BY COMMUNITY • FOR COMMUNITY

#GLOBALAZURE

2024

#GlobalAzure
#GlobalAzureMilano

Proteggere workload in ambienti ibridi e multicloud con Microsoft Defender for Cloud

Michele Sensalari - OVERNET
Mario Serra - OVERNET

#GlobalAzure
#GlobalAzureMilano

Mario Serra

Security Consultant @ Overnet in ambiti di Cloud Adoption, Security Posture e Remediation, Azure, Microsoft 365, Device Management, Microsoft Purview etc..

Microsoft MVP per 5 anni, ora MVP Alumni

Speaker in molte conferenze come WPC, BeConnected, Cloud Conference, Aperiteams etc..

Trainer

Contatti:

Blog: www.marioserra.eu
Linkedin: https://www.linkedin.com/in/mario-serra-85829828/
Email: Email: mario.serra@overneteducation.it

#GlobalAzure
#GlobalAzureMilano

Michele Sensalari

Senior Consultant – Speaker – Trainer (26 anni)

Dal 2020 - Microsoft MVP – Enterprise Mobility / Security

Dipendente 50% su tecnologie Microsoft Dipartimento di Informatica – Università degli Studi di Milano

CTO e Senior Consultant Overnet Education

Responsabile e speaker di conferenze quali: WPC, WPC Days, BeConnectedDay (BCD) in ambito ITPRO e Security

MVP
Microsoft
Most Valuable Professional

Contatti:

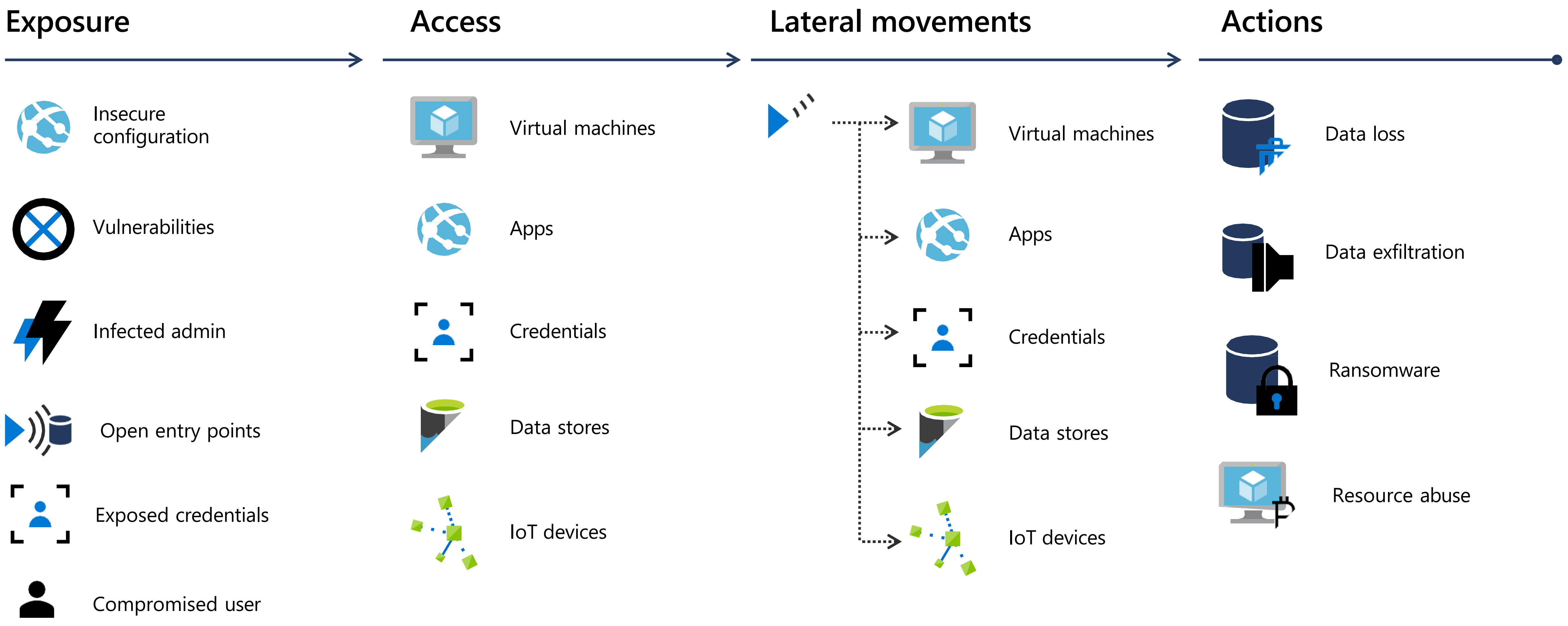
Twitter: @ilsensa7
Linkedin: https://www.linkedin.com/in/michele-sensalari-4988b7/
Email: michele@sensalari.com - michele.sensalari@overneteducation.it

Agenda

1. Cloud Security
2. Microsoft Defender for Cloud
   1. Cloud Security Posture Management
   2. Cloud Workload Protection
3. Integration with other providers (AWS, GCP)
4. Hybrid Configuration (on-prem!)
5. Cloud-native application protection platform

…all with some DEMOS!

The cloud kill chain model



Exposure

- Insecure configuration
- Vulnerabilities
- Infected admin
- Open entry points
- Exposed credentials
- Compromised user

Access

- Virtual machines
- Apps
- Credentials
- Data stores
- IoT devices

Lateral movements

- Virtual machines
- Apps
- Credentials
- Data stores
- IoT devices

Actions

- Data loss
- Data exfiltration
- Ransomware
- Resource abuse

Applying Security to Multi-Cloud

Protection against sophisticated attacks

$4.24M

It was the average cost of cyberattacks in 2021.[3]

Visibility for Security and Compliance

86%

of respondents believe that the security strategy adopted in their companies does not offer multi-cloud coverage [2]

IT Security Skills shortage wordwide

>40%

of respondents worldwide expected the biggest shortage regarding IT security skills to be for IT security administrators

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

AI allows for a paradigm shift

Continuously assess and improve posture with **hyperscale real-time visibility and context**

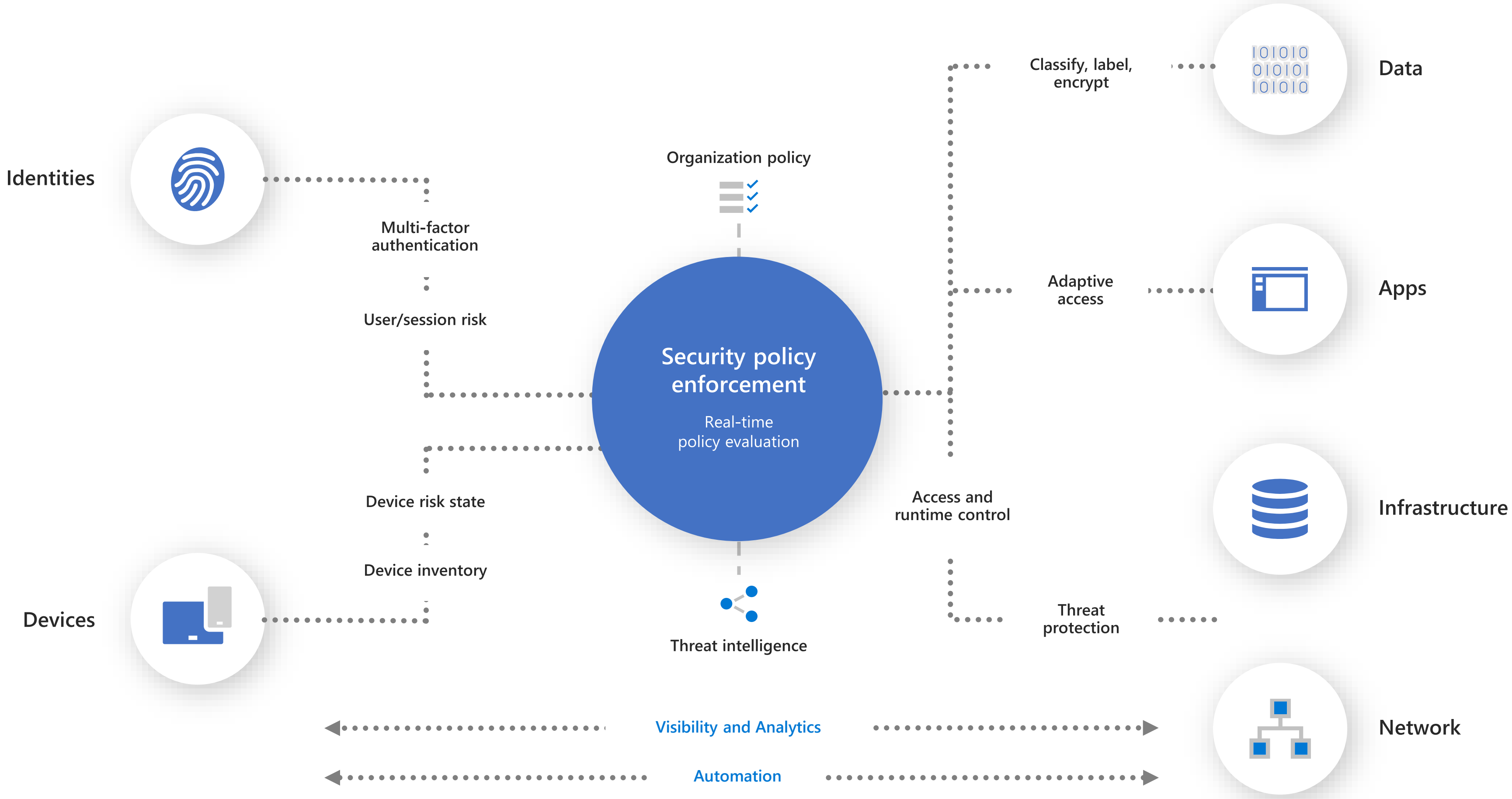
Investigate and respond to threats with unprecedented **speed and expertise**

Improve productivity and collaboration with **streamlined natural language workflows**

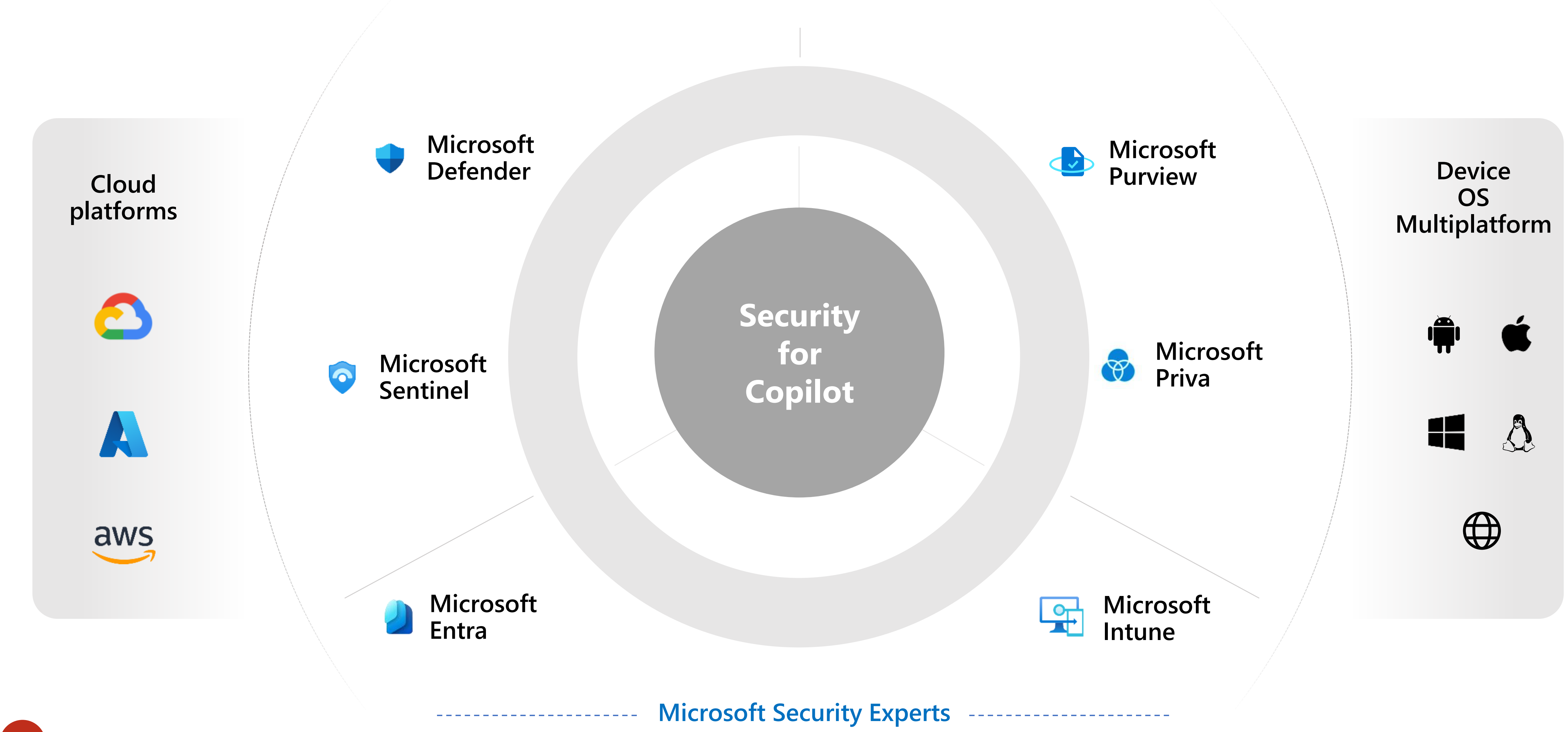
Microsoft Zero Trust architecture

Principles of Zero Trust

- ✓ **Verify explicitly** – Validate trust of users, devices, applications, and more using data/telemetry
- ✓ **Use least privileged access** – to limit the impact of any given compromise
- ✓ **Assume breach** – Assume that attackers will succeed (partially or fully) and design accordingly



Microsoft Security Portfolio



Cloud platforms

Microsoft Defender

Microsoft Sentinel

Microsoft Entra

Security for Copilot

Microsoft Purview

Microsoft Priva

Microsoft Intune

Device OS Multiplatform

Microsoft Security Experts

Microsoft Defender For Cloud & DevOps

Microsoft Defender for Cloud enables comprehensive visibility, posture management, and threat protection across multicloud environments including Azure, AWS, GCP, and on-premises resources.

Harden and manage your Security Posture

CSPM

Secure configuration of resources

Management of compliance requirements

Detect threats and protect your workloads

CWS

Full-stack threat protection

Vulnerability assessment & management

Respond & Automate

CWS

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

Key pillars

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

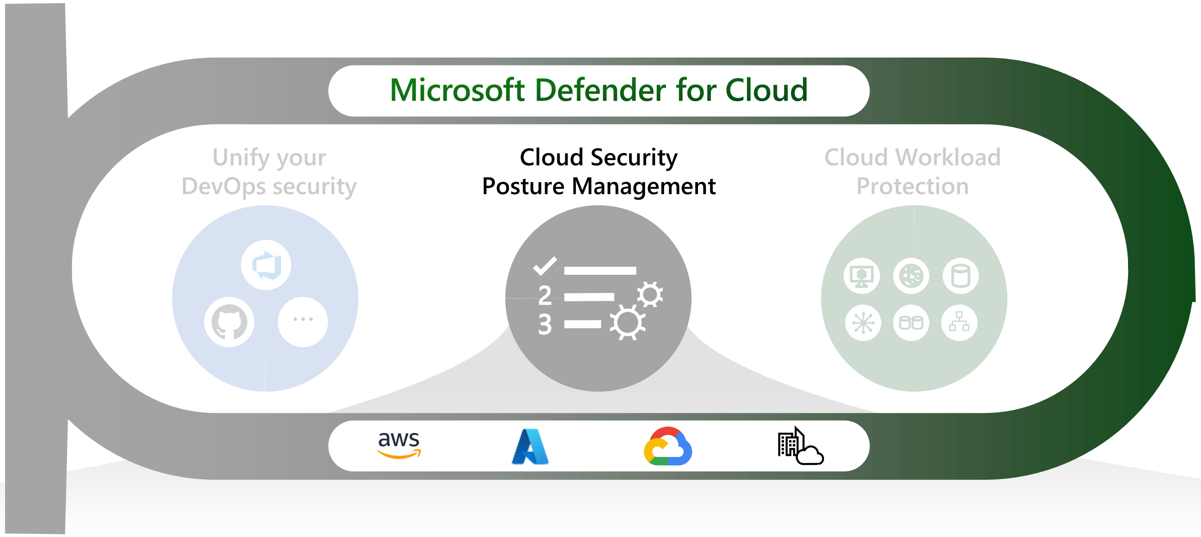
Secure Score

- 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

Cloud security posture management CSPM


Microsoft Defender for Cloud
Unify your DevOps security
Cloud Security Posture Management
Cloud Workload Protection
aws

Foundational CSPM

Free

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

Advanced remediation
Quick-fix remediation | Automated remediation using LogicApps | Enforcement policies

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

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

Defender CSPM

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

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

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

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

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

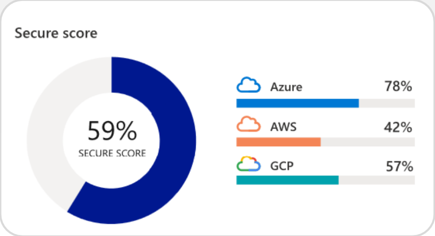
Data-aware security posture
Multicloud data estate discovery | Identify data flows and resources containing sensitive and shadow data | Uncover potential sensitive data exposure and data breaches

Free

Foundational CSPM

Secure Score and continuous assessments

Understand the bottom line of your security posture, implement recommendations, and monitor over time



Cross-cloud resource inventory

Discover and govern your cloud resource in centralized security tool

Data visualization and reporting

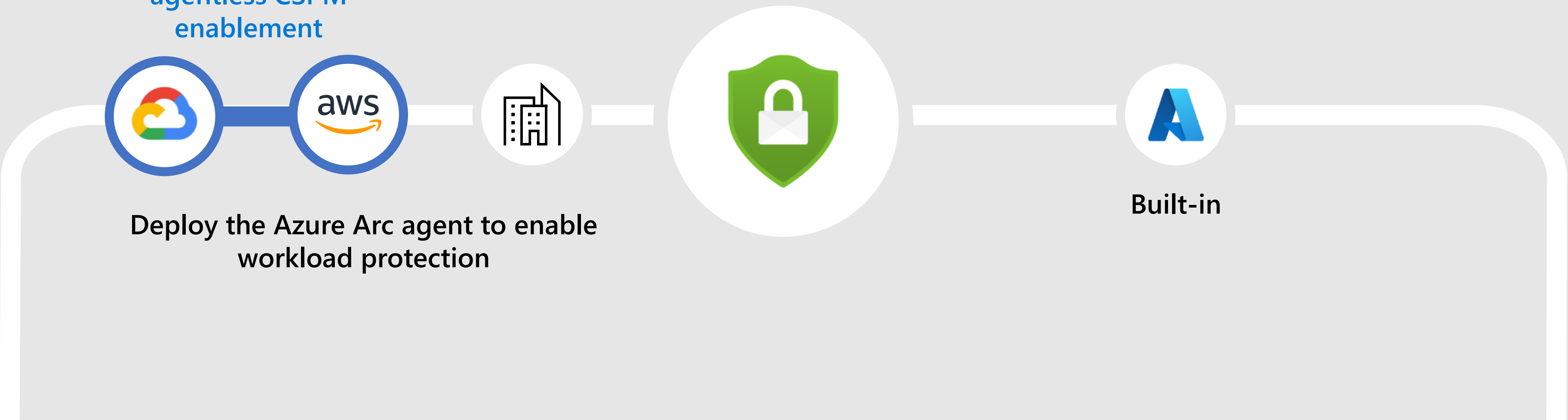
Create dynamic reports for both sec teams and C level with Azure Workbooks integrated experience, complimented by continuous data streaming

Workflow automation and data exporting

Automate incident response with built in Logic App template gallery, streamline security events and integrate with SIEM

Multicloud and hybrid protection

- Automatic onboarding for Azure subscriptions
- Use API connectors to onboard AWS and GCP accounts to posture management capabilities
- Use the Azure Arc agent to onboard workloads outside of Azure and protect them against threats



Use API connectors for agentless CSPM enablement

Deploy the Azure Arc agent to enable workload protection

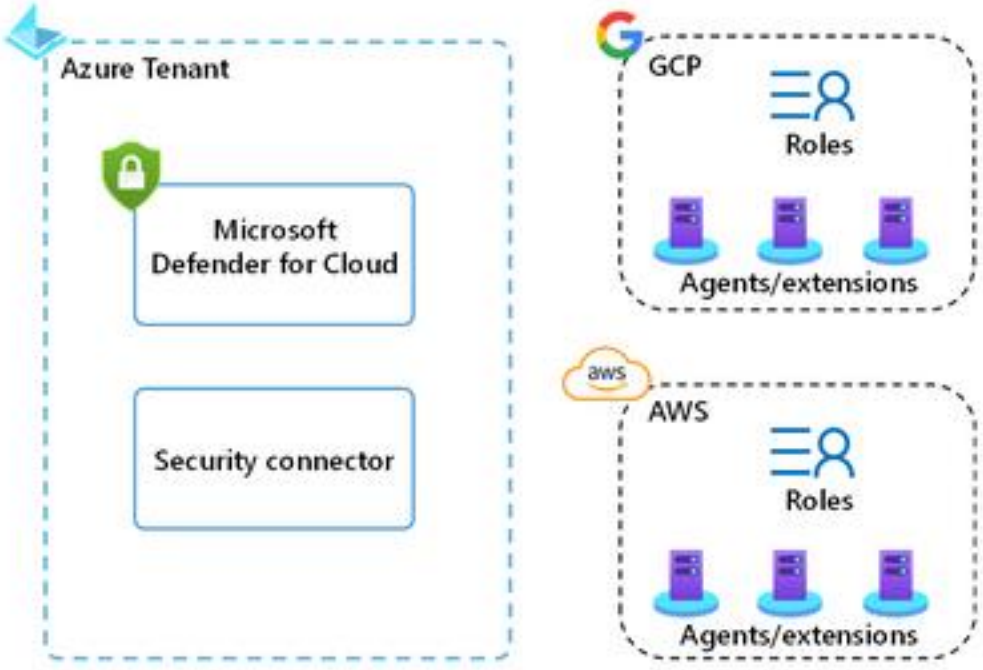
Built-in

Security Connectors

- ✓ To onboard AWS/GCP environment to Defender for Cloud, it is necessary to create a **security connector** in Defender for Cloud.

- ✓ Cloud Formation template in AWS or a cloud shell script in GCP creates the roles and resources that Defender for Cloud requires to provide security recommendations and alerts for your workloads.

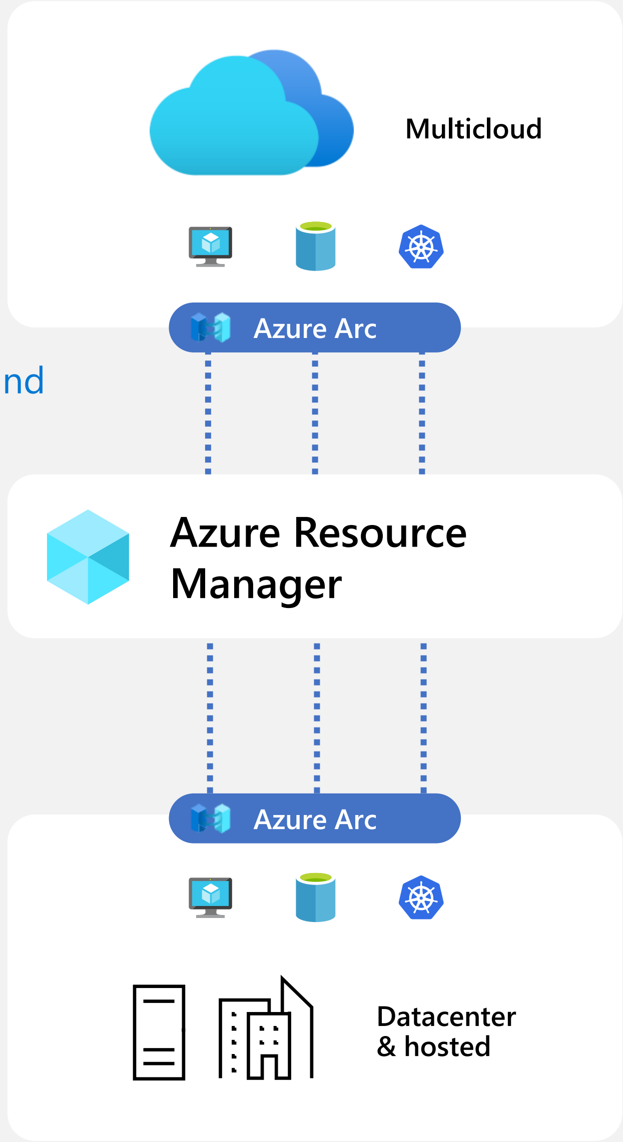
- ✓ The resources and roles created in AWS/GCP depend on the Defender for Cloud plans you select on the security connector.



For AWS you can start at https://learn.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws#prerequisites
For GCP you can start at https://learn.microsoft.com/en-us/azure/defender-for- cloud/quickstart-onboard-gcp#prerequisites

Deploy Microsoft Defender for Cloud threat protection to your workloads anywhere with Azure Arc

- ✓ Azure Arc unlocks hybrid and multicloud scenarios so you can manage security for all your resources in a consistent way
- ✓ Extension installation, e.g. Microsoft Monitor Agent / Azure Monitor 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

Microsoft Defender CSPM

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

Continuous monitoring and intelligent prioritization from attack path analysis

Prevent data breaches and sensitive data exposure

Defender CSPM

Agentless vulnerability scanning

Visibility on software and CVEs | Disc snapshots | Insecure secrets and keys

Integrated data and insights

Defender for DevOps | Defender External Attack Surface Management | Entra Permissions Management

Contextual cloud security and risk prioritization

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

Regulatory compliance and industry benchmarks

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

Governance management

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

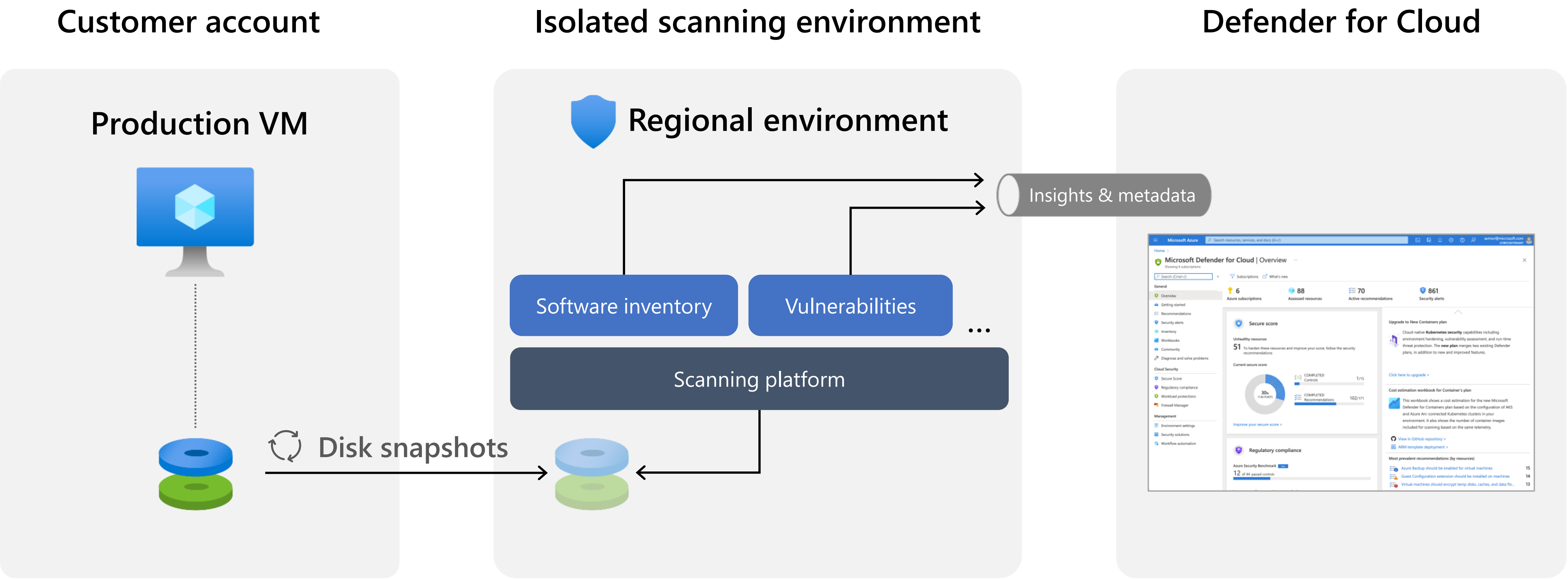
Data-aware security posture

Multicloud data estate discovery | Identify data flows and resources containing sensitive and shadow data | Uncover potential sensitive data exposure and data breaches

Centralized visibility with integrated CNAPP insights

Remediate vulnerabilities and misconfigurations with governance rules and remediation

Agentless scanning for Machines



Microsoft Azure
Search resources, services, and docs (G+/)
avmor@microsoft.com
CORECISOTENANT

Home >

Microsoft Defender for Cloud | Overview

Showing 6 subscriptions

Search (Cmd+/)

6 Azure subscriptions
88 Assessed resources
70 Active recommendations
861 Security alerts

Secure score

Unhealthy resources

51 To harden these resources and improve your score, follow the security recommendations

Current secure score

30% 17.46 POINTS

COMPLETED Controls 1/15

COMPLETED Recommendations 102/171

Improve your secure score >

Regulatory compliance

Azure Security Benchmark

12 of 44 passed controls

Upgrade to New Containers plan

Cloud-native **Kubernetes security** capabilities including environment hardening, vulnerability assessment, and run-time threat protection. The **new plan** merges two existing Defender plans, in addition to new and improved features.

Click here to upgrade >

Cost estimation workbook for Container's plan

This workbook shows a cost estimation for the new Microsoft Defender for Containers plan based on the configuration of AKS and Azure Arc-connected Kubernetes clusters in your environment. It also shows the number of container images included for scanning based on the same telemetry.

View in GitHub repository >

ARM template deployment >

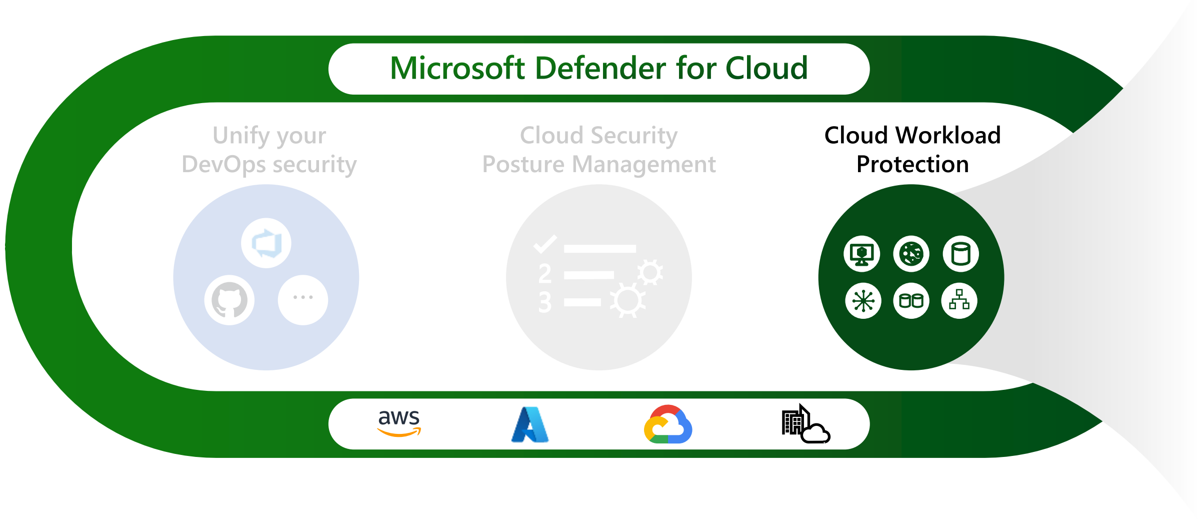
Most prevalent recommendations (by resources)

Azure Backup should be enabled for virtual machines	15
Guest Configuration extension should be installed on machines	14
Virtual machines should encrypt temp disks, caches, and data flo...	13

Foundational CSPM vs Defender CSPM

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

Cloud workload protection


Microsoft Defender for Cloud
Unify your DevOps security
Cloud Security Posture Management
Cloud Workload Protection
aws

Compute: Any server · Azure VMSS · Azure K8s · App Services · Unmanaged K8s

Service layer: Azure DNS · Key Vault · Network Layer V1 · Resource Management

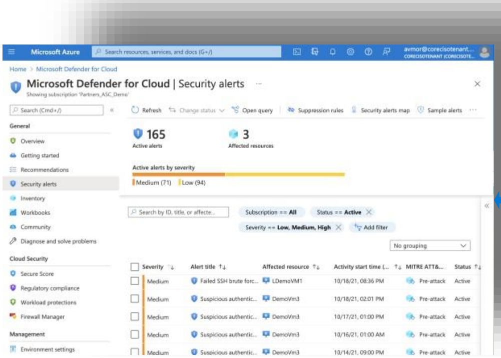
Databases and storage: Blob storage · File storage · Maria DB · Cosmos DB · Azure SQL · MySQL · Postgres SQL · SQL on VM

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

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

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

Microsoft Defender for Server



Microsoft Defender for Cloud | Security alerts

Showing subscription 'Partners_ASC_Demo'

165 Active alerts

3 Affected resources

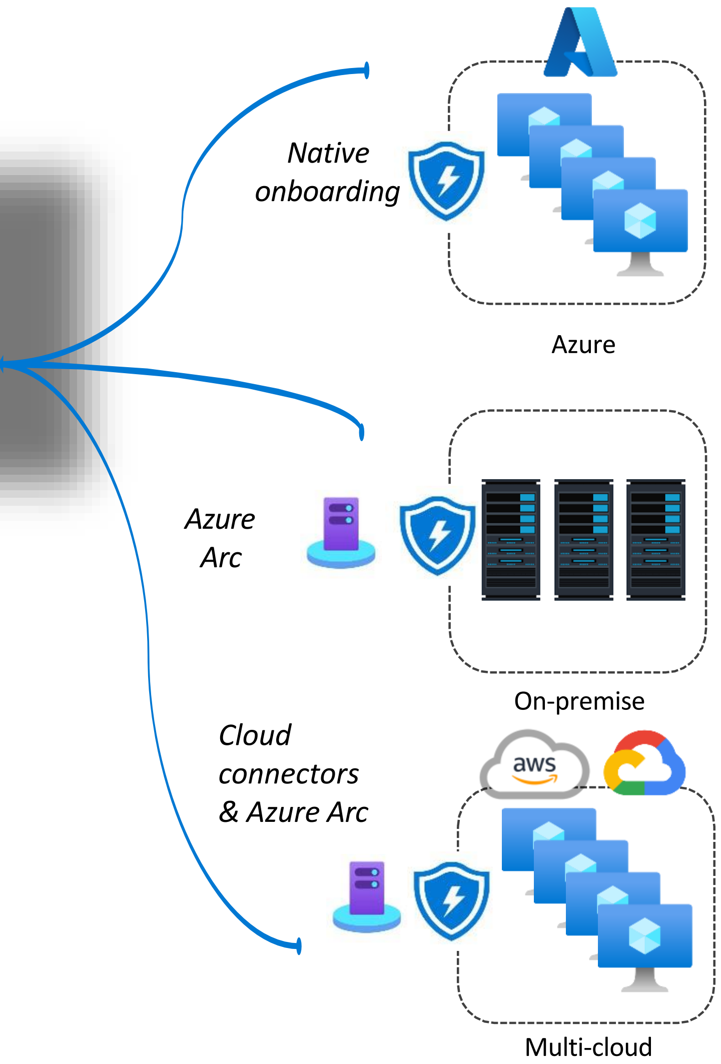
Active alerts by severity

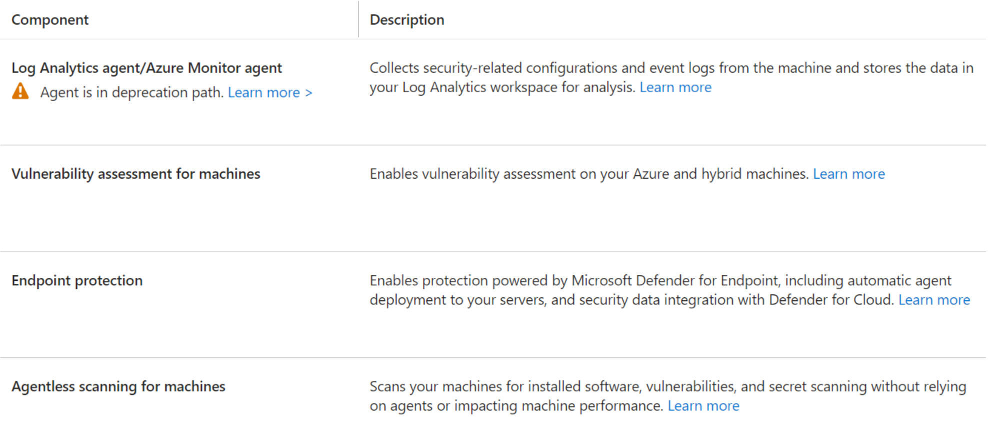
Medium (71) Low (94)

Subscription == **All** Status == **Active** Severity == **Low, Medium, High**

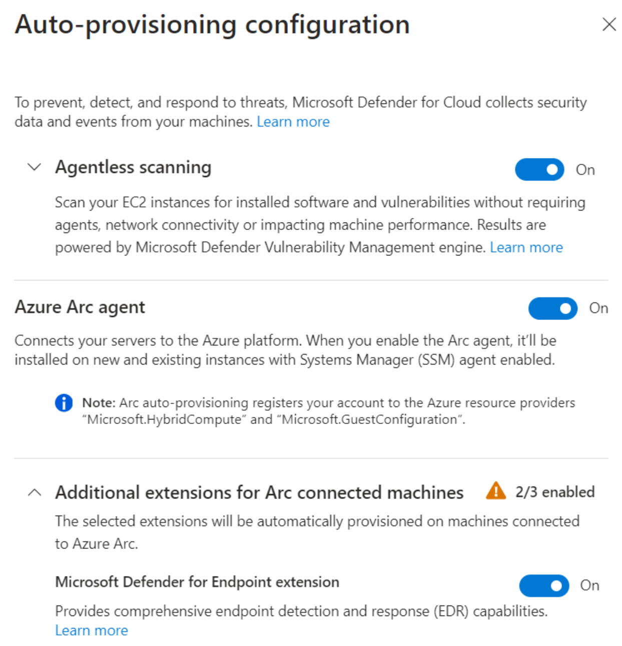
Severity	Alert title	Affected resource	Activity start time (...	MITRE ATT&...	Status
Medium	Failed SSH brute forc...	LDemoVM1	10/18/21, 08:36 PM	Pre-attack	Active
Medium	Suspicious authentic...	DemoVm3	10/18/21, 02:01 PM	Pre-attack	Active
Medium	Suspicious authentic...	DemoVm3	10/17/21, 01:00 PM	Pre-attack	Active
Medium	Suspicious authentic...	DemoVm3	10/16/21, 01:00 AM	Pre-attack	Active
Medium	Suspicious authentic...	DemoVm3	10/14/21, 09:00 PM	Pre-attack	Active

Defender for Cloud portal





Component	Description
Log Analytics agent/Azure Monitor agent ⚠ Agent is in deprecation path. Learn more >	Collects security-related configurations and event logs from the machine and stores the data in your Log Analytics workspace for analysis. Learn more
Vulnerability assessment for machines	Enables vulnerability assessment on your Azure and hybrid machines. Learn more
Endpoint protection	Enables protection powered by Microsoft Defender for Endpoint, including automatic agent deployment to your servers, and security data integration with Defender for Cloud. Learn more
Agentless scanning for machines	Scans your machines for installed software, vulnerabilities, and secret scanning without relying on agents or impacting machine performance. Learn more



Auto-provisioning configuration

To prevent, detect, and respond to threats, Microsoft Defender for Cloud collects security data and events from your machines. Learn more

Agentless scanning — On

Scan your EC2 instances for installed software and vulnerabilities without requiring agents, network connectivity or impacting machine performance. Results are powered by Microsoft Defender Vulnerability Management engine. Learn more

Azure Arc agent — On

Connects your servers to the Azure platform. When you enable the Arc agent, it'll be installed on new and existing instances with Systems Manager (SSM) agent enabled.

Note: Arc auto-provisioning registers your account to the Azure resource providers "Microsoft.HybridCompute" and "Microsoft.GuestConfiguration".

Additional extensions for Arc connected machines ⚠ 2/3 enabled

The selected extensions will be automatically provisioned on machines connected to Azure Arc.

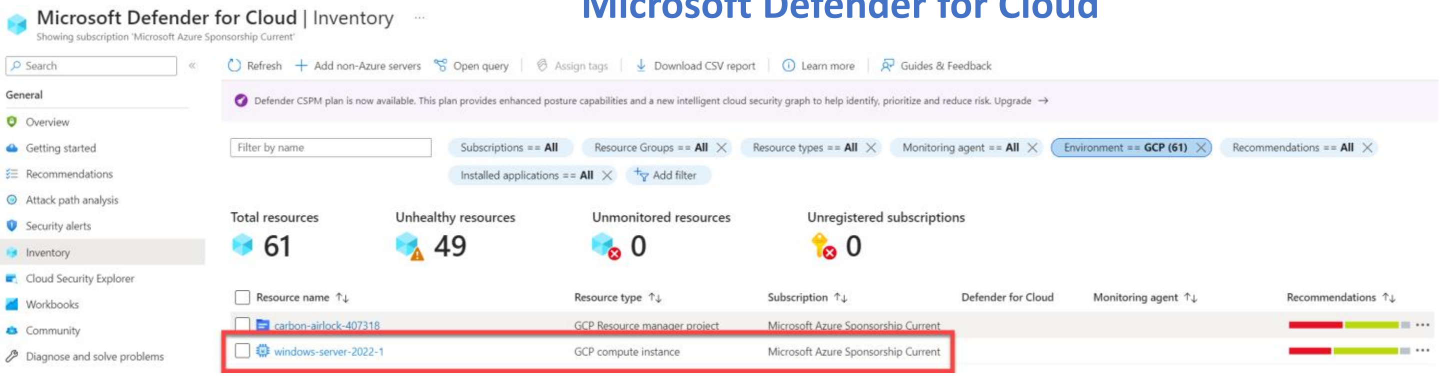
Microsoft Defender for Endpoint extension — On

Provides comprehensive endpoint detection and response (EDR) capabilities. Learn more

Microsoft Defender XDR: MDC, MDS, MDE

OVERNET.

Microsoft Defender for Cloud



Microsoft Defender for Cloud | Inventory ...
Showing subscription 'Microsoft Azure Sponsorship Current'

Search «

Refresh | Add non-Azure servers | Open query | Assign tags | Download CSV report | Learn more | Guides & Feedback

General
- Overview
- Getting started
- Recommendations
- Attack path analysis
- Security alerts
- Inventory
- Cloud Security Explorer
- Workbooks
- Community
- Diagnose and solve problems

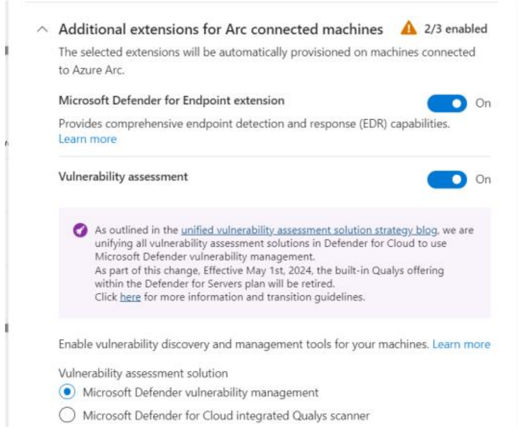
Defender CSPM plan is now available. This plan provides enhanced posture capabilities and a new intelligent cloud security graph to help identify, prioritize and reduce risk. Upgrade →

Filter by name | Subscriptions == **All** | Resource Groups == **All** ✕ | Resource types == **All** ✕ | Monitoring agent == **All** ✕ | Environment == **GCP (61)** ✕ | Recommendations == **All** ✕ | Installed applications == **All** ✕ | Add filter

Total resources: 61 | Unhealthy resources: 49 | Unmonitored resources: 0 | Unregistered subscriptions: 0

□	Resource name ↑↓	Resource type ↑↓	Subscription ↑↓	Defender for Cloud	Monitoring agent ↑↓	Recommendations ↑↓
□	carbon-airlock-407318	GCP Resource manager project	Microsoft Azure Sponsorship Current			...
□	windows-server-2022-1	GCP compute instance	Microsoft Azure Sponsorship Current			...

Microsoft Defender for Server



Additional extensions for Arc connected machines ⚠ 2/3 enabled

The selected extensions will be automatically provisioned on machines connected to Azure Arc.

Microsoft Defender for Endpoint extension: On

Provides comprehensive endpoint detection and response (EDR) capabilities. Learn more

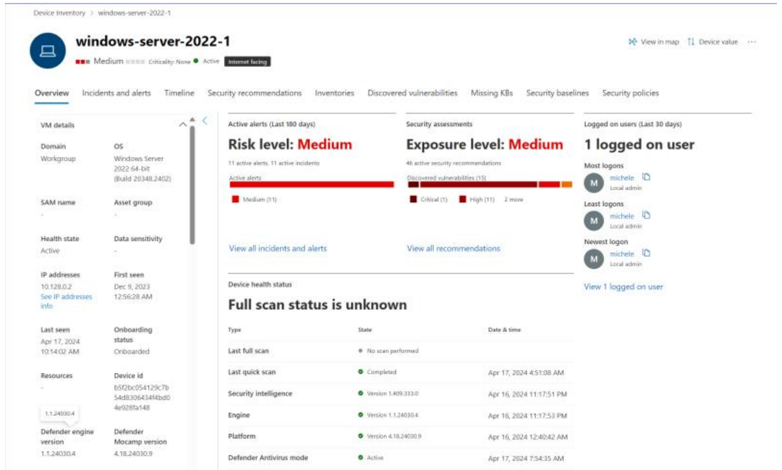
Vulnerability assessment: On

As outlined in the unified vulnerability assessment solution strategy blog, we are unifying all vulnerability assessment solutions in Defender for Cloud to use Microsoft Defender vulnerability management.
As part of this change, Effective May 1st, 2024, the built-in Qualys offering within the Defender for Servers plan will be retired.
Click here for more information and transition guidelines.

Enable vulnerability discovery and management tools for your machines. Learn more

Vulnerability assessment solution
- ● Microsoft Defender vulnerability management
- ○ Microsoft Defender for Cloud integrated Qualys scanner

Microsoft Defender for Endpoint



Device Inventory > windows-server-2022-1

windows-server-2022-1
Medium | Criticality: None | Active | Internet facing

View in map | Device value ...

Overview | Incidents and alerts | Timeline | Security recommendations | Inventories | Discovered vulnerabilities | Missing KBs | Security baselines | Security policies

VM details

Domain Workgroup	OS Windows Server 2022 64-bit (Build 20348.2402)
SAM name -	Asset group -
Health state Active	Data sensitivity -
IP addresses 10.128.0.2 See IP addresses info	First seen Dec 9, 2023 12:56:28 AM
Last seen Apr 17, 2024 10:14:02 AM	Onboarding status Onboarded
Resources -	Device id b5f2bc054129c7b54d830643f4bd04e928fa148
Defender engine version 1.1.24030.4	Defender Mocamp version 4.18.24030.9

Active alerts (Last 180 days)
Risk level: Medium
11 active alerts, 11 active incidents
Active alerts: Medium (11)
View all incidents and alerts

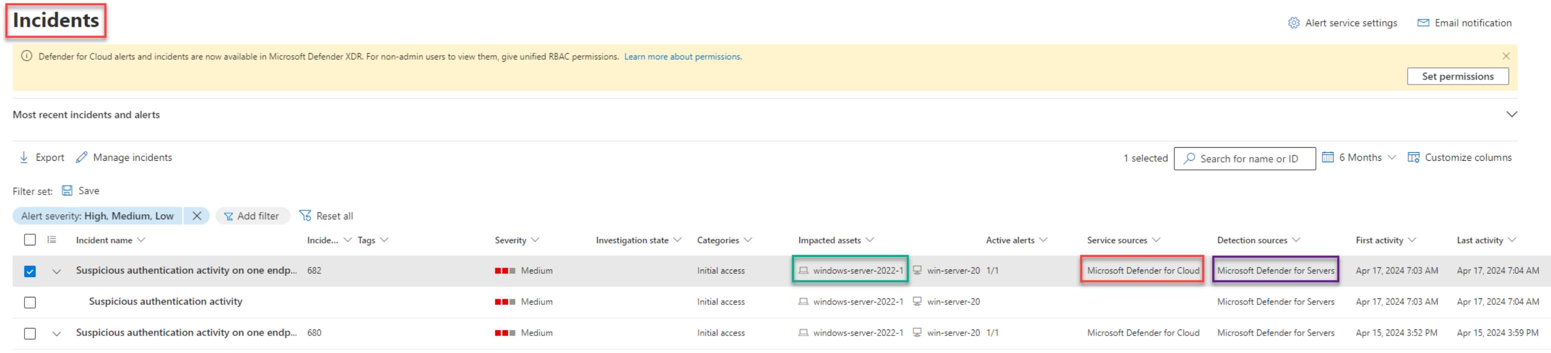
Security assessments
Exposure level: Medium
46 active security recommendations
Discovered vulnerabilities (15): Critical (1) | High (11) | 2 more
View all recommendations

Logged on users (Last 30 days)
1 logged on user
Most logons: michele, Local admin
Least logons: michele, Local admin
Newest logon: michele, Local admin
View 1 logged on user

Device health status
Full scan status is unknown

Type	State	Date & time
Last full scan	No scan performed	
Last quick scan	Completed	Apr 17, 2024 4:51:08 AM
Security intelligence	Version 1.409.333.0	Apr 16, 2024 11:17:51 PM
Engine	Version 1.1.24030.4	Apr 16, 2024 11:17:53 PM
Platform	Version 4.18.24030.9	Apr 16, 2024 12:40:42 AM
Defender Antivirus mode	Active	Apr 17, 2024 7:54:35 AM

Microsoft Defender XDR



Incidents

Alert service settings | Email notification

Defender for Cloud alerts and incidents are now available in Microsoft Defender XDR. For non-admin users to view them, give unified RBAC permissions. Learn more about permissions.

Set permissions

Most recent incidents and alerts

Export | Manage incidents

1 selected | Search for name or ID | 6 Months | Customize columns

Filter set: Save

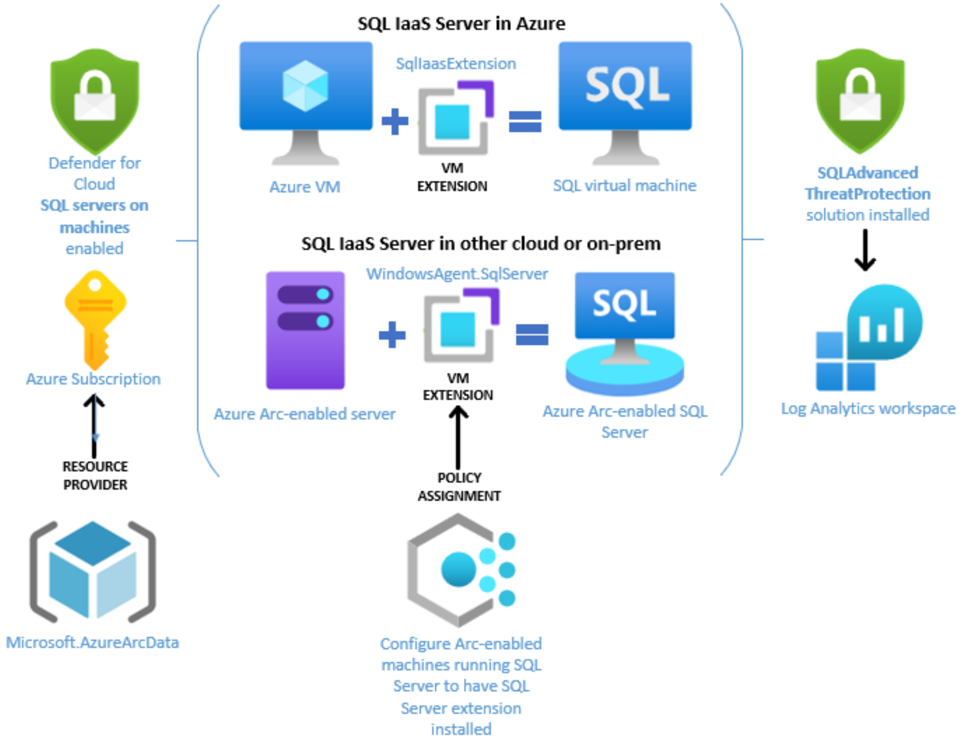
Alert severity: High, Medium, Low ✕ | Add filter | Reset all

□	Incident name	Incide...	Tags	Severity	Investigation state	Categories	Impacted assets	Active alerts	Service sources	Detection sources	First activity	Last activity
☑	Suspicious authentication activity on one endp...	682		Medium		Initial access	windows-server-2022-1 win-server-20	1/1	Microsoft Defender for Cloud	Microsoft Defender for Servers	Apr 17, 2024 7:03 AM	Apr 17, 2024 7:04 AM
□	Suspicious authentication activity			Medium		Initial access	windows-server-2022-1 win-server-20			Microsoft Defender for Servers	Apr 17, 2024 7:03 AM	Apr 17, 2024 7:04 AM
□	Suspicious authentication activity on one endp...	680		Medium		Initial access	windows-server-2022-1 win-server-20	1/1	Microsoft Defender for Cloud	Microsoft Defender for Servers	Apr 15, 2024 3:52 PM	Apr 15, 2024 3:59 PM

Microsoft Defender for SQL on VM

Defender for SQL protects your IaaS SQL Servers by identifying and mitigating potential database vulnerabilities and detecting anomalous activities that could indicate threats to your databases.

Defender for Cloud populates with alerts when it detects suspicious database activities, potentially harmful attempts to access or exploit SQL machines, SQL injection attacks, anomalous database access, and query patterns.

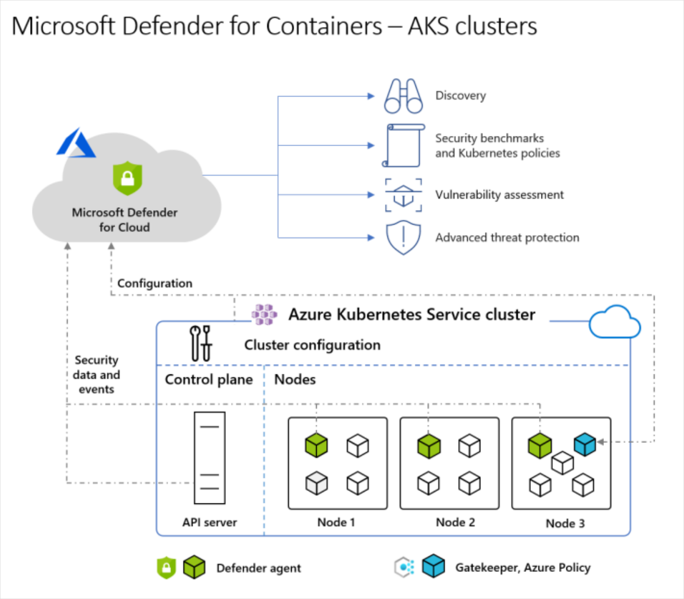


Microsoft Defender for Containers

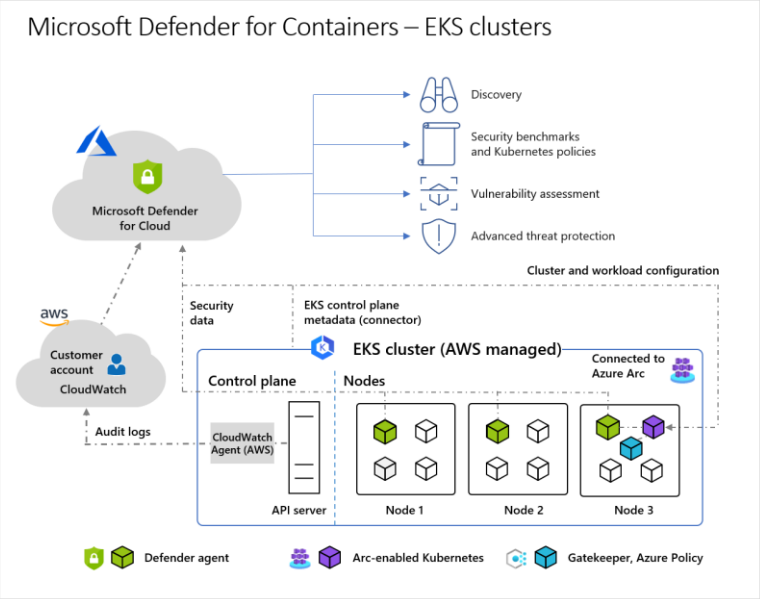
OVERNET.

Microsoft Defender for Containers is a cloud-native solution to improve, monitor, and maintain the security of your containerized assets (Kubernetes clusters, Kubernetes nodes, Kubernetes workloads, container registries, container images and more), and their applications, across multicloud and on-premises environments. Defender for Containers assists you with four core domains of container security:

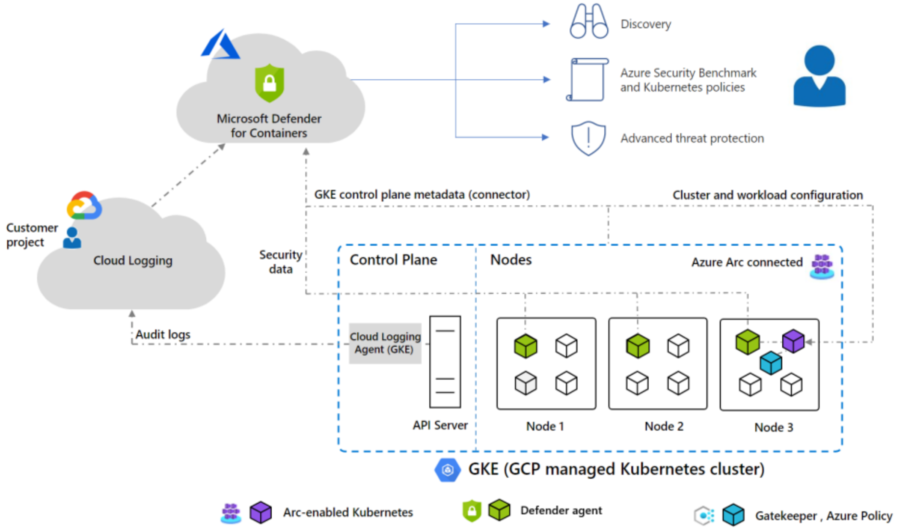
- Security posture management
- Vulnerability assessment
- Run-time threat protection
- Deployment & monitoring



Microsoft Defender for Containers – AKS clusters



Microsoft Defender for Containers – EKS clusters



Discovery
Azure Security Benchmark and Kubernetes policies
Advanced threat protection
Microsoft Defender for Containers
Customer project
Cloud Logging
Audit logs
Security data
GKE control plane metadata (connector)
Cluster and workload configuration
Control Plane
Nodes
Azure Arc connected
Cloud Logging Agent (GKE)
API Server
Node 1
Node 2
Node 3
GKE (GCP managed Kubernetes cluster)
Arc-enabled Kubernetes
Defender agent
Gatekeeper , Azure Policy

Azure Kubernetes Service (AKS)
Microsoft's managed service for developing, deploying, and managing containerized applications.

Amazon Elastic Kubernetes Service (EKS) in a connected Amazon Web Services (AWS) account Amazon's managed service for running Kubernetes on AWS without needing to install, operate, and maintain your own Kubernetes control plane or nodes.

Google Kubernetes Engine (GKE) in a connected Google Cloud Platform (GCP) project
Google's managed environment for deploying, managing, and scaling applications using GCP infrastructure.

To protect your Kubernetes containers, Defender for Containers receives and analyzes:

- Audit logs and security events from the API server
- Cluster configuration information from the control plane
- Workload configuration from Azure Policy
- Security signals and events from the node level

Respond and automate

- Leverage “Quick Fixes” for the fastest way to implement recommendations
- Automate threat alert responses with Azure Logic Apps and use the apps of your choice to create intelligent workflows
- Connect to Microsoft Sentinel and easily move between the portals when investigating and managing incidents

Azure Log Analytics

Azure Logic Apps

Outlook

Microsoft Teams

slack

servicenow

Microsoft Sentinel

Cloud-native application protection platform

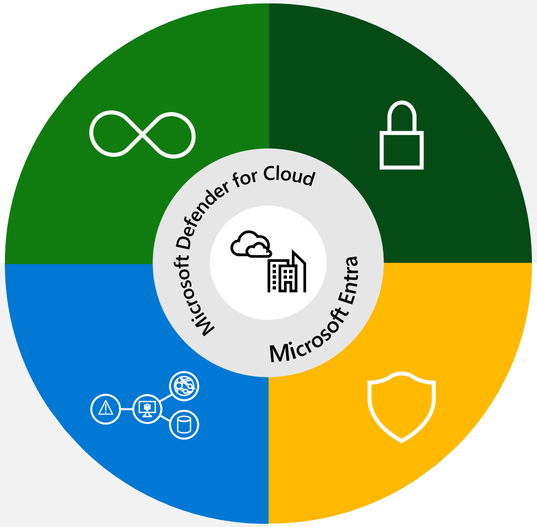
OVERNET.

DevSecOps

Unify your DevOps security management across multi-pipelines

Cloud infrastructure entitlement management

Enforce principle of least privilege across multicloud with CIEM



Cloud security posture management

Full visibility and contextual insights to identify and remediate your most critical risk

Cloud workload protection

Help detect and respond to modern threats across your cloud workloads in runtime

Integrated to protect across your cloud infrastructure

Microsoft Purview (Data Security)	Microsoft Defender External Attack Surface Management (EASM)	Azure Network Security	Microsoft Sentinel (SIEM)

Unify your DevOps security

DevOps security within Defender for Cloud uses a central console to empower security teams with the ability to protect applications and resources from code to cloud across multi-pipeline environments, including Azure DevOps, GitHub, and GitLab.

DevOps posture visibility

Code | Dependencies | Secrets | Container images | Infrastructure-as-Code security insights

Infrastructure-as-Code security

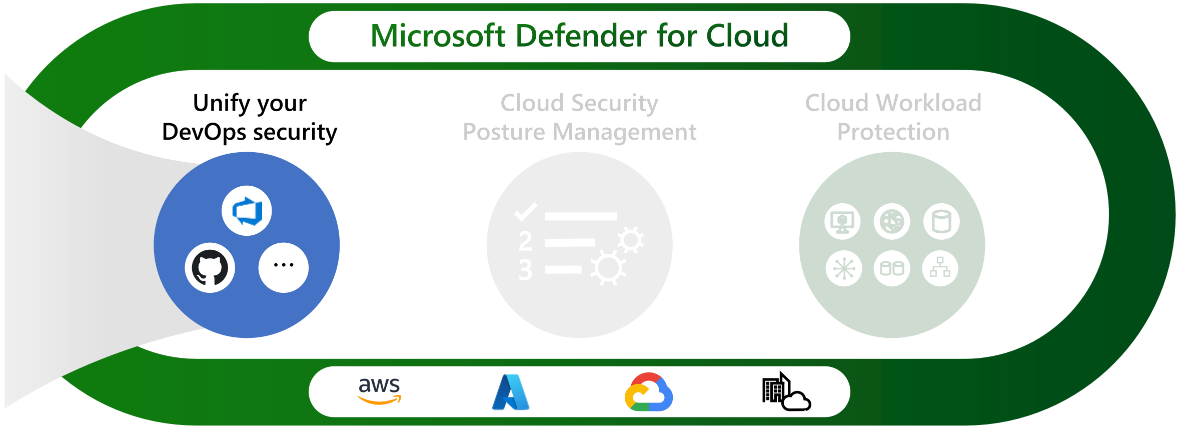
ARM | Bicep | Terraform | CloudFormation | Many more

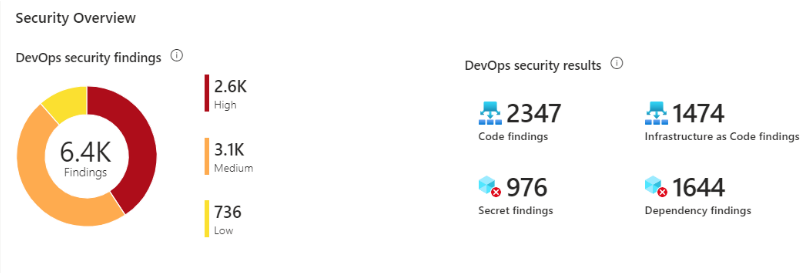
Code-to-cloud contextualization

Across multipipeline and multicloud environments

Integrated workflows

Pull request annotations | Developer ownership assignments


Microsoft Defender for Cloud
Unify your DevOps security
Cloud Security Posture Management
Cloud Workload Protection
aws



Security Overview

DevOps security findings

6.4K Findings

2.6K High

3.1K Medium

736 Low

DevOps security results

2347 Code findings

1474 Infrastructure as Code findings

976 Secret findings

1644 Dependency findings

DevOps posture management uses DevOps scanners to identify weaknesses in source code management and continuous integration/continuous delivery pipelines by running checks against the security configurations and access controls.

Resources

- ✓ Microsoft Defender for Cloud Security Posture Management
- ✓ Defender for Cloud Blog
- ✓ Prioritize Risk remediation with Attack Path Analysis
- ✓ A Proactive Approach to Cloud Security Posture Management
- ✓ Proacting Hunting with Cloud Security Explorer
- ✓ One click to cover containers & Kubernetes in Defender CSPM
- ✓ Container Security in Microsoft Defender for Cloud
- ✓ Data security capabilities in Microsoft Defender for Cloud
- ✓ Defender for Cloud in the field video series
- ✓ Cloud security explorer and Attack path analysis
- ✓ Agentless Container Posture Management

#GlobalAzure
#GlobalAzureMilano

THANK YOU!!!

Slides will be available on Global Azure 2024 page
on Azure Meetup Milano website