

		Microsoft Defender for Cloud		
Feature / Feature set	Defender for Endpoint for Servers P2 ($5)	Free	Defender for Servers P1 ($5)	Defender for Servers P2 ($15)
CSPM – anti-malware health and OS baselines, system updates		🟩	🟩	🟩
Vulnerability assessment - BYOL		🟩	🟩	🟩
Automatic onboarding of agents		🟩	🟩	🟩
Asset Discovery	🟩		🟩	🟩
Threat & Vulnerability Management	🟩		🟩	🟩
Attack Surface Reduction	🟩		🟩	🟩
Next Gen Antivirus Protection	🟩		🟩	🟩
Endpoint Detection & Response	🟩		🟩	🟩
Automated Self-healing	🟩		🟩	🟩
License for Microsoft Defender for Endpoint P1 for servers			🟩	🟩
MDE data integration – Alerts, software inventory, TVM VA			🟩	🟩
Log-analytics (500MB free)				🟩
Security Policy & Regulatory Compliance				🟩
Vulnerability Assessment using Qualys				🟩
Threat Detections: OS level, network layer, control plane				🟩
Adaptive application controls				🟩
File integrity monitoring				🟩
Just-in time VM access				🟩
Adaptive Network Hardening				🟩

Turn on built-in vulnerability assessment for VMs

Available as part of Defender for Servers

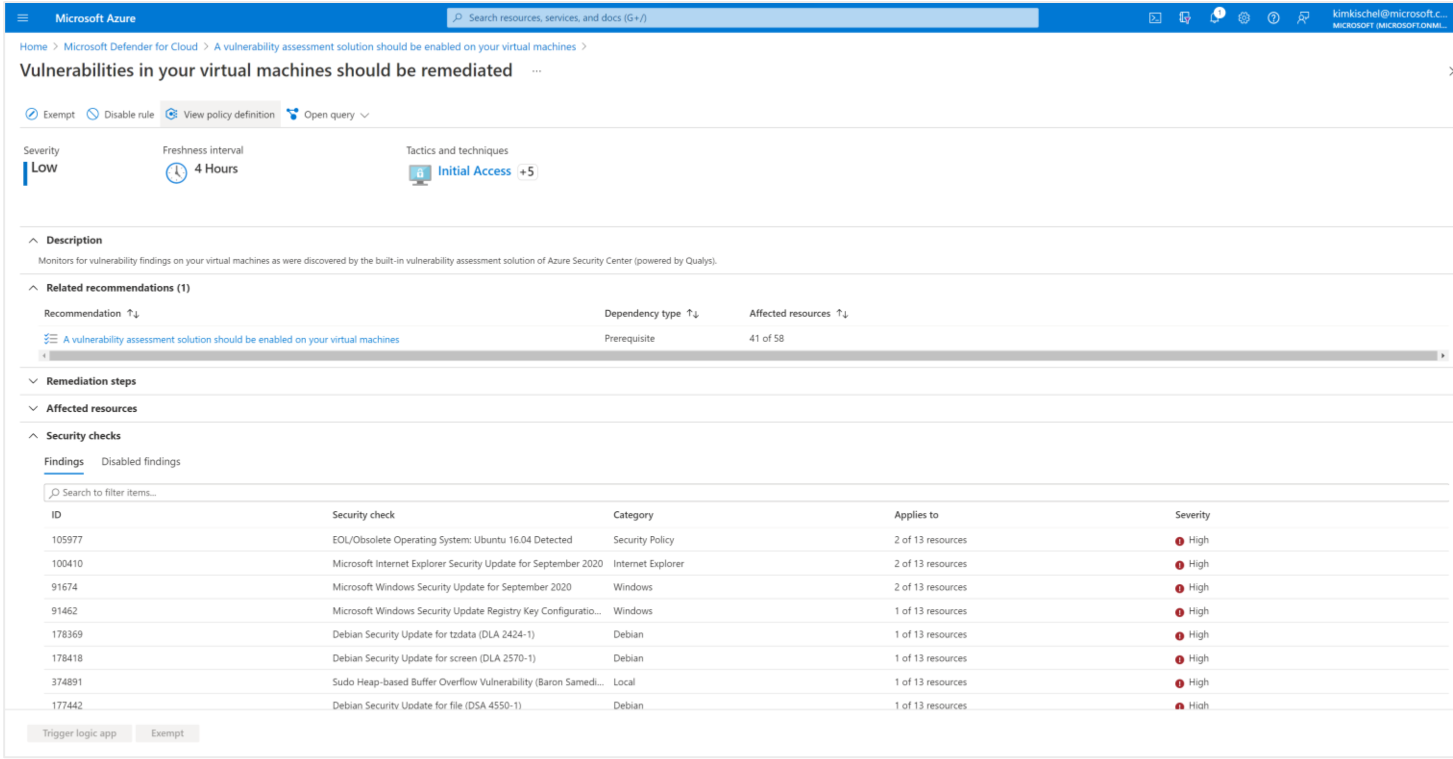
Google Cloud aws Azure

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.


Microsoft Azure
Search resources, services, and docs (G+/)
kimkischel@microsoft.c...
MICROSOFT (MICROSOFT.ONMI...
Home > Microsoft Defender for Cloud > A vulnerability assessment solution should be enabled on your virtual machines >
Exempt
Disable rule
View policy definition
Open query
Trigger logic app
Exempt

Vulnerabilities in your virtual machines should be remediated ...

Severity: Low

Freshness interval: 4 Hours

Tactics and techniques: Initial Access +5

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)

Recommendation ↑↓	Dependency type ↑↓	Affected resources ↑↓
A vulnerability assessment solution should be enabled on your virtual machines	Prerequisite	41 of 58

Remediation steps

Affected resources

Security checks

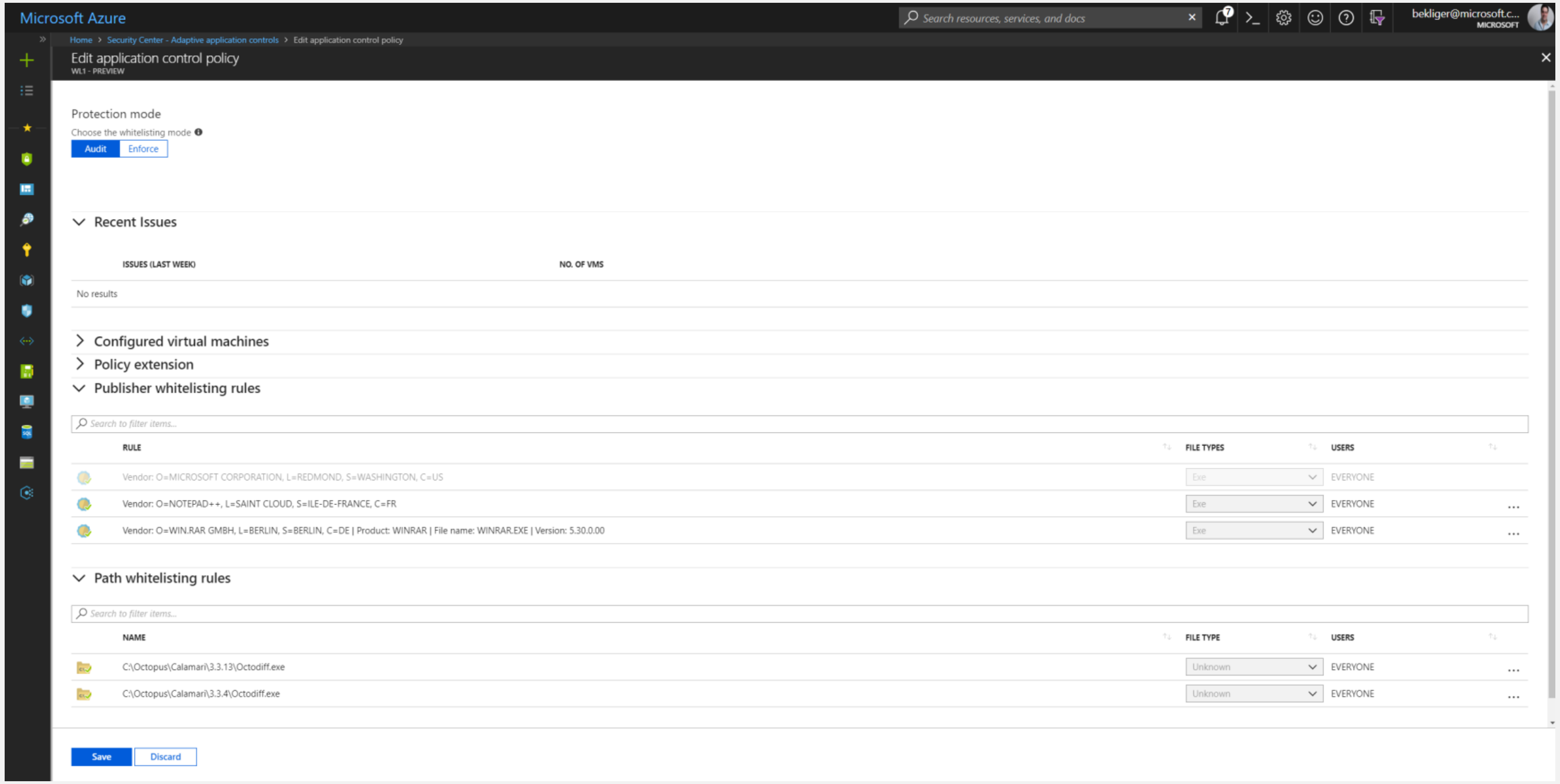
Findings | Disabled findings

Search to filter items...

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

Adaptive Application Controls

- Identify potential malware, even any that might be missed by antimalware solutions
- Improve compliance with local security policies that dictate the use of only licensed software
- Identify outdated or unsupported versions of applications
- Identify software that's banned by your organization
- Increase oversight of apps that access sensitive data


Microsoft Azure
Search resources, services, and docs
bekliger@microsoft.c...
MICROSOFT
Home > Security Center - Adaptive application controls > Edit application control policy

Edit application control policy
WL1 - PREVIEW

Protection mode

Choose the whitelisting mode

[✓ Audit] Enforce

Recent Issues

ISSUES (LAST WEEK)	NO. OF VMS
No results	

Configured virtual machines

Policy extension

Publisher whitelisting rules

Search to filter items...

RULE	FILE TYPES	USERS
Vendor: O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US	Exe	EVERYONE
Vendor: O=NOTEPAD++, L=SAINT CLOUD, S=ILE-DE-FRANCE, C=FR	Exe	EVERYONE
Vendor: O=WIN.RAR GMBH, L=BERLIN, S=BERLIN, C=DE | Product: WINRAR | File name: WINRAR.EXE | Version: 5.30.0.00	Exe	EVERYONE

Path whitelisting rules

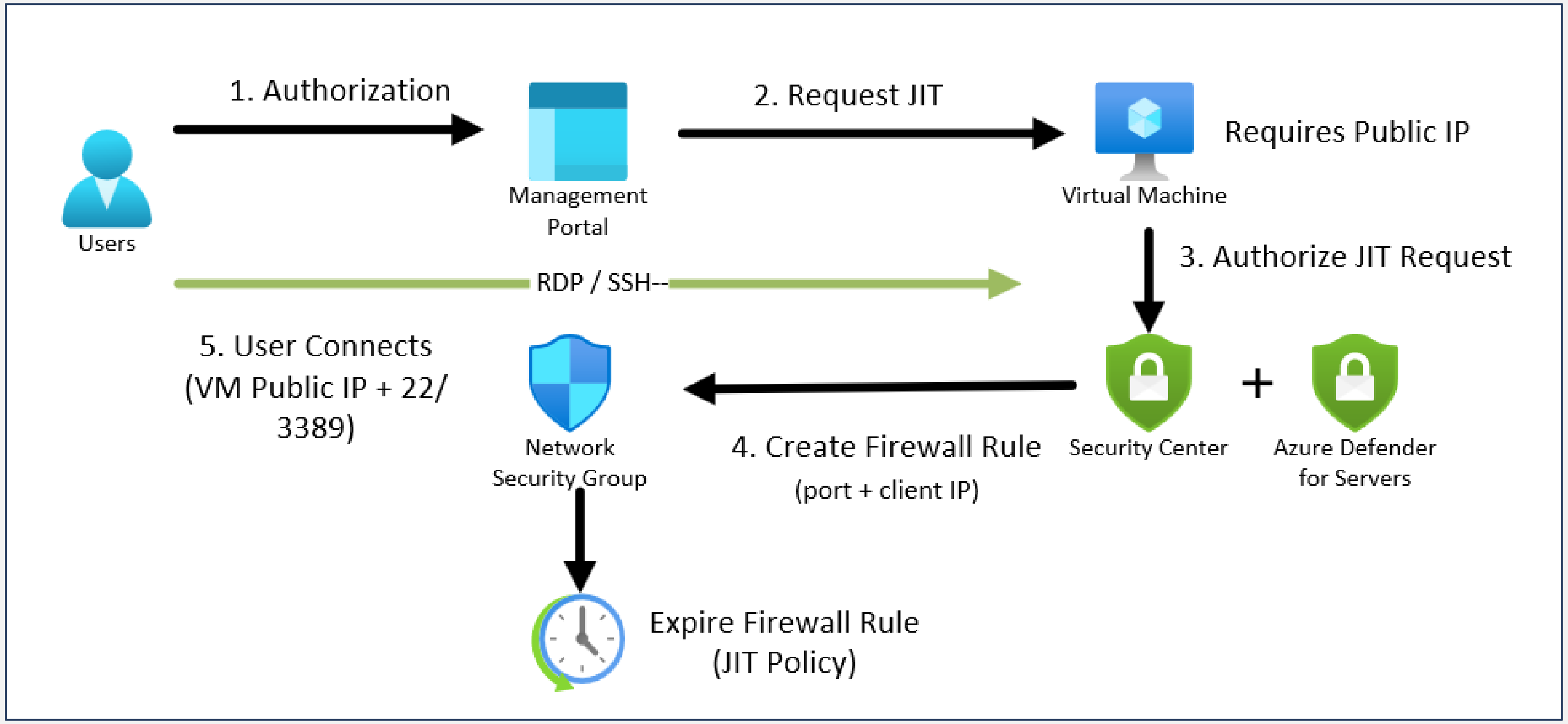
Search to filter items...

NAME	FILE TYPE	USERS
C:\Octopus\Calamari\3.3.13\Octodiff.exe	Unknown	EVERYONE
C:\Octopus\Calamari\3.3.4\Octodiff.exe	Unknown	EVERYONE

Just in Time Virtual Machine Access

Azure Virtual Machines Only

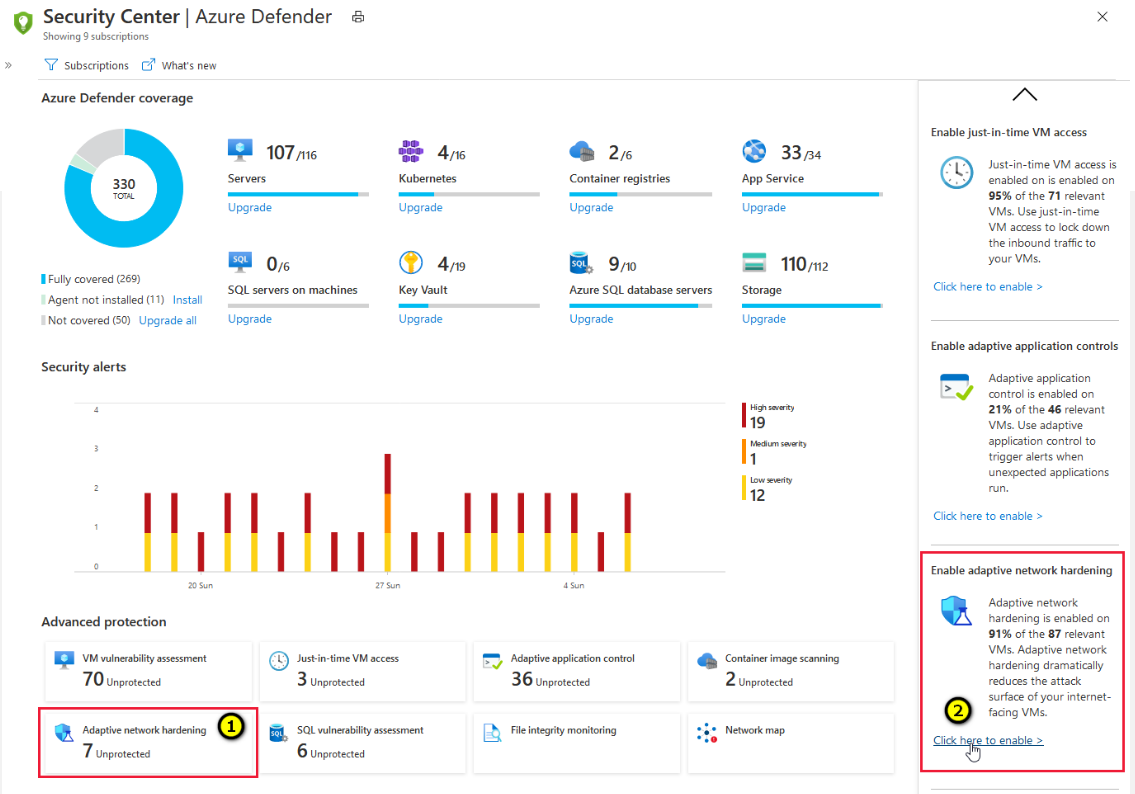
- Lock down the inbound traffic to your VMs, reducing exposure to attacks while providing easy access to connect to VMs when needed
- Provide Just in Time Access to RDP and SSH
- Security Center configures the NSGs and Azure Firewall to allow inbound traffic to the selected ports from the relevant IP address (or range)



Adaptive Network Hardening

Azure Virtual Machines Only

- 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



Security Center | Azure Defender

Showing 9 subscriptions

Subscriptions · What's new

Azure Defender coverage

330 TOTAL

- Fully covered (269)
- Agent not installed (11) Install
- Not covered (50) Upgrade all

107/116 Servers Upgrade	4/16 Kubernetes Upgrade	2/6 Container registries Upgrade	33/34 App Service Upgrade
0/6 SQL servers on machines Upgrade	4/19 Key Vault Upgrade	9/10 Azure SQL database servers Upgrade	110/112 Storage Upgrade

Security alerts

High severity 19

Medium severity 1

Low severity 12

Advanced protection

VM vulnerability assessment 70 Unprotected	Just-in-time VM access 3 Unprotected	Adaptive application control 36 Unprotected	Container image scanning 2 Unprotected
Adaptive network hardening (1) 7 Unprotected	SQL vulnerability assessment 6 Unprotected	File integrity monitoring	Network map

Enable just-in-time VM access

Just-in-time VM access is enabled on is enabled on **95%** of the **71** relevant VMs. Use just-in-time VM access to lock down the inbound traffic to your VMs.

Click here to enable >

Enable adaptive application controls

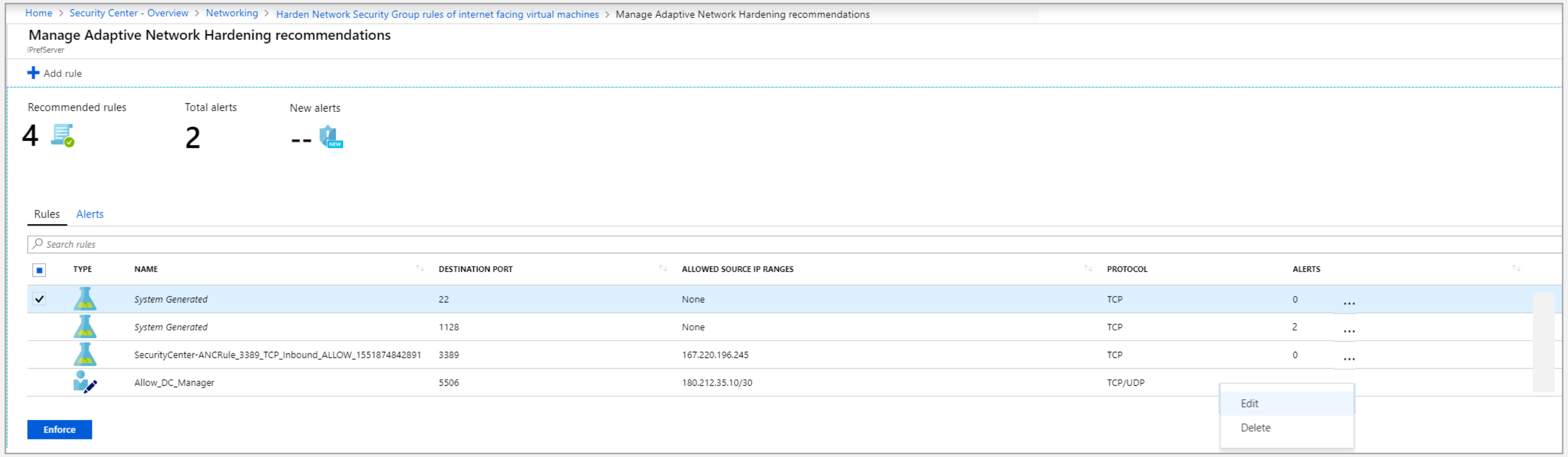
Adaptive application control is enabled on **21%** of the **46** relevant VMs. Use adaptive application control to trigger alerts when unexpected applications run.

Click here to enable >

Enable adaptive network hardening

Adaptive network hardening is enabled on **91%** of the **87** relevant VMs. Adaptive network hardening dramatically reduces the attack surface of your internet-facing VMs.

(2) Click here to enable >



Home > Security Center - Overview > Networking > Harden Network Security Group rules of internet facing virtual machines > Manage Adaptive Network Hardening recommendations

Manage Adaptive Network Hardening recommendations

iPrefServer

Add rule

Recommended rules	Total alerts	New alerts
4	2	--

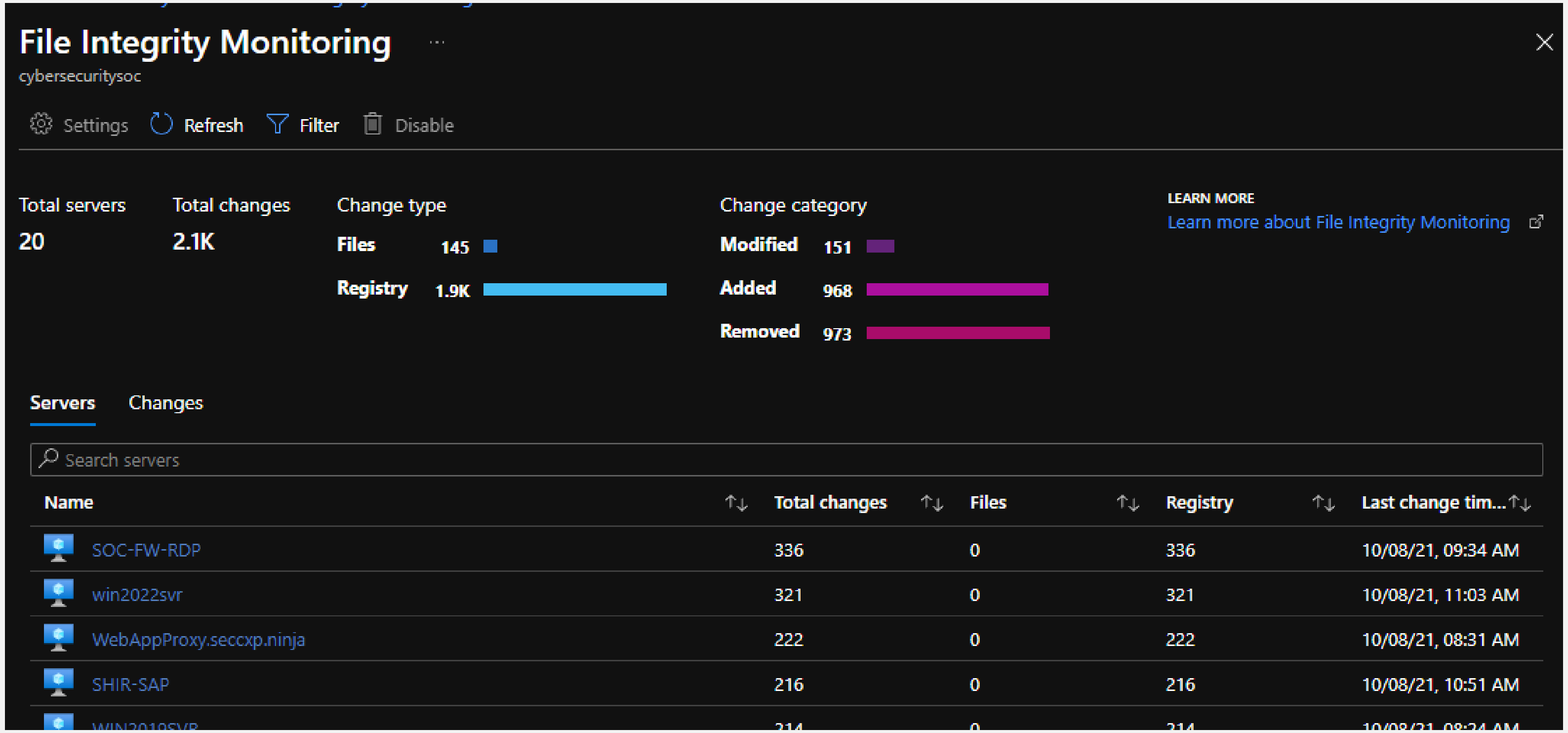
Rules · Alerts

Search rules

■	TYPE	NAME	DESTINATION PORT	ALLOWED SOURCE IP RANGES	PROTOCOL	ALERTS
✓		*System Generated*	22	None	TCP	0
		System Generated	1128	None	TCP	2
		SecurityCenter-ANCRule_3389_TCP_Inbound_ALLOW_1551874842891	3389	167.220.196.245	TCP	0
		Allow_DC_Manager	5506	180.212.35.10/30	TCP/UDP	

File integrity monitoring

- Examines files and registries of the operating system, application software, and others for changes that might indicate an attack
- Validates the integrity of Windows files, Windows registry, and Linux files.
- Select the files that you want to be monitored by enabling File Integration Monitoring (FIM)



File Integrity Monitoring

cybersecuritysoc

Total servers 20

Total changes 2.1K

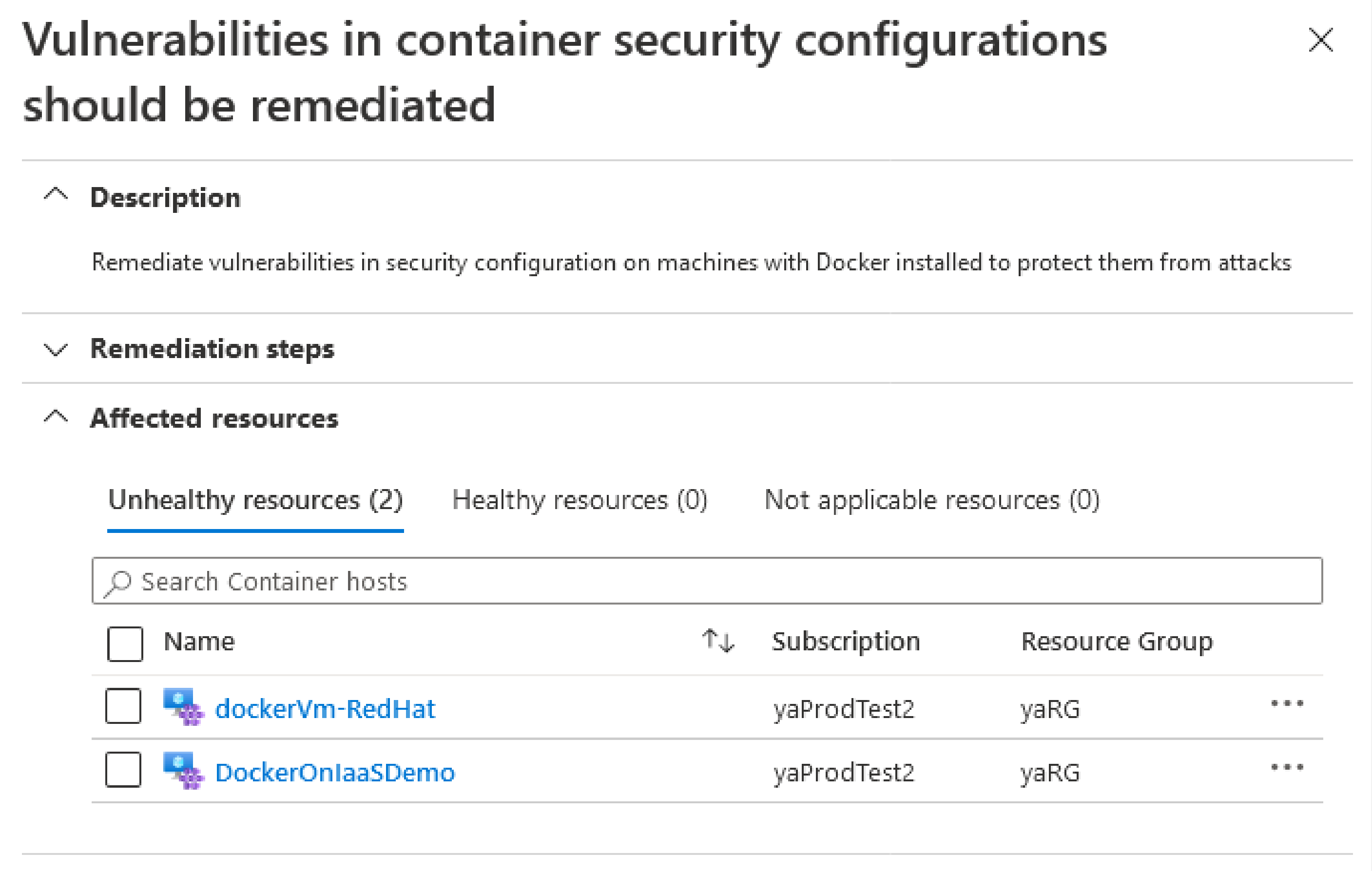
Change type	
Files	145
Registry	1.9K

Change category	
Modified	151
Added	968
Removed	973

Name	Total changes	Files	Registry	Last change tim...
SOC-FW-RDP	336	0	336	10/08/21, 09:34 AM
win2022svr	321	0	321	10/08/21, 11:03 AM
WebAppProxy.seccxp.ninja	222	0	222	10/08/21, 08:31 AM
SHIR-SAP	216	0	216	10/08/21, 10:51 AM
WIN2019SVR	314	0	314	10/08/21, 08:24 AM

Docker Host Hardening

- Identifies unmanaged containers hosted on IaaS Linux VMs, or other Linux machines running Docker containers
- Continuously assesses the configurations of containers
- Generates security recommendations based on vulnerabilities and the CIS benchmark



Vulnerabilities in container security configurations should be remediated

Description

Remediate vulnerabilities in security configuration on machines with Docker installed to protect them from attacks

Remediation steps

Affected resources

Unhealthy resources (2) | Healthy resources (0) | Not applicable resources (0)

Search Container hosts

□	Name	Subscription	Resource Group	
□	dockerVm-RedHat	yaProdTest2	yaRG	···
□	DockerOnIaaSDemo	yaProdTest2	yaRG	···

Fileless Attack Detection

Complement EDR with increased detection coverage

Google Cloud

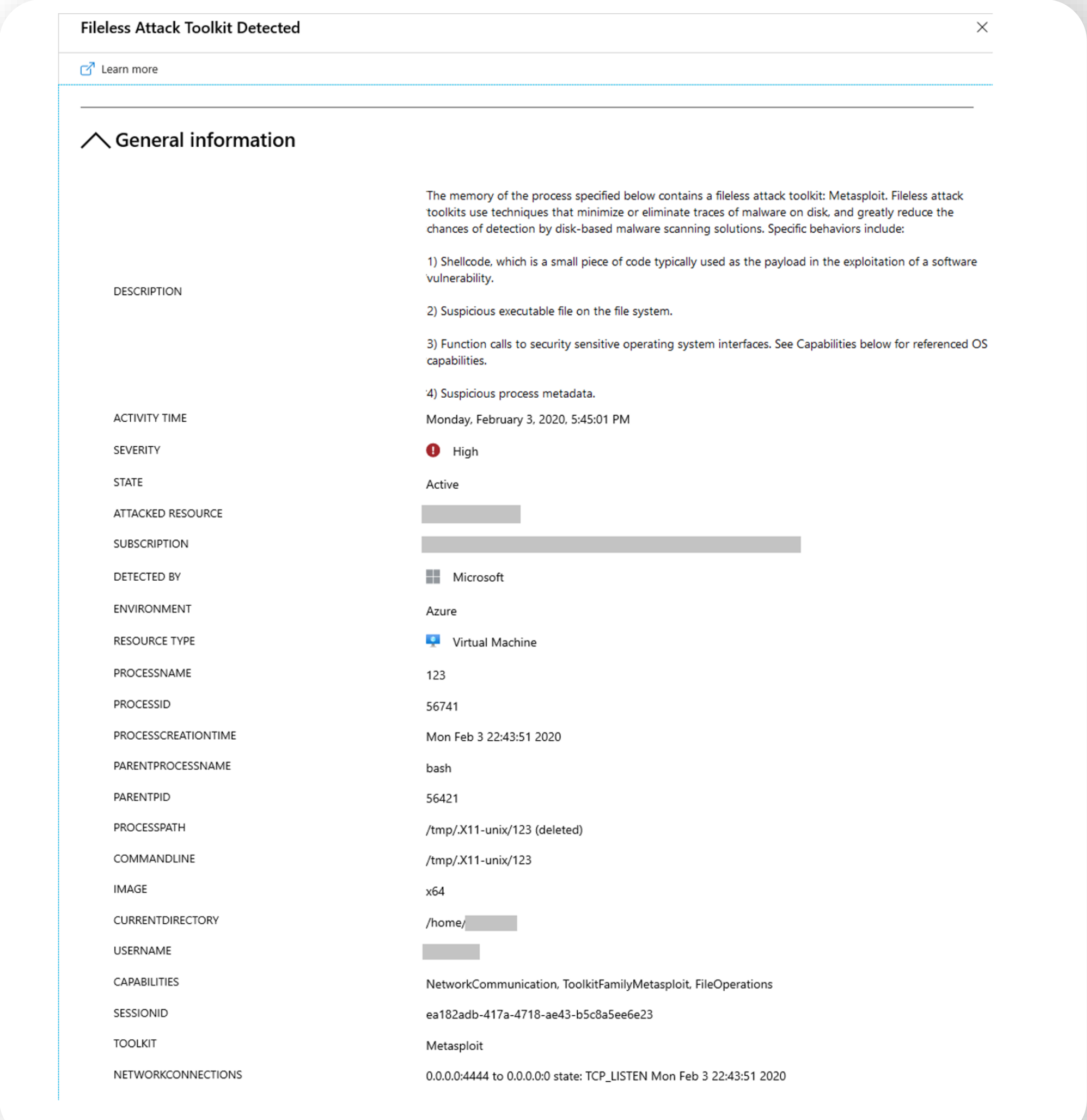
aws

Azure

Automated memory forensic techniques identify fileless attack toolkits, techniques, and behaviors

Periodically scans your machine at runtime, and extracts insights directly from the memory of processes to detect:

- Well-known toolkits and crypto mining software
- Shellcode, which is a small piece of code typically used as the payload in the exploitation of a software vulnerability.
- Injected malicious executable in process memory, LD_PRELOAD based rootkits to preload malicious libraries.
- Elevation of privilege of a process from non-root to root.
- Remote control of another process using ptrace.



Fileless Attack Toolkit Detected

General information

DESCRIPTION	The memory of the process specified below contains a fileless attack toolkit: Metasploit. Fileless attack toolkits use techniques that minimize or eliminate traces of malware on disk, and greatly reduce the chances of detection by disk-based malware scanning solutions. Specific behaviors include: 1) Shellcode, which is a small piece of code typically used as the payload in the exploitation of a software vulnerability. 2) Suspicious executable file on the file system. 3) Function calls to security sensitive operating system interfaces. See Capabilities below for referenced OS capabilities. 4) Suspicious process metadata.
ACTIVITY TIME	Monday, February 3, 2020, 5:45:01 PM
SEVERITY	● High
STATE	Active
ATTACKED RESOURCE	[redacted]
SUBSCRIPTION	[redacted]
DETECTED BY	Microsoft
ENVIRONMENT	Azure
RESOURCE TYPE	Virtual Machine
PROCESSNAME	123
PROCESSID	56741
PROCESSCREATIONTIME	Mon Feb 3 22:43:51 2020
PARENTPROCESSNAME	bash
PARENTPID	56421
PROCESSPATH	/tmp/.X11-unix/123 (deleted)
COMMANDLINE	/tmp/.X11-unix/123
IMAGE	x64
CURRENTDIRECTORY	/home/[redacted]
USERNAME	[redacted]
CAPABILITIES	NetworkCommunication, ToolkitFamilyMetasploit, FileOperations
SESSIONID	ea182adb-417a-4718-ae43-b5c8a5ee6e23
TOOLKIT	Metasploit
NETWORKCONNECTIONS	0.0.0.0:4444 to 0.0.0.0:0 state: TCP_LISTEN Mon Feb 3 22:43:51 2020

Workload protection

Defender for Storage – **security alerts suite**

Suspicious access patterns

- Access from a **Tor exit node**
- Access from **suspicious IPs**
- Access from **suspicious applications**
- Unusual anonymous access
- Access from an unusual location
- Access from unusual application

Upload of malicious content

- **Distribution of malware** from the storage account
- Unusual upload of files
- **Potential malware** upload

Suspicious behavior

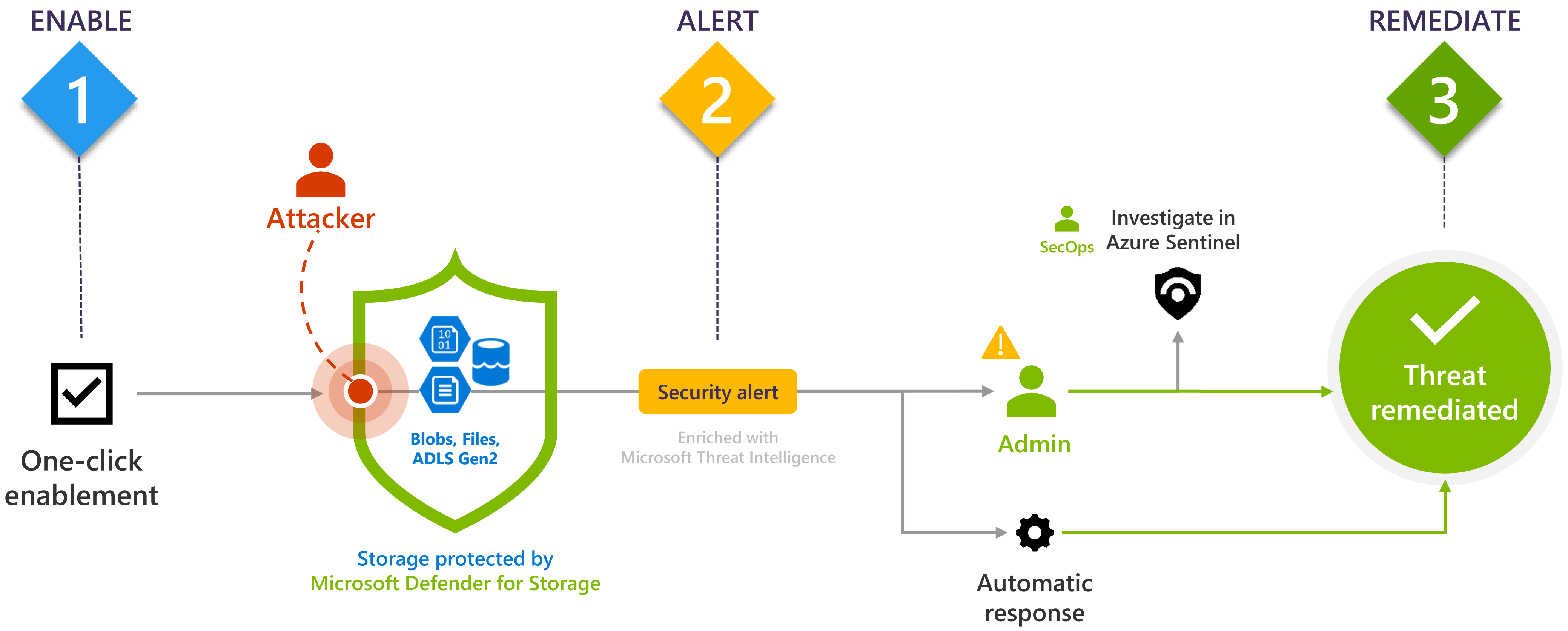
- Unusual amount of **data extracted**
- Unusual **access inspection**
- Unusual change of permissions
- Unusual data exploration
- Unusual **deletion**

Other threats

- **Scanning attempts of publicly open containers**
- **Potentially sensitive data** has been **made publicly available**
- **Phishing** content hosted on an account

Detections match the techniques of Enterprise Techniques chart, by MITRE

Microsoft Defender for Storage - Overview



Azure Native Security

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

Rich Detection Suite

Covering top Storage threats powered by Microsoft Threat Intelligence

Response at scale

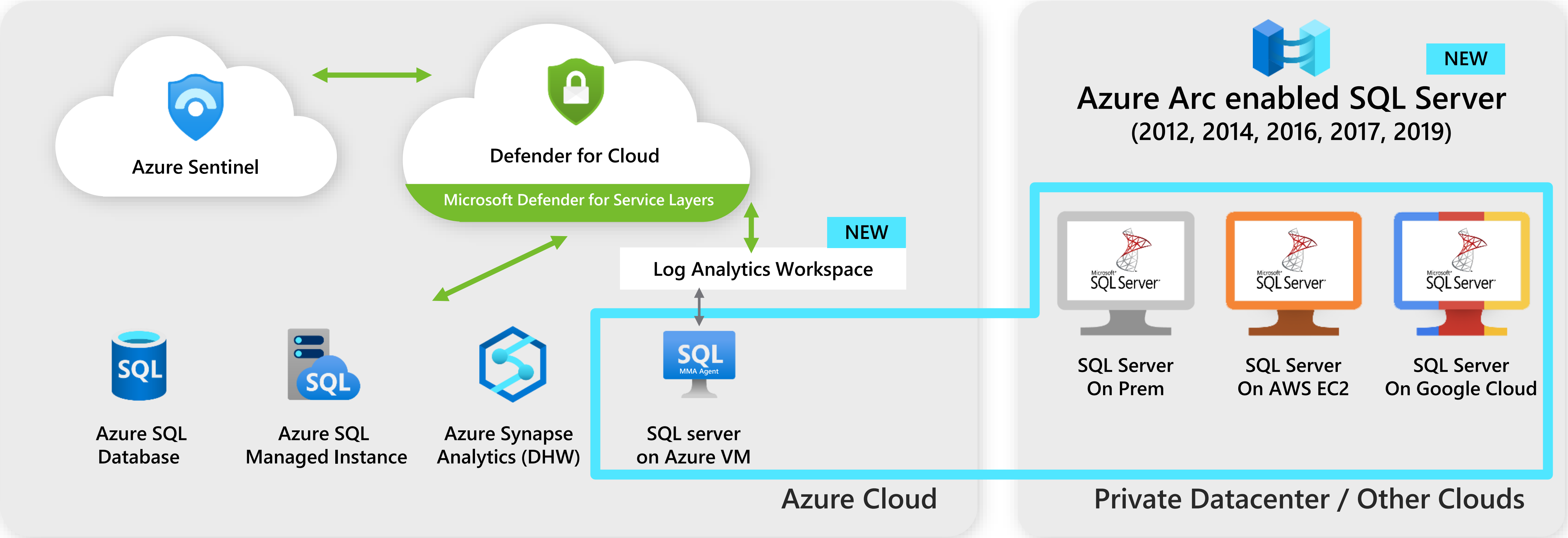
Reduce frictions preventing and responding to top threats

Centralized & Integrated

Centralize security across all data assets managed by Azure and built-in integration services such as Azure Sentinel

Microsoft Defender for SQL multi-cloud support

Advanced security capabilities to protect every SQL workload in Azure and outside Azure



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

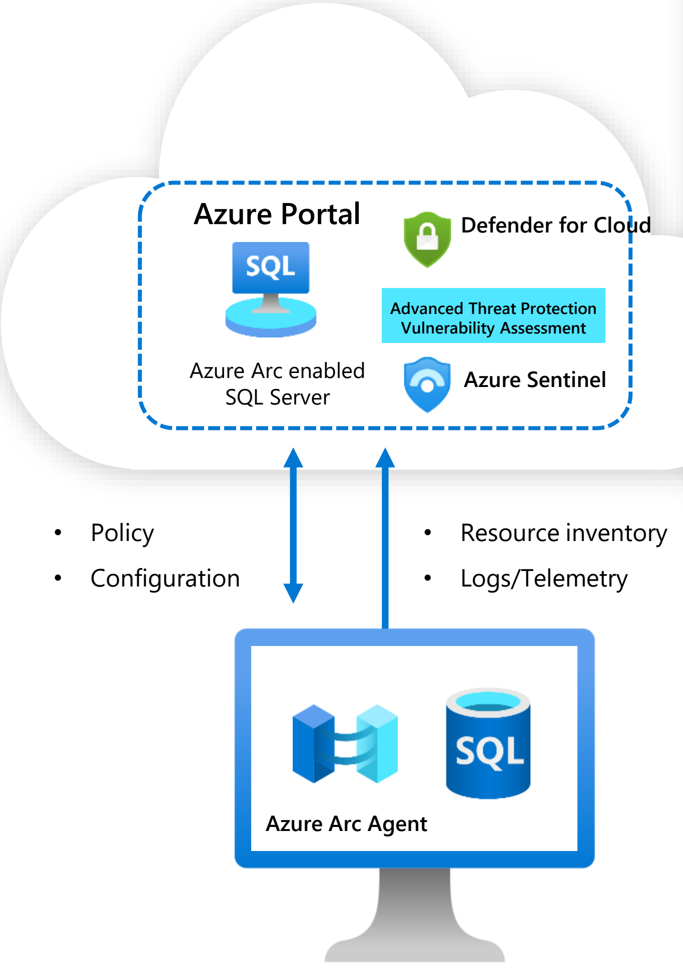
Vulnerability Assessment: discover and remediate security misconfigurations in SQL servers across hybrid estate

NEW

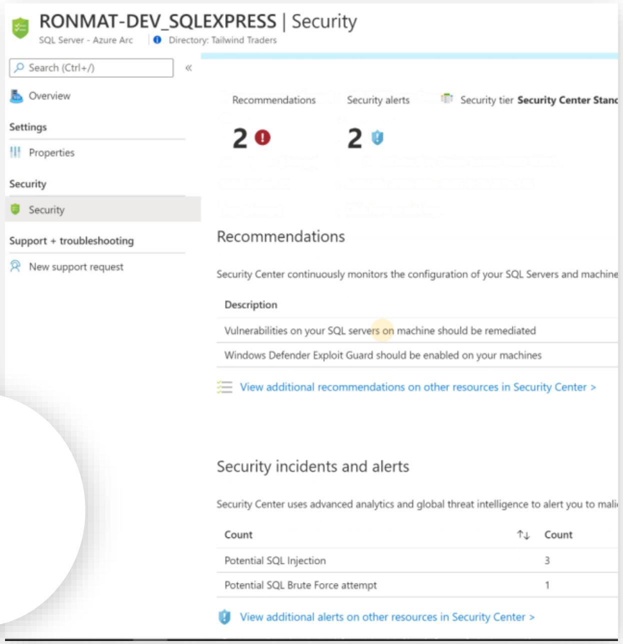
Microsoft Defender for SQL servers outside Azure

Advanced security capabilities to protect SQL servers outside Azure

- Just turn it ON
- Support SQL Servers >2012
- Detects potential SQL injections, unusual access and suspicious queries
- Identify security misconfigurations, allow secure score tracking & compliance report
- View alerts and security findings across hybrid SQL estate using Defender for Cloud
- Investigate alerts using Azure Sentinel



Azure Arc Enabled SQL Server



RONMAT-DEV_SQLEXPRESS | Security

SQL Server - Azure Arc | Directory: Tailwind Traders

Search (Ctrl+/) «

Overview

Settings

Properties

Security

Security

Support + troubleshooting

New support request

Recommendations 2 | Security alerts 2 | Security tier **Security Center Stanc**

Recommendations

Security Center continuously monitors the configuration of your SQL Servers and machine

Description
Vulnerabilities on your SQL servers on machine should be remediated
Windows Defender Exploit Guard should be enabled on your machines

View additional recommendations on other resources in Security Center >

Security incidents and alerts

Security Center uses advanced analytics and global threat intelligence to alert you to mali

Count ↑↓	Count
Potential SQL Injection	3
Potential SQL Brute Force attempt	1

View additional alerts on other resources in Security Center >

Protecting against common threats in SQL servers

Defender for Cloud

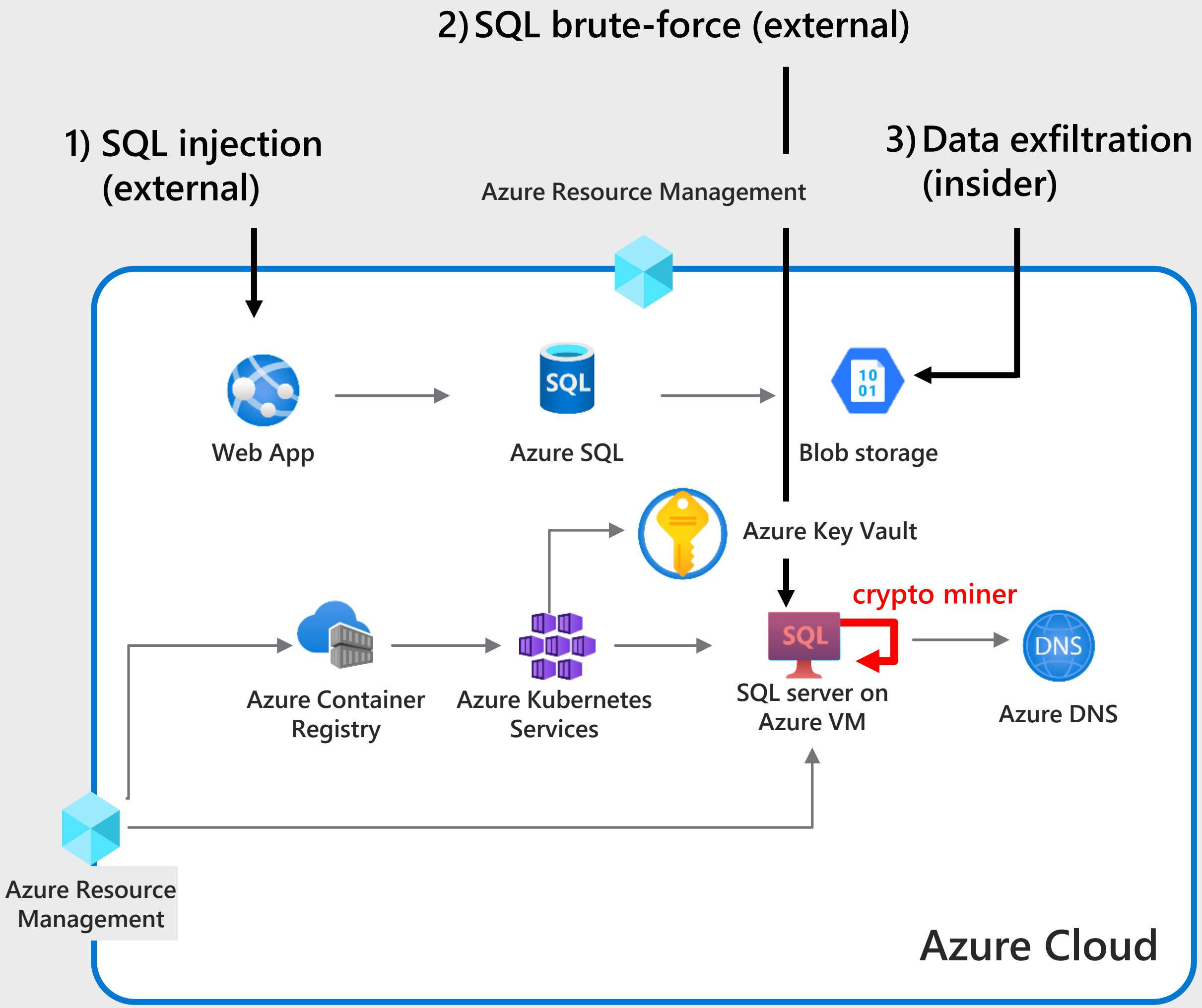
Microsoft Defender for Service Layers

Recommends

- To disable 'sa' login
- To disable ‘xp_cmdshell‘

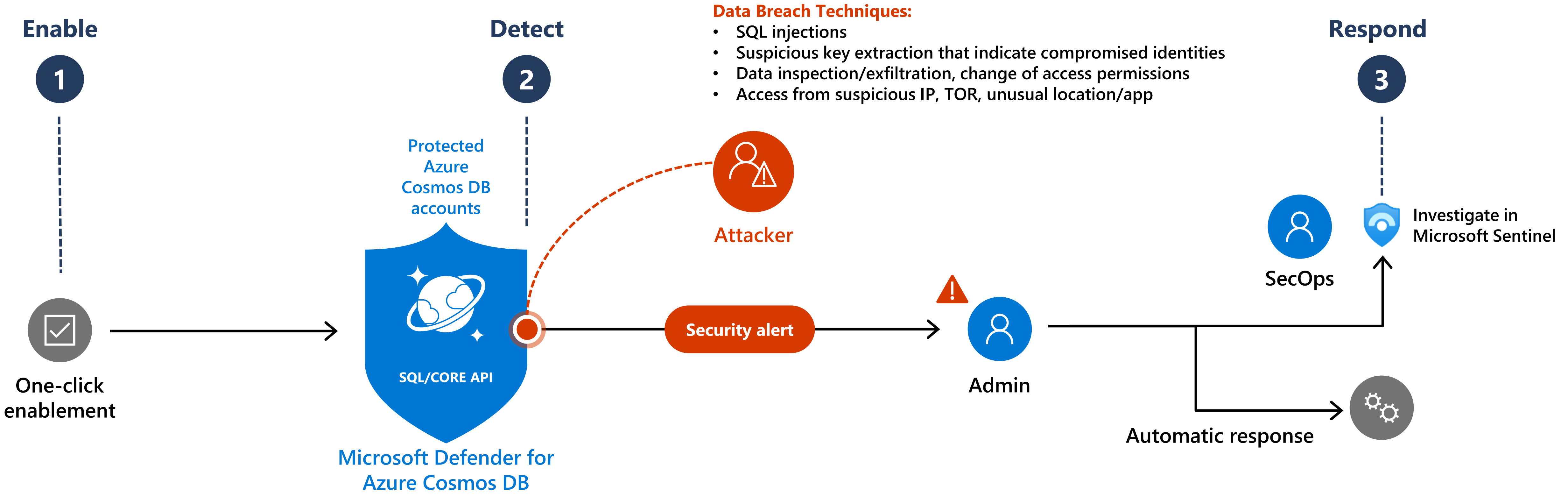
Detects

- Potential SQL Injection
- SQL brute force
- Crypto miner in a VM
- Potential data exfiltration


2) SQL brute-force (external)
1) SQL injection (external)
Azure Resource Management
3) Data exfiltration (insider)
Web App
Azure SQL
Blob storage
Azure Key Vault
crypto miner
Azure Container Registry
Azure Kubernetes Services
SQL server on Azure VM
Azure DNS
Azure Resource Management
Azure Cloud

New: Microsoft Defender for Azure Cosmos DB

Protect Azure Cosmos DB accounts in the cloud



Enable

1

One-click enablement

Detect

2

Protected Azure Cosmos DB accounts

SQL/CORE API

Microsoft Defender for Azure Cosmos DB

Data Breach Techniques:

- SQL injections
- Suspicious key extraction that indicate compromised identities
- Data inspection/exfiltration, change of access permissions
- Access from suspicious IP, TOR, unusual location/app

Attacker

Security alert

Admin

Respond

3

SecOps

Investigate in Microsoft Sentinel

Automatic response

Azure native security

Built-in with Azure with one-click enablement to protect SQL

Rich detection suite

Covering No-SQL DB threats powered by Defender for Cosmos DB and Microsoft Threat Intelligence

Respond at scale

Reduce frictions preventing and responding to top threats

Centralized and integrated

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

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

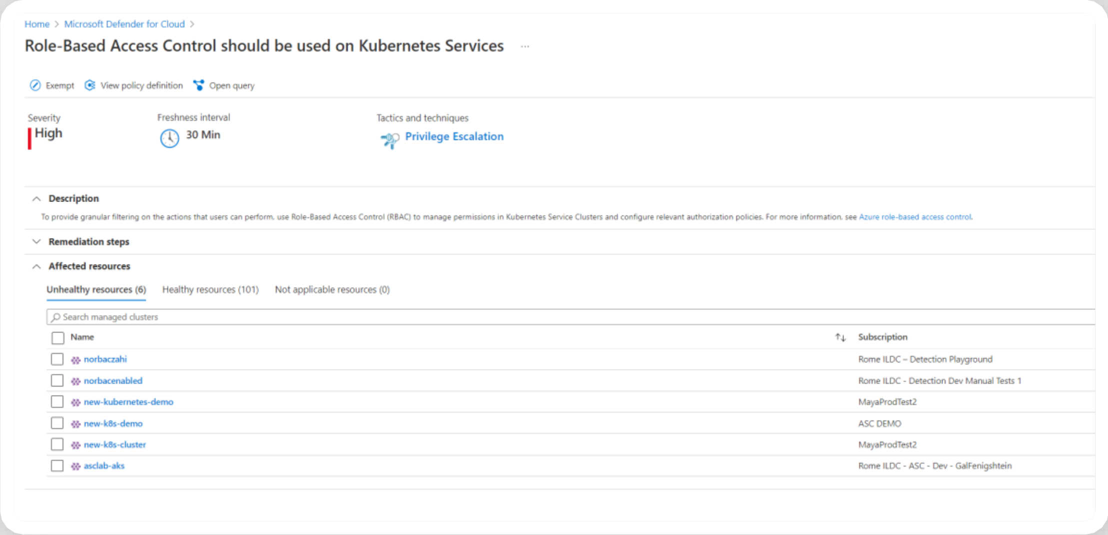
- → Understand the bottom line of your security posture
- → Prioritized view of containerized assets' security posture

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



Role-Based Access Control should be used on Kubernetes Services

Severity: High

Freshness interval: 30 Min

Tactics and techniques: Privilege Escalation

Description

To provide granular filtering on the actions that users can perform, use Role-Based Access Control (RBAC) to manage permissions in Kubernetes Service Clusters and configure relevant authorization policies. For more information, see Azure role-based access control.

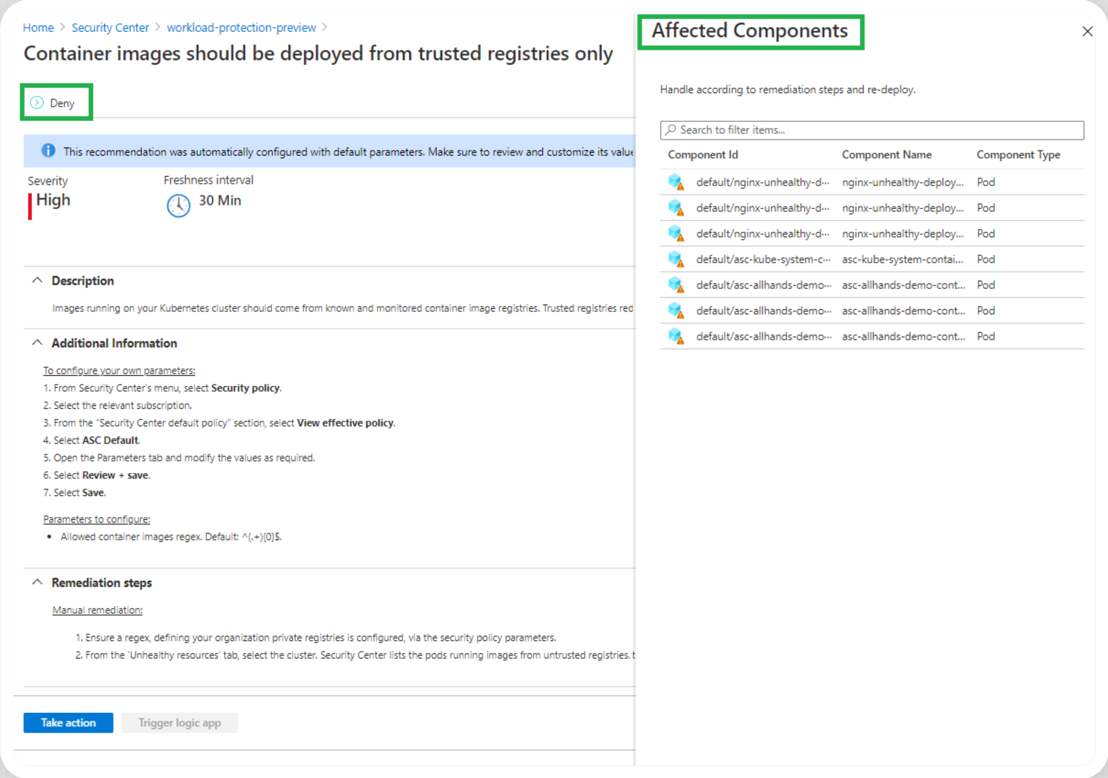
Remediation steps

Affected resources

Unhealthy resources (6) | Healthy resources (101) | Not applicable resources (0)

Search managed clusters

Name	Subscription
norbaczahi	Rome ILDC – Detection Playground
norbacenabled	Rome ILDC - Detection Dev Manual Tests 1
new-kubernetes-demo	MayaProdTest2
new-k8s-demo	ASC DEMO
new-k8s-cluster	MayaProdTest2
asclab-aks	Rome ILDC - ASC - Dev - GalFenigshtein



Container images should be deployed from trusted registries only

This recommendation was automatically configured with default parameters. Make sure to review and customize its value

Severity: High

Freshness interval: 30 Min

Description

Images running on your Kubernetes cluster should come from known and monitored container image registries. Trusted registries red

Additional Information

To configure your own parameters:

1. From Security Center's menu, select **Security policy**.
2. Select the relevant subscription.
3. From the "Security Center default policy" section, select **View effective policy**.
4. Select **ASC Default**.
5. Open the Parameters tab and modify the values as required.
6. Select **Review + save**.
7. Select **Save**.

Parameters to configure:

- Allowed container images regex. Default: ^(.+){0}$.

Remediation steps

Manual remediation:

1. Ensure a regex, defining your organization private registries is configured, via the security policy parameters.
2. From the 'Unhealthy resources' tab, select the cluster. Security Center lists the pods running images from untrusted registries. t

Affected Components

Handle according to remediation steps and re-deploy.

Search to filter items...

Component Id	Component Name	Component Type
default/nginx-unhealthy-d···	nginx-unhealthy-deploy...	Pod
default/nginx-unhealthy-d···	nginx-unhealthy-deploy...	Pod
default/nginx-unhealthy-d···	nginx-unhealthy-deploy...	Pod
default/asc-kube-system-c···	asc-kube-system-contai...	Pod
default/asc-allhands-demo···	asc-allhands-demo-cont...	Pod
default/asc-allhands-demo···	asc-allhands-demo-cont...	Pod
default/asc-allhands-demo···	asc-allhands-demo-cont...	Pod

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

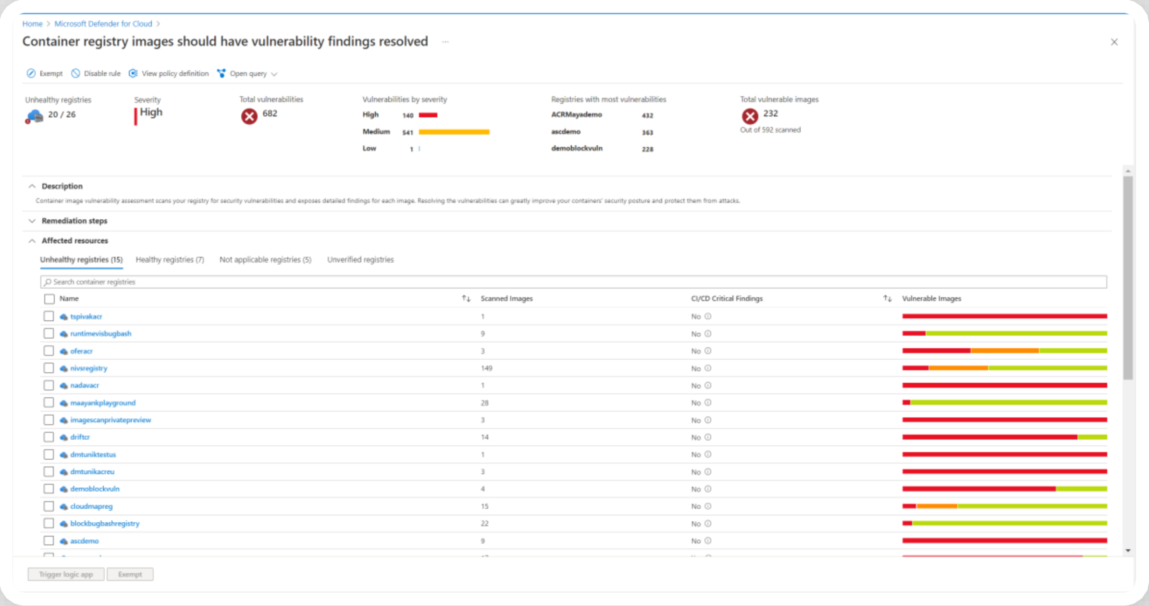
→ Continuous scanning of running images

→ Visibility of running images with vulnerabilities

Build

Coming soon

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



Container registry images should have vulnerability findings resolved

Unhealthy registries 20 / 26

Severity High

Total vulnerabilities 682

Vulnerabilities by severity	
High	140
Medium	541
Low	1

Registries with most vulnerabilities	
ACRMayademo	432
ascdemo	363
demoblockvuln	228

Total vulnerable images 232
Out of 592 scanned

Description

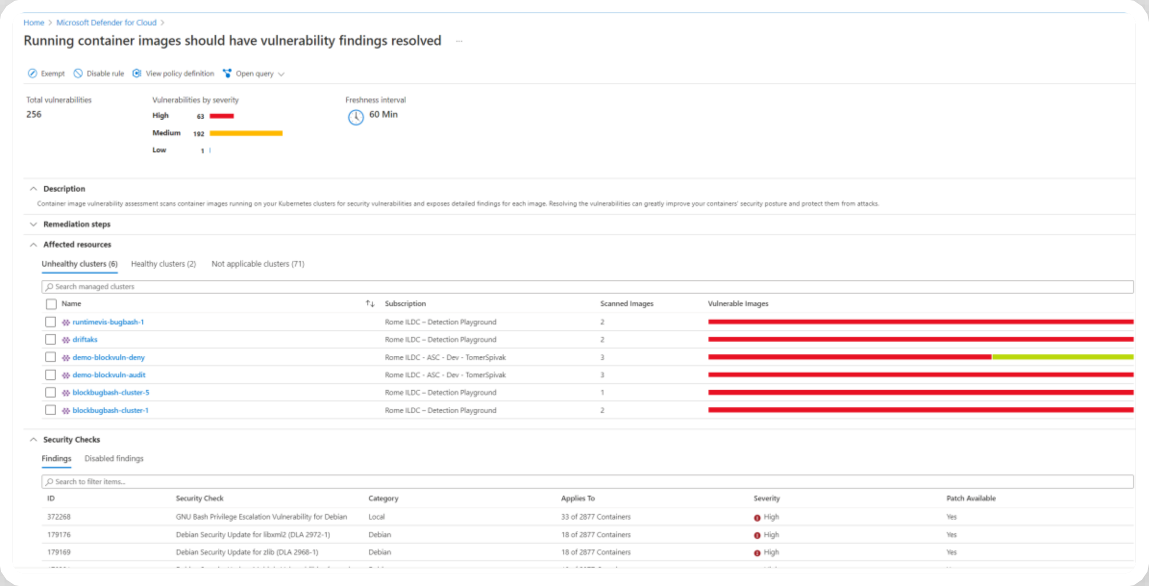
Container image vulnerability assessment scans your registry for security vulnerabilities and exposes detailed findings for each image. Resolving the vulnerabilities can greatly improve your containers' security posture and protect them from attacks.

Remediation steps

Affected resources

Unhealthy registries (15)
Healthy registries (7)
Not applicable registries (5)
Unverified registries
Search container registries

Name	Scanned Images	CI/CD Critical Findings	Vulnerable Images
tspivakacr	1	No	
runtimevisbugbash	9	No	
oferacr	3	No	
nivsregistry	149	No	
nadavacr	1	No	
maayankplayground	28	No	
imagescanprivatepreview	3	No	
driftcr	14	No	
dmtuniktestus	1	No	
dmtunikacreu	3	No	
demoblockvuln	4	No	
cloudmapreg	15	No	
blockbugbashregistry	22	No	
ascdemo	9	No	



Running container images should have vulnerability findings resolved

Total vulnerabilities 256

Vulnerabilities by severity	
High	63
Medium	192
Low	1

Freshness interval 60 Min

Description

Container image vulnerability assessment scans container images running on your Kubernetes clusters for security vulnerabilities and exposes detailed findings for each image. Resolving the vulnerabilities can greatly improve your containers' security posture and protect them from attacks.

Remediation steps

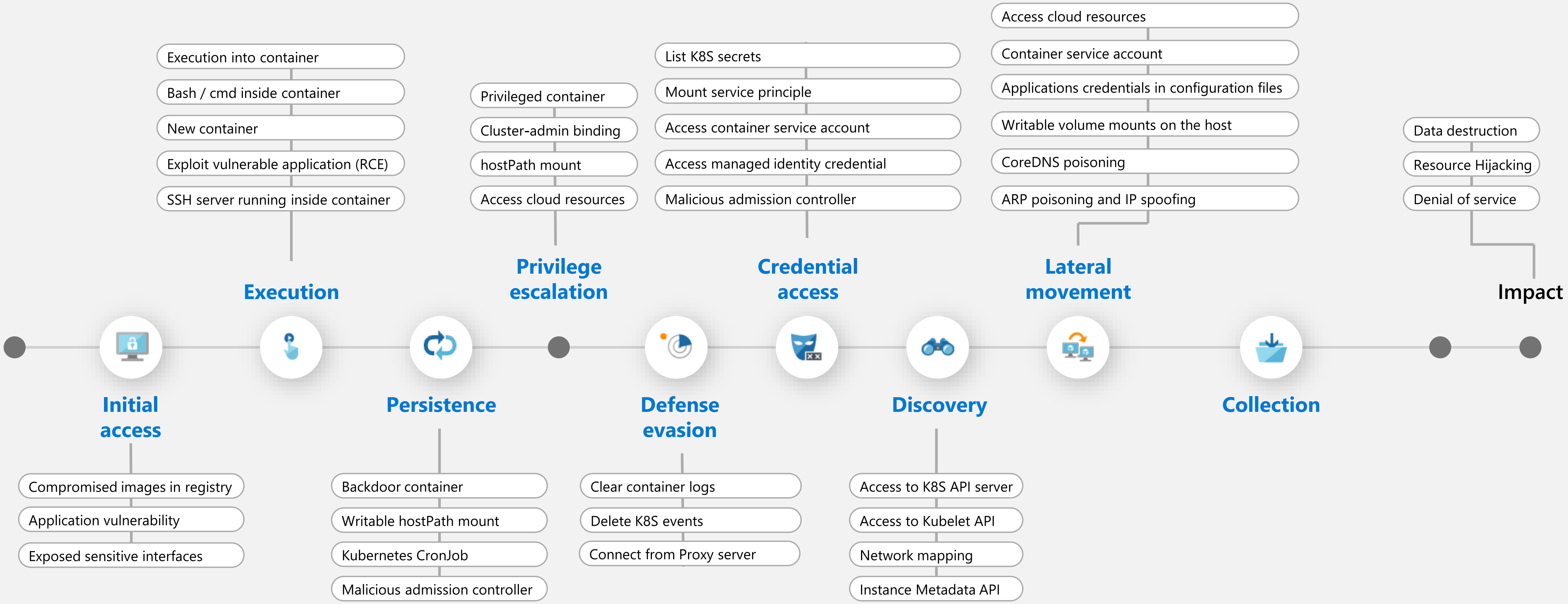
Affected resources

Name	Subscription	Scanned Images	Vulnerable Images
runtimevis-bugbash-1	Rome ILDC – Detection Playground	2	
driftaks	Rome ILDC – Detection Playground	2	
demo-blockvuln-deny	Rome ILDC - ASC - Dev - TomerSpivak	3	
demo-blockvuln-audit	Rome ILDC - ASC - Dev - TomerSpivak	3	
blockbugbash-cluster-5	Rome ILDC – Detection Playground	1	
blockbugbash-cluster-1	Rome ILDC – Detection Playground	2	

Security Checks

ID	Security Check	Category	Applies To	Severity	Patch Available
372268	GNU Bash Privilege Escalation Vulnerability for Debian	Local	33 of 2877 Containers	High	Yes
179176	Debian Security Update for libxml2 (DLA 2972-1)	Debian	18 of 2877 Containers	High	Yes
179169	Debian Security Update for zlib (DLA 2968-1)	Debian	18 of 2877 Containers	High	Yes

Threat detections aligned to the Kubernetes Attack Matrix



Initial access
- Compromised images in registry
- Application vulnerability
- Exposed sensitive interfaces

Execution
- Execution into container
- Bash / cmd inside container
- New container
- Exploit vulnerable application (RCE)
- SSH server running inside container

Persistence
- Backdoor container
- Writable hostPath mount
- Kubernetes CronJob
- Malicious admission controller

Privilege escalation
- Privileged container
- Cluster-admin binding
- hostPath mount
- Access cloud resources

Defense evasion
- Clear container logs
- Delete K8S events
- Connect from Proxy server

Credential access
- List K8S secrets
- Mount service principle
- Access container service account
- Access managed identity credential
- Malicious admission controller

Discovery
- Access to K8S API server
- Access to Kubelet API
- Network mapping
- Instance Metadata API

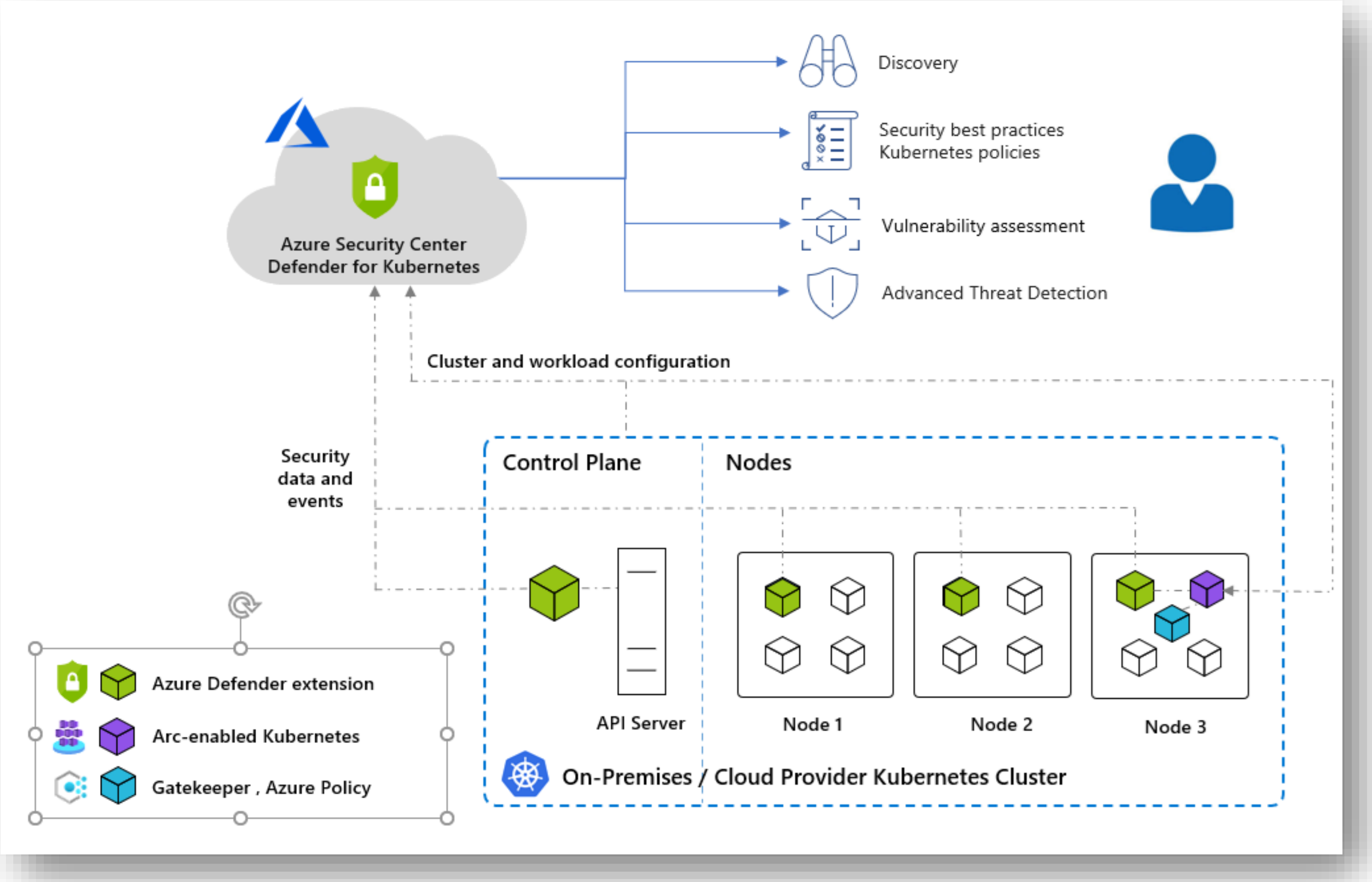
Lateral movement
- Access cloud resources
- Container service account
- Applications credentials in configuration files
- Writable volume mounts on the host
- CoreDNS poisoning
- ARP poisoning and IP spoofing

Collection

Impact
- Data destruction
- Resource Hijacking
- Denial of service

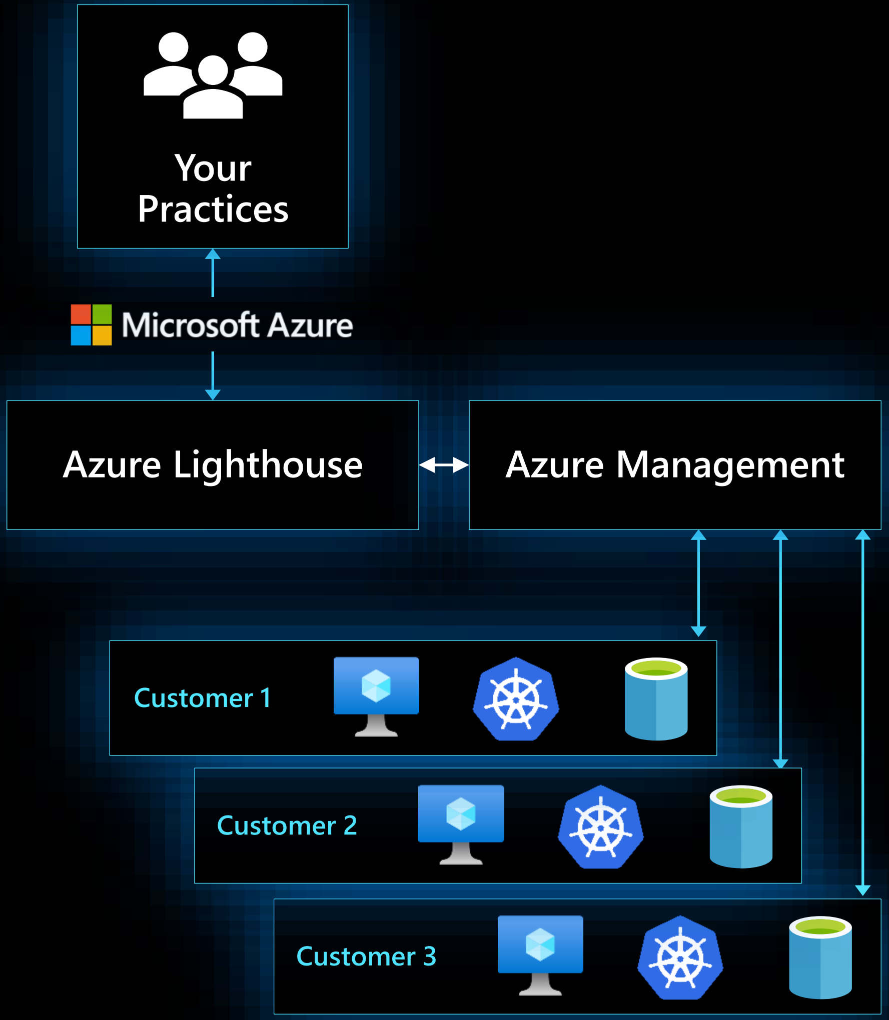
Solution components

- ✓ Workloads for:
  - ✓ The connection to **Azure Arc** (enabled K8s)
  - ✓ **Defender Extension** (DaemonSet)
  - ✓ **Azure Policy Extension** (w/ Gatekeeper)
- ✓ In EKS and GKE there is a different mechanism for K8s audit collection
- ✓ In AKS there is no Arc component, the Azure policy is connected through an add-in and the audit log collection is native.



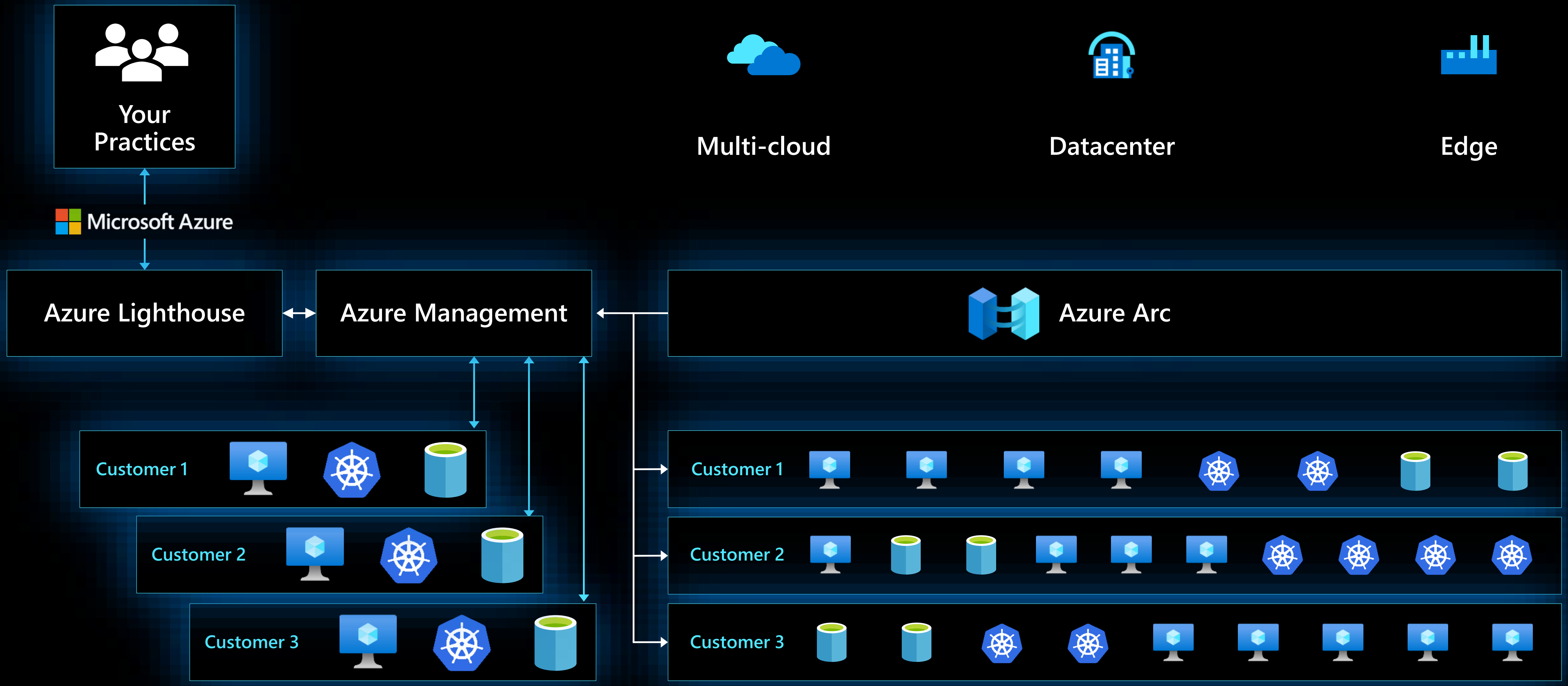
Azure Security Center Defender for Kubernetes
Discovery
Security best practices Kubernetes policies
Vulnerability assessment
Advanced Threat Detection
Cluster and workload configuration
Security data and events
Control Plane
Nodes
API Server
Node 1
Node 2
Node 3
On-Premises / Cloud Provider Kubernetes Cluster
Azure Defender extension
Arc-enabled Kubernetes
Gatekeeper , Azure Policy

Azure Lighthouse



Azure Lighthouse and Azure Arc

Azure Arc extends Azure management, services, and Azure Lighthouse anywhere



Windows Server | Linux | Kubernetes | SQL | Azure data services

Azure Arc enabled servers

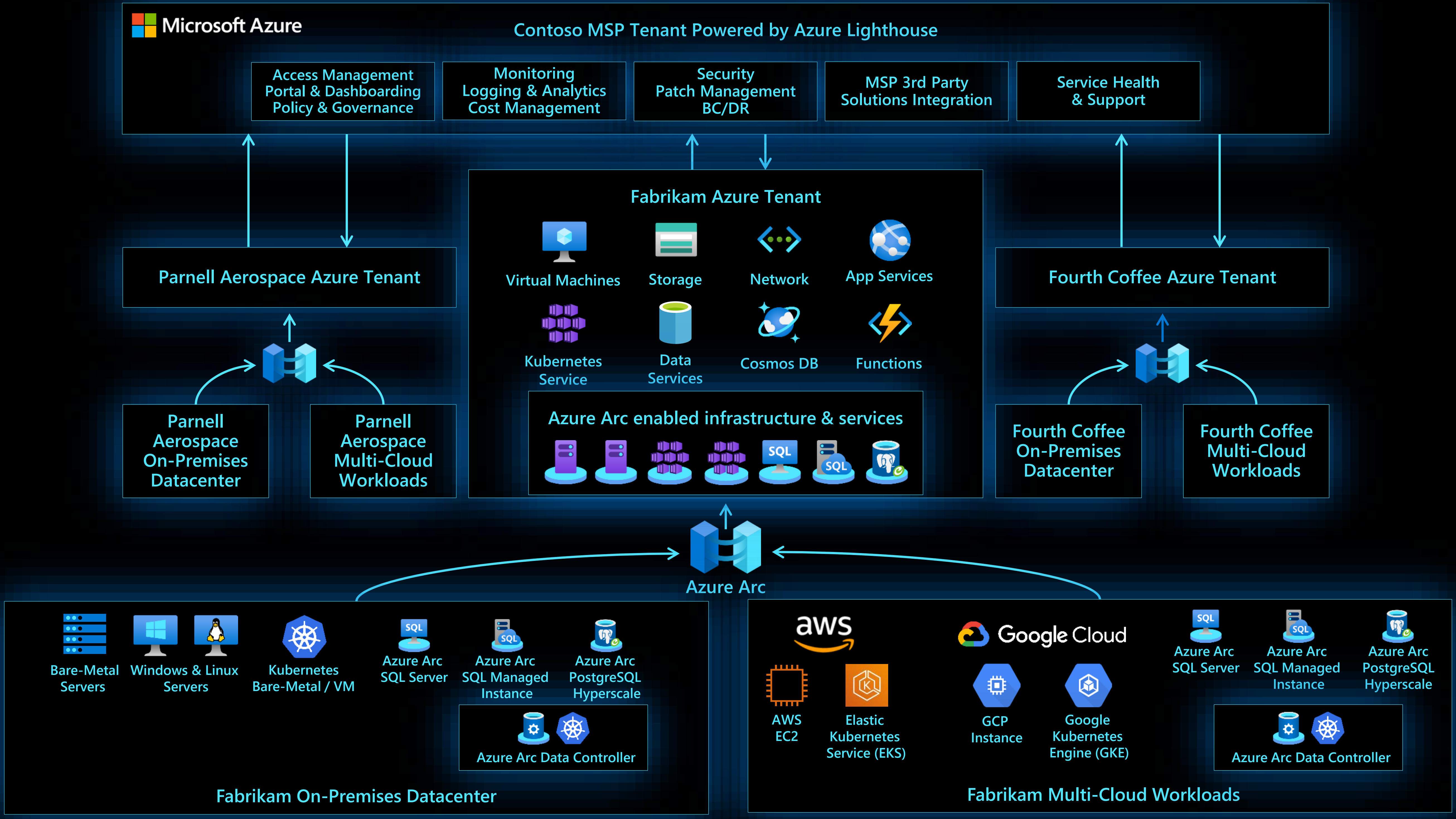
Azure Arc enabled servers are auto-enrolled with additional Azure services

Windows Server
suse
Red Hat
aws
AWS Linux 2

Additional services

- Azure Policy
- Defender for Cloud
- Microsoft Sentinel
- Azure Monitor
- Change and inventory tracking
- Update management

Just turn them on when you want to use them



Microsoft Azure

Contoso MSP Tenant Powered by Azure Lighthouse

Access Management
Portal & Dashboarding
Policy & Governance

Monitoring
Logging & Analytics
Cost Management

Security
Patch Management
BC/DR

MSP 3rd Party
Solutions Integration

Service Health
& Support

Parnell Aerospace Azure Tenant

Parnell Aerospace On-Premises Datacenter

Parnell Aerospace Multi-Cloud Workloads

Fabrikam Azure Tenant

Virtual Machines

Storage

Network

App Services

Kubernetes Service

Data Services

Cosmos DB

Functions

Azure Arc enabled infrastructure & services

Fourth Coffee Azure Tenant

Fourth Coffee On-Premises Datacenter

Fourth Coffee Multi-Cloud Workloads

Azure Arc

Bare-Metal Servers

Windows & Linux Servers

Kubernetes Bare-Metal / VM

Azure Arc SQL Server

Azure Arc SQL Managed Instance

Azure Arc PostgreSQL Hyperscale

Azure Arc Data Controller

Fabrikam On-Premises Datacenter

aws

AWS EC2

Elastic Kubernetes Service (EKS)

Google Cloud

GCP Instance

Google Kubernetes Engine (GKE)

Azure Arc SQL Server

Azure Arc SQL Managed Instance

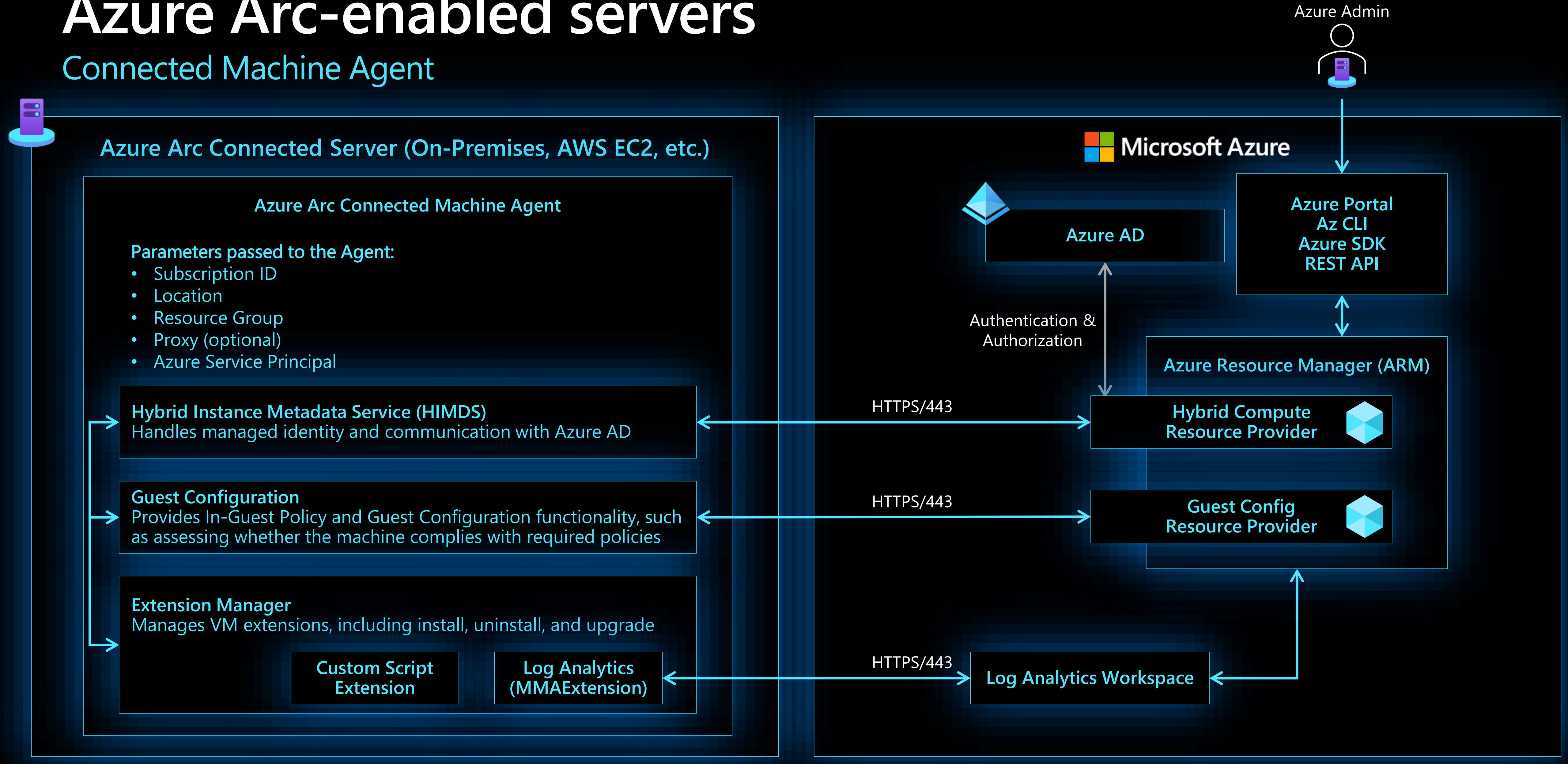
Azure Arc PostgreSQL Hyperscale

Azure Arc Data Controller

Fabrikam Multi-Cloud Workloads

Azure Arc-enabled servers

Connected Machine Agent



Azure Arc Connected Server (On-Premises, AWS EC2, etc.)

Azure Arc Connected Machine Agent

Parameters passed to the Agent:

- Subscription ID
- Location
- Resource Group
- Proxy (optional)
- Azure Service Principal

Hybrid Instance Metadata Service (HIMDS)
Handles managed identity and communication with Azure AD

Guest Configuration
Provides In-Guest Policy and Guest Configuration functionality, such as assessing whether the machine complies with required policies

Extension Manager
Manages VM extensions, including install, uninstall, and upgrade

Custom Script Extension

Log Analytics (MMAExtension)

Microsoft Azure

Azure AD

Azure Portal
Az CLI
Azure SDK
REST API

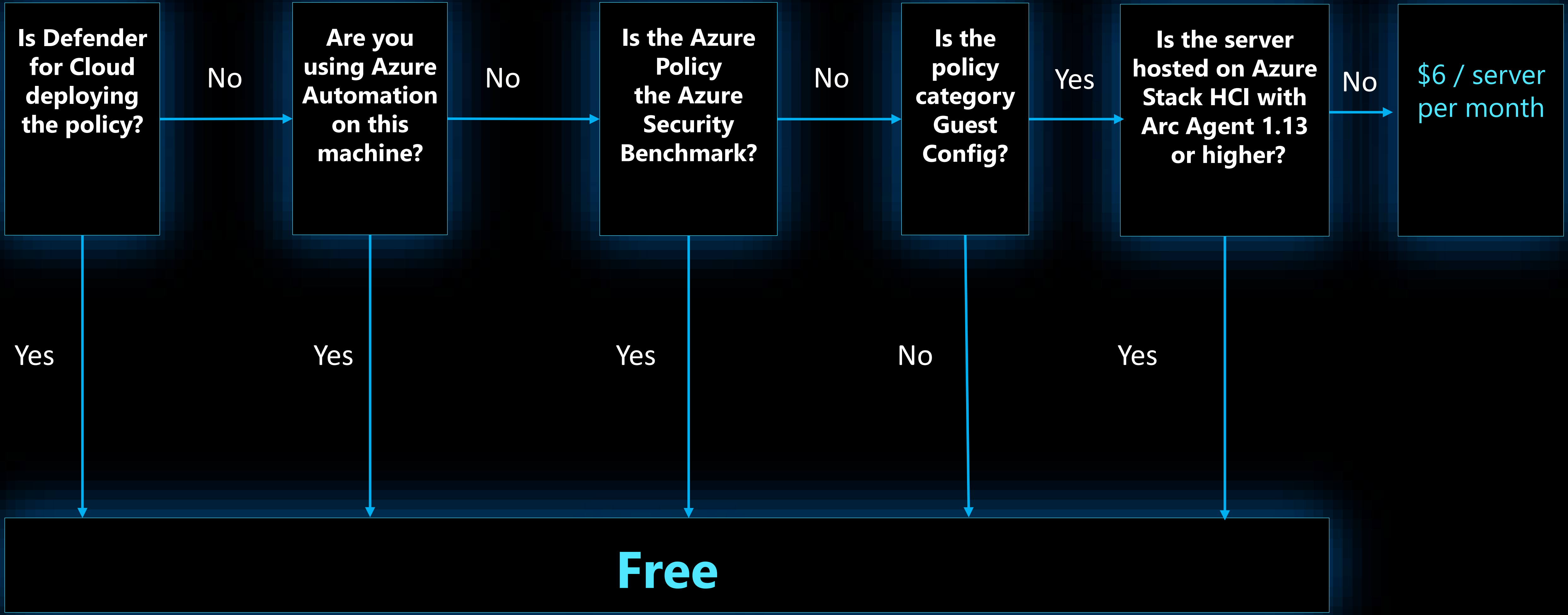
Azure Resource Manager (ARM)

Hybrid Compute Resource Provider

Guest Config Resource Provider

Log Analytics Workspace

It is free to use most Azure Policies on Arc-enabled servers



Is Defender for Cloud deploying the policy?

No

Are you using Azure Automation on this machine?

No

Is the Azure Policy the Azure Security Benchmark?

No

Is the policy category Guest Config?

Yes

Is the server hosted on Azure Stack HCI with Arc Agent 1.13 or higher?

No

$6 / server per month

Yes

Yes

Yes

No

Yes

Free

Demo

Microsoft Defender for Cloud Key takeaways

Native Cloud Solution

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

Deep Security Value

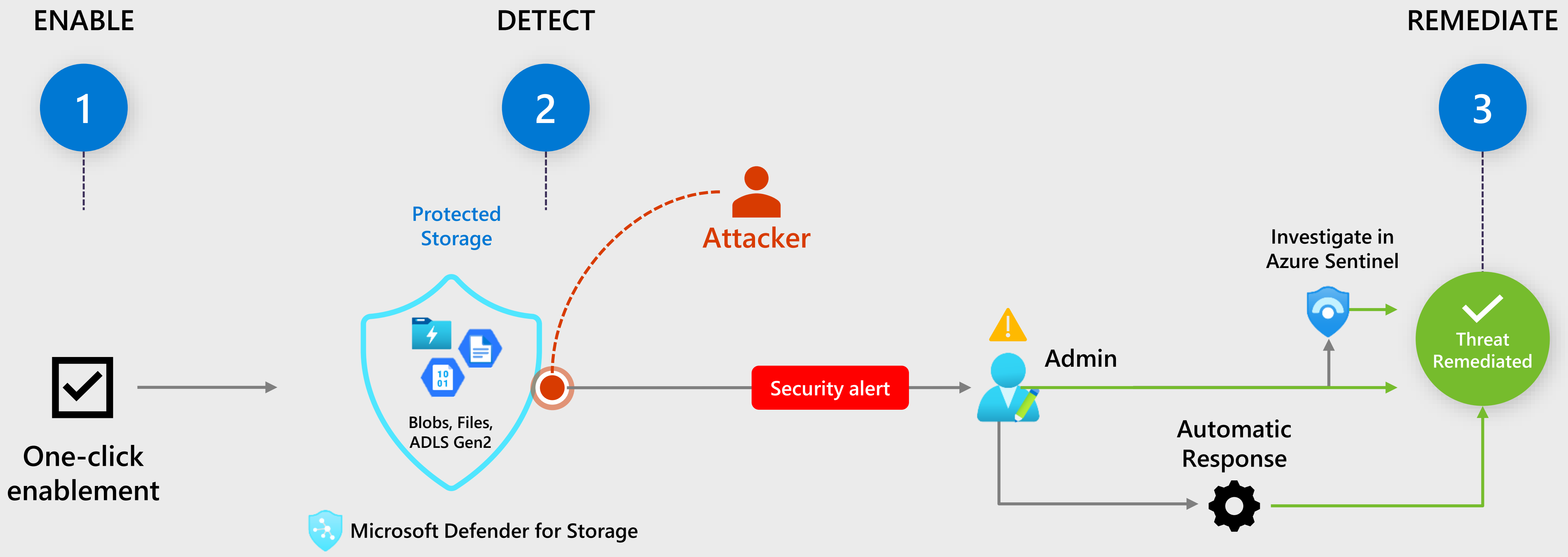
15 security alerts utilizing the advanced capabilities of Microsoft Threat Intelligence

Response at scale

Reduce frictions preventing and responding to top threats

Centralized & Integrated

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



Thank you