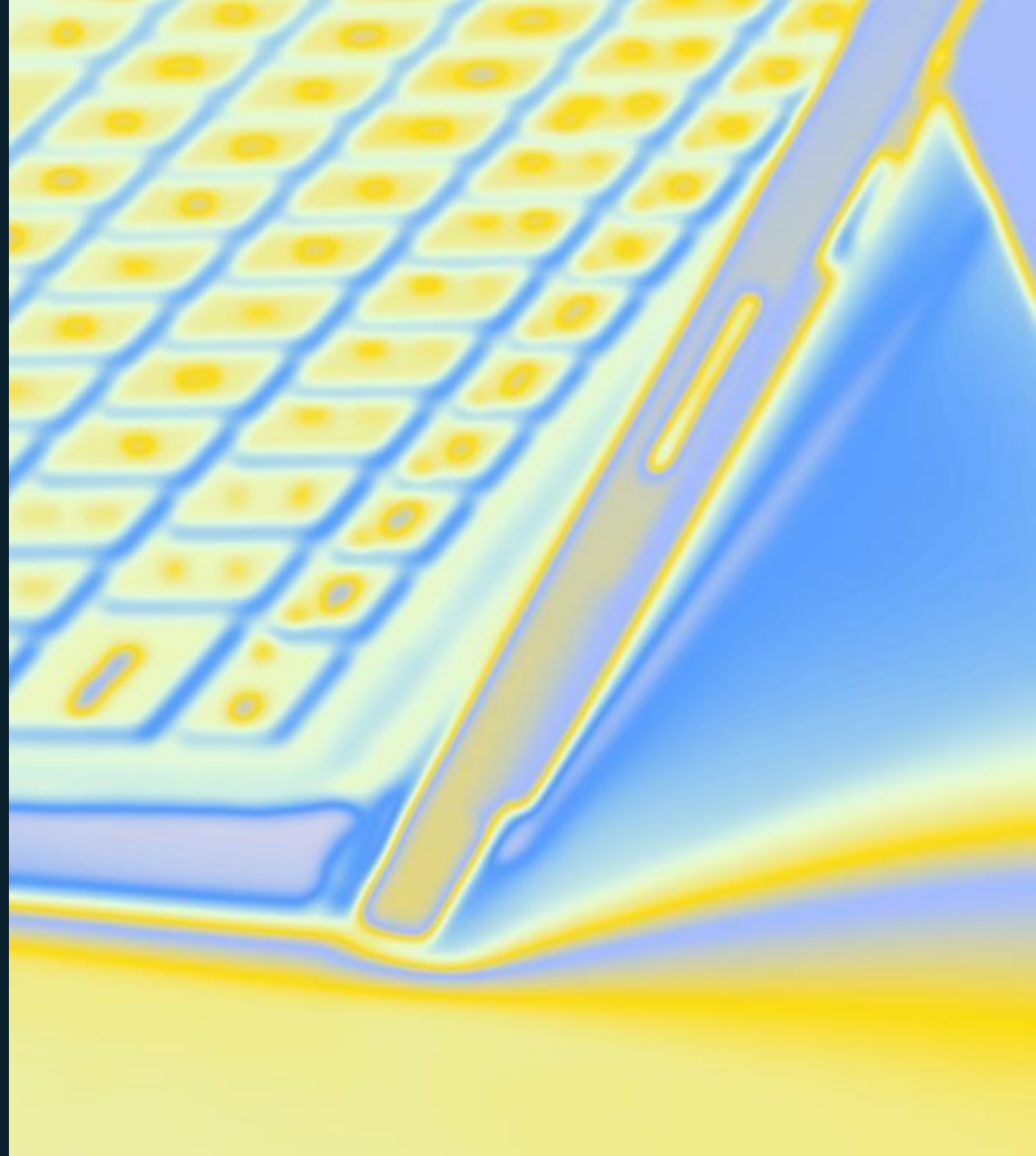
Microsoft Security

CSPM as the glue between cloud and security

Rhesa Baar



Rhesa

Sr. Solution Engineer

@ Microsoft

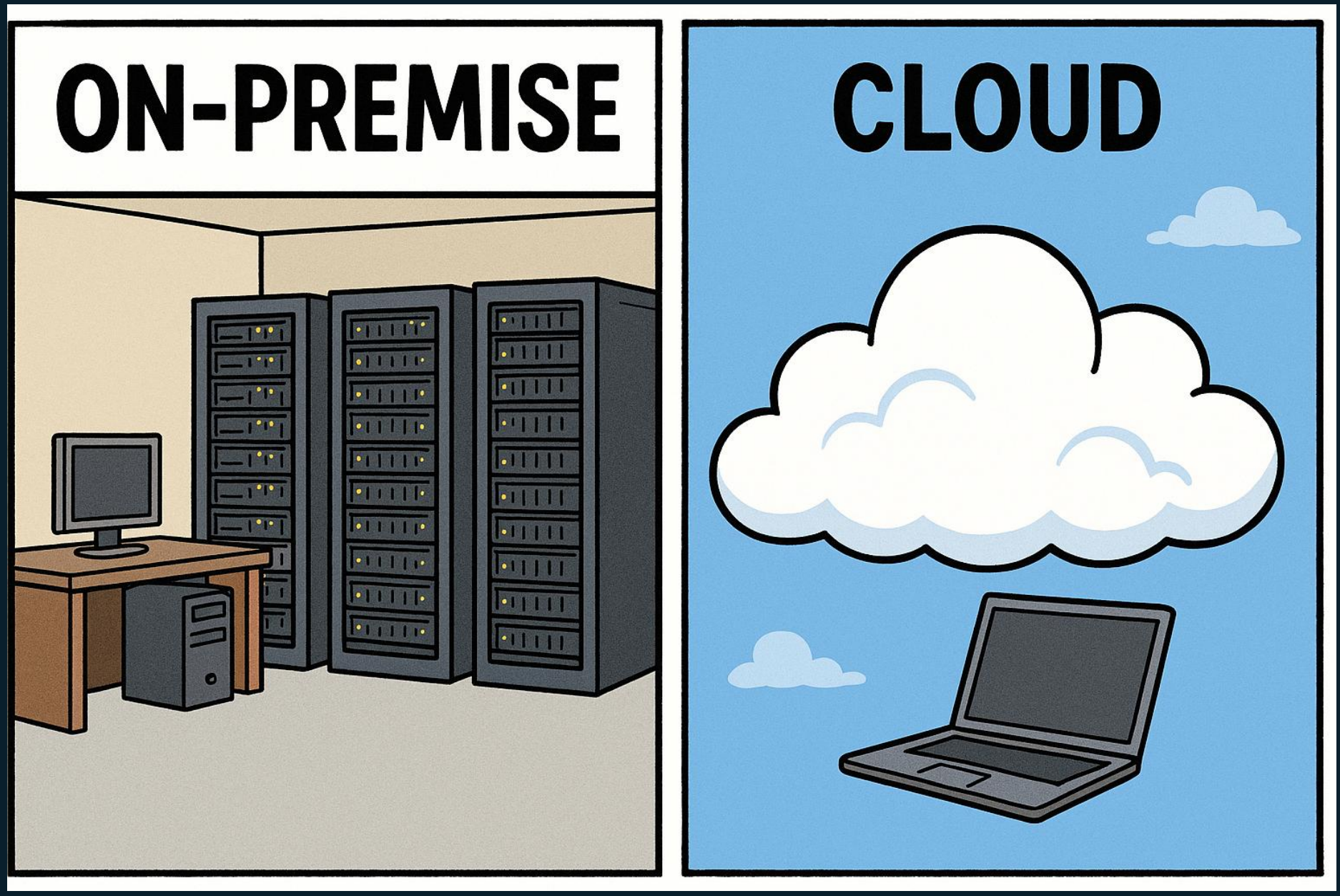
Cloud & AI

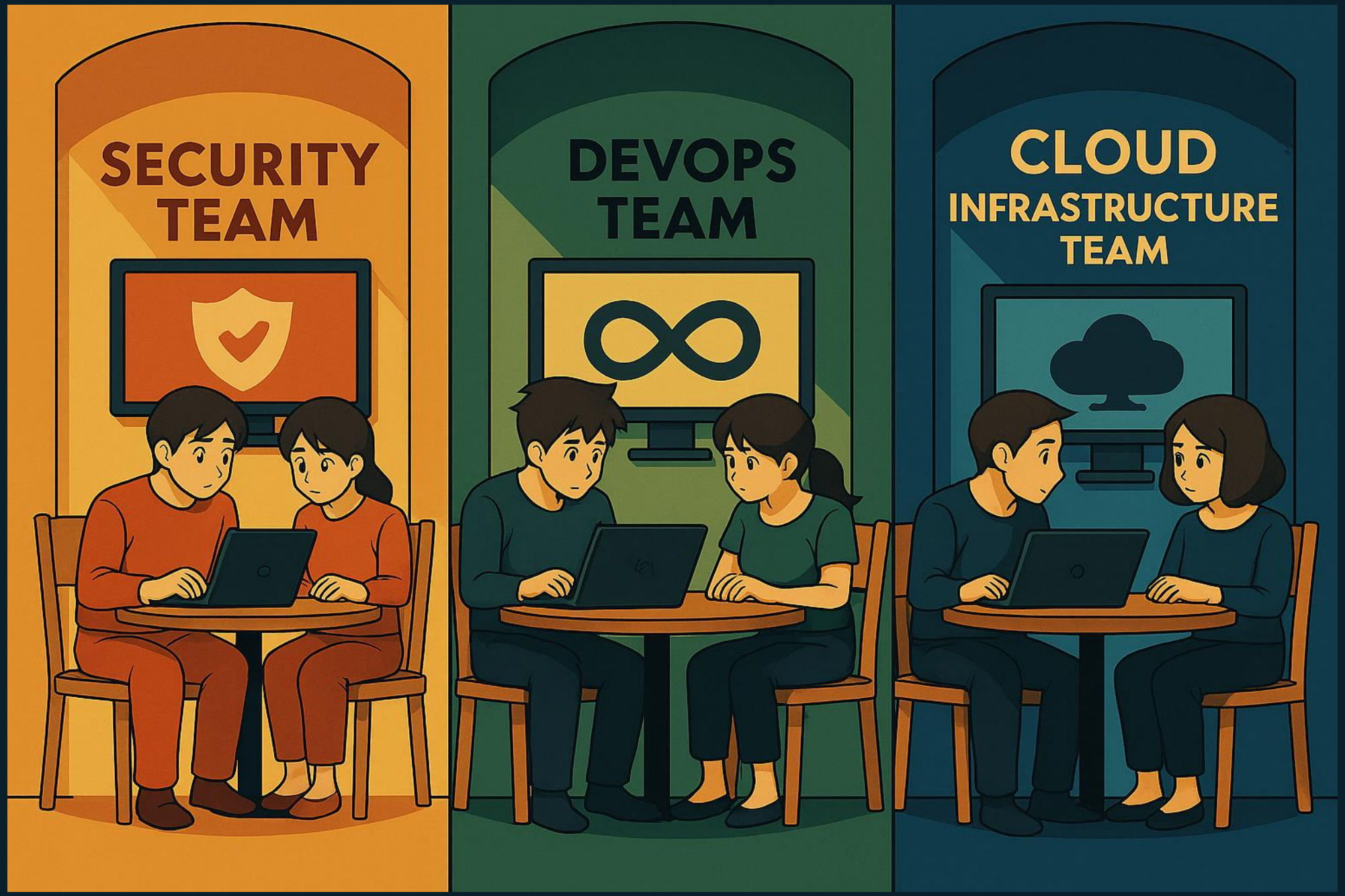
Infrastructure & Security

Agenda

- Defender for Cloud
  - CSPM
- Integration with XDR
- Q&A


DEMO
GOD

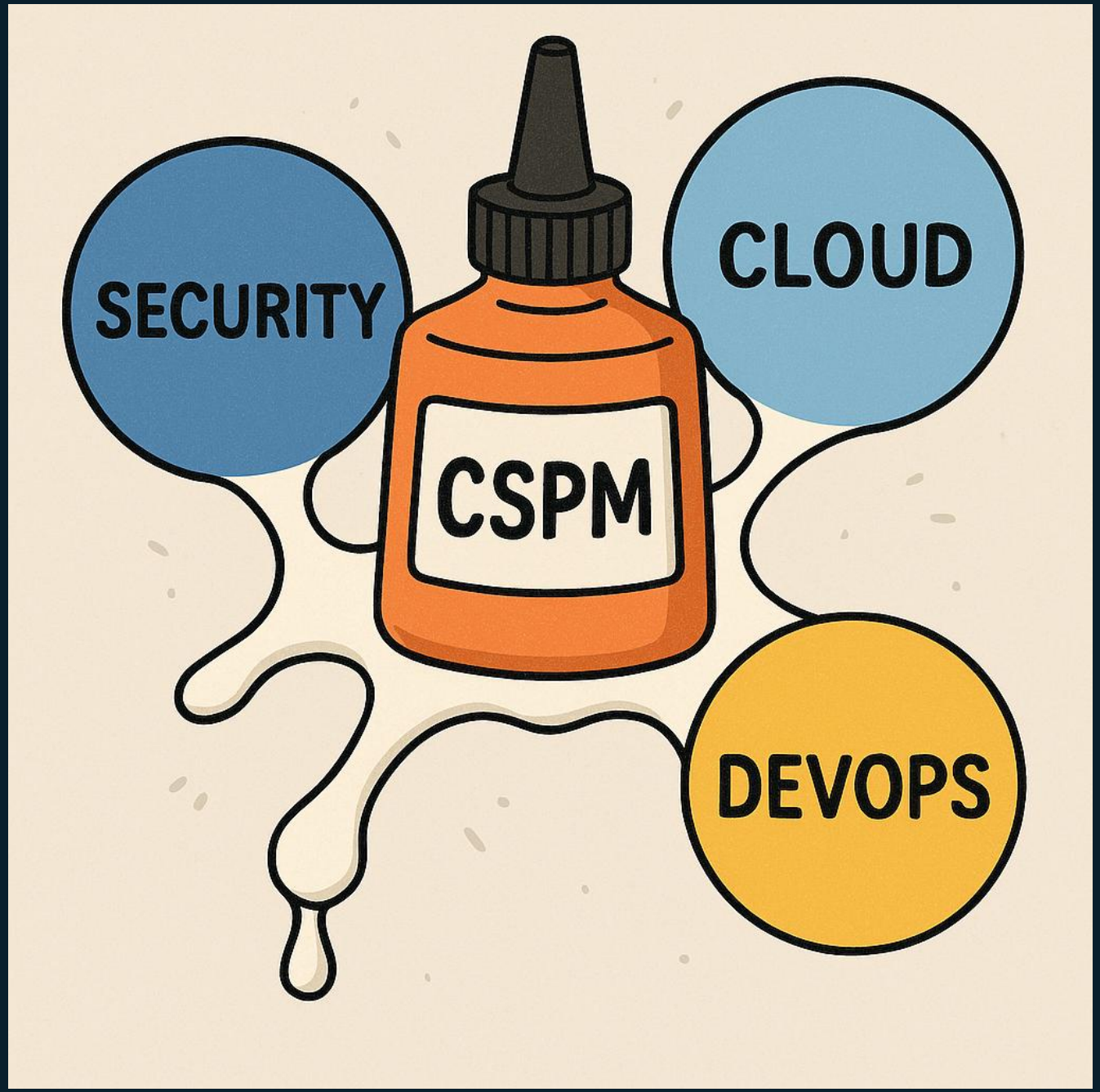

ON-PREMISE
CLOUD


SECURITY TEAM
DEVOPS TEAM
CLOUD INFRASTRUCTURE TEAM

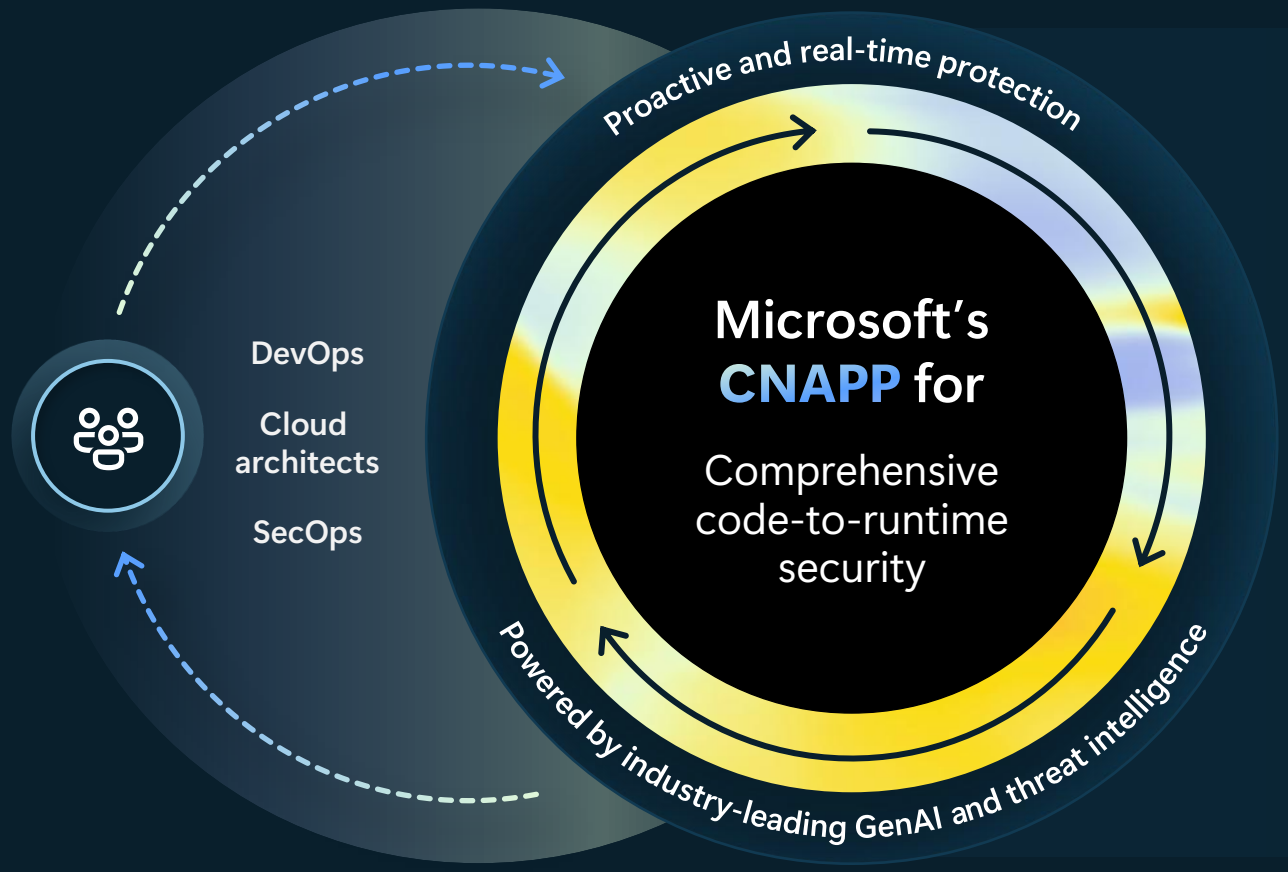
AZURE POLICIES
AZURE
LANDING ZONES


VULNERABILITIES
HIGH
HIGH
HIGH
HIGH
HIGH
VULNERABILITIES
HIGH
HIGH
HIGH
HIGH
HIGH
VULNERABILITIES
HIGH
HIGH
HIGH
HIGH
HIGH
SECURITY


VULNERABILITIES
LOW LOW
LOW LOW
LOW LOW
VULNERABILITIES
LOW LOW
LOW LOW
VULNERABILITIES
LOW LOW
LOW LOW
LOW LOW
DEVOPS


SECURITY
CLOUD
CSPM
DEVOPS

Microsoft Defender for Cloud



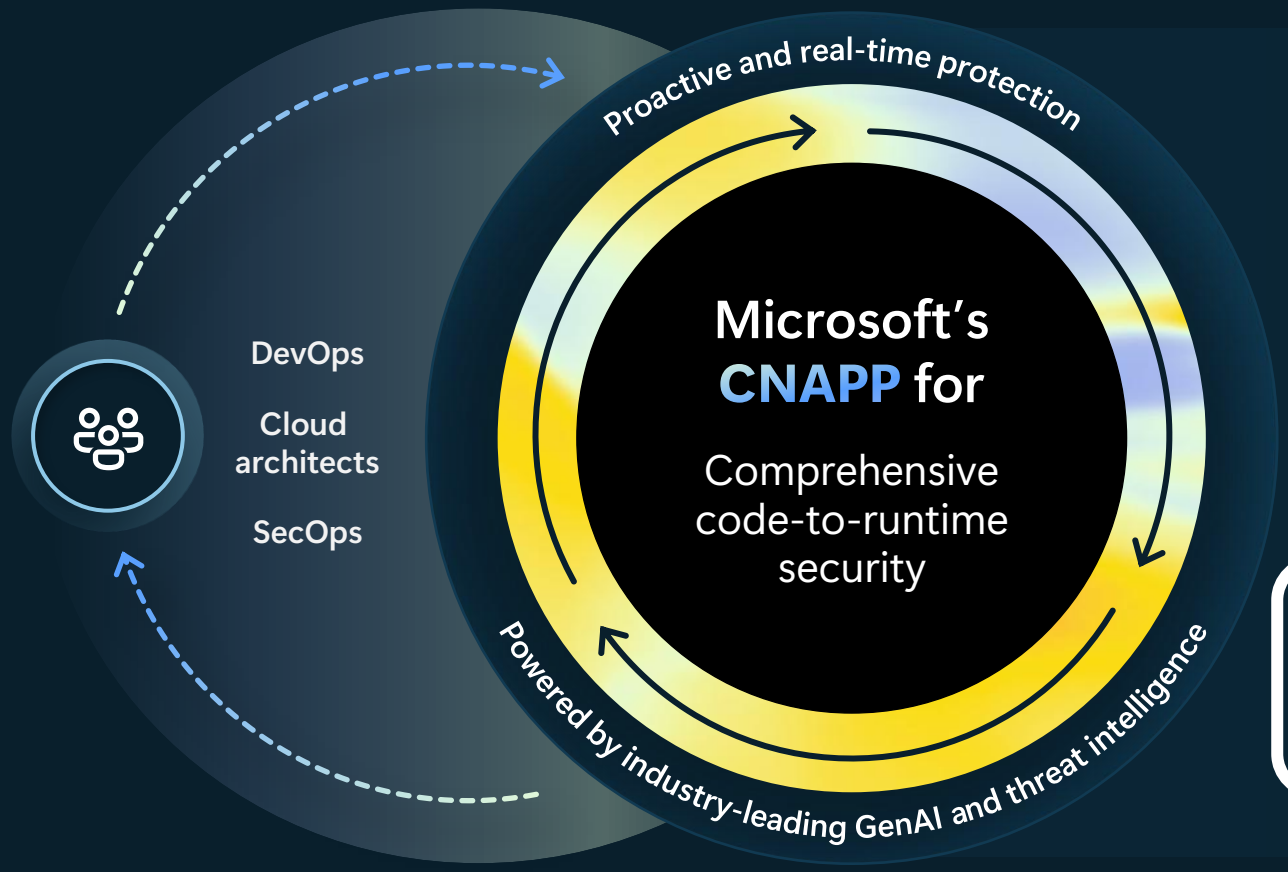
Unify security across the full app lifecycle

Prioritize the risks that matter most

Respond to cloud threats in near real-time

AWS | Azure | Google Cloud | Azure DevOps | GitHub | GitLab

Microsoft Defender for Cloud



Unify security across the full app lifecycle

Prioritize the risks that matter most

Respond to cloud threats in near real-time

AWS | Azure | Google Cloud | Azure DevOps | GitHub | GitLab

Threat Protection on all layers

Compute

- Any server
- Azure VMSS
- Unmanaged Kubernetes
- Kubernetes
- Azure AKS
- Amazon EKS
- Amazon EC2
- Google GKE
- Google Compute

Service layer

- Azure DNS
- Azure Key Vault
- Azure Resource Manager
- Azure App Services
- Azure API Management
- Azure Bastion
- Azure Firewall
- Azure Web Application Firewall
- Azure DDoS Protection

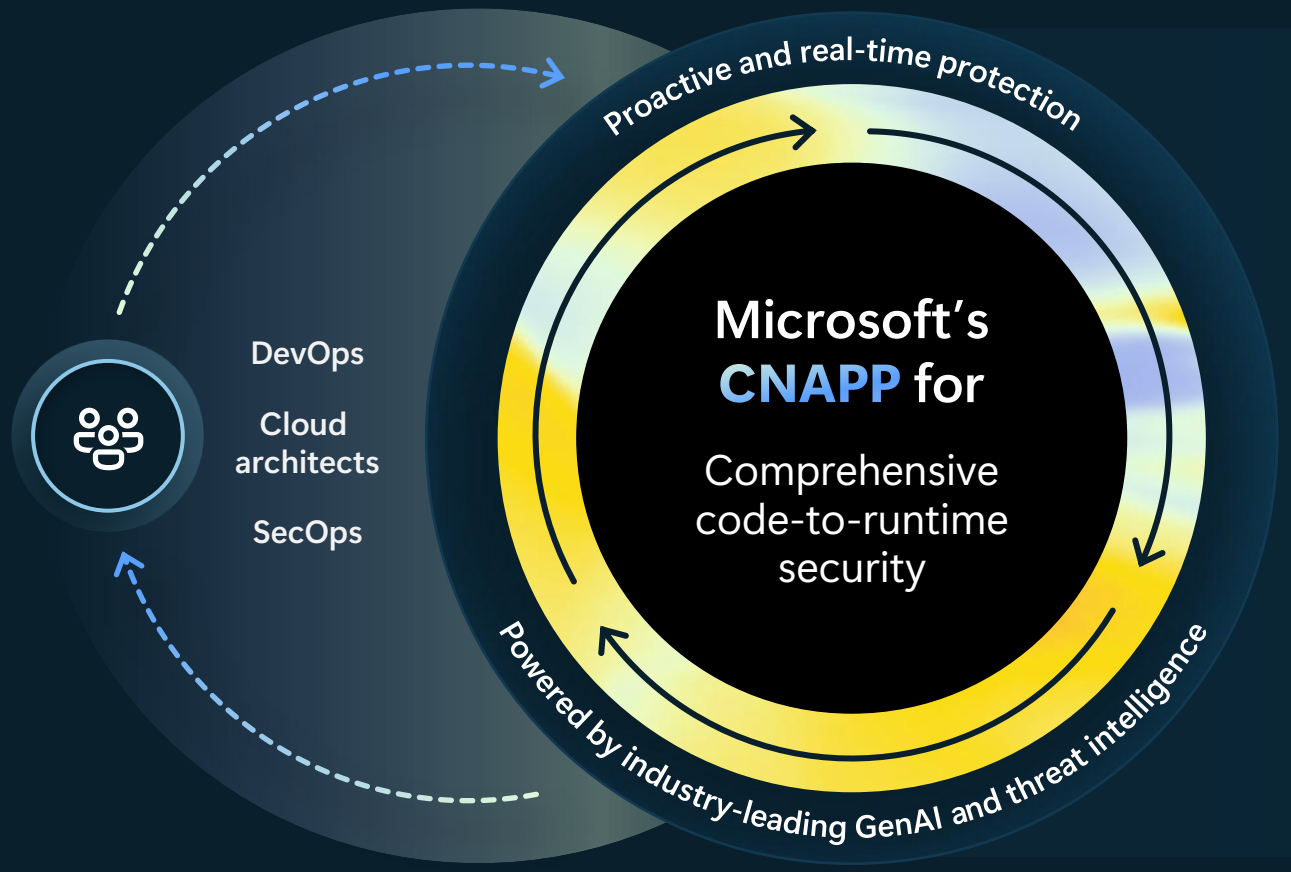
Databases and storage

- Azure Blob Storage
- Azure Files
- Azure Data Lake Storage
- Azure SQL
- SQL on Multicloud VM
- MySQL
- Postgres SQL
- Maria DB
- Azure Cosmos DB
- AWS RDS

AI workloads and models

- Azure OpenAI
- Azure AI Foundry Models

Microsoft Defender for Cloud



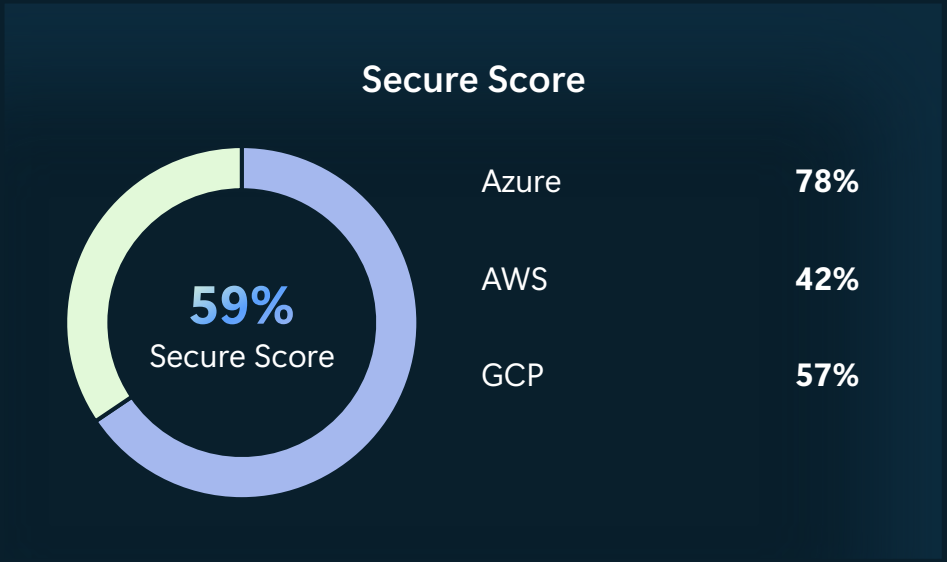
Unify security across the full app lifecycle

Prioritize the risks that matter most

Respond to cloud threats in near real-time

AWS | Azure | Google Cloud | Azure DevOps | GitHub | GitLab

Where it started with



Cloud Security Posture Management in Microsoft Defender

Contextual and prioritized security posture management across the entire cloud application lifecycle

Pinpoint and remediate risks

Identify and remediate critical risks and potential attack paths across your cloud environments and developer pipelines

Unify security standards and cloud policies

Streamline multicloud compliance and security best practices with built-in security standards and custom recommendations

Fortify sensitive data across clouds

Maintain ongoing visibility into your cloud data estate and proactively harden at-risk resources containing sensitive data

Prevent future risks by fixing in code

Prevent reoccurring risks by tracing issues and enable developer collaboration to fix issues in infrastructure as code (IaC) templates

AWS **Azure** **Google Cloud** **Azure DevOps** **GitHub** **GitLab**

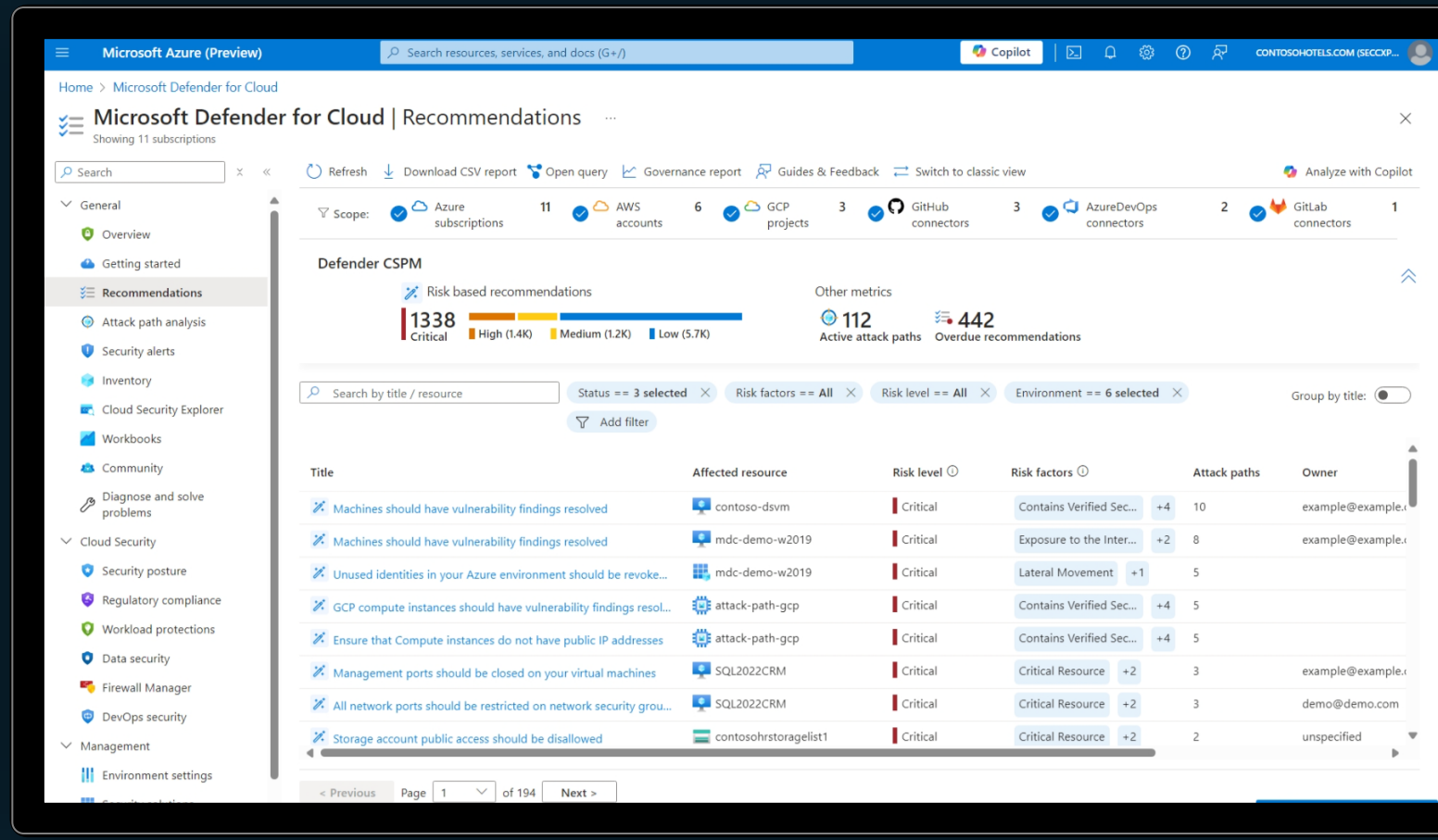
Note: Microsoft is unifying cloud posture management capabilities directly within the Defender portal. The Azure portal remains important for Defender for Cloud personas beyond security teams such as DevOps. Hence, adding security for new resources continues to remain in the Azure portal. Looking ahead, we will offer security and management of new resources directly within the Defender portal. Additionally, large organizations will be able to manage multiple-tenants from this unified experience as well.

Take a risk-based approach to prioritize remediation

Context-aware risk prioritization engine calculates the risk level of each security recommendation

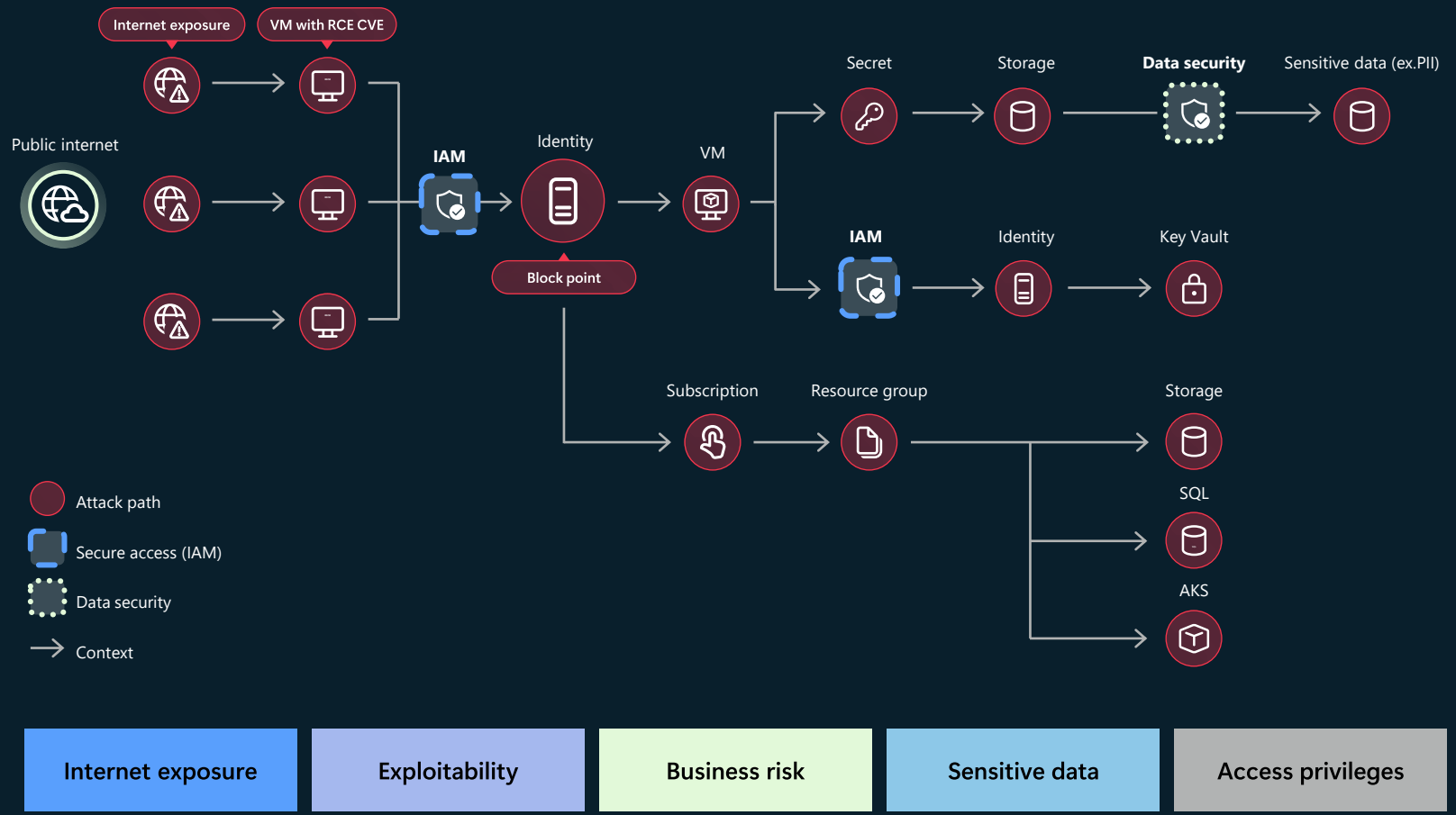
Aggregate exploitability and business impact of risk factors of each resource, potential impact of security issue, and attack paths determine risk levels

Granular visibility at the resource level with the ability to exempt resources to filter out unnecessary security recommendations



Cut through the noise and get in front of your most critical multicloud risks

- **Trace risks across** the development lifecycle with code-to-cloud mapping
- **Identify sophisticated attack paths** such as lateral movement across clouds using contextual security insights
- **Define critical resources to prioritize action** on risks that pose the most risks to your organization
- **Accelerate risk remediation** further with the integrated power of generative AI using Microsoft Security Copilot



Microsoft Defender for Cloud | Cloud Security Explorer

Showing 7 subscriptions

Search

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

Cloud Security
- Security posture
- Regulatory compliance
- Workload protections
- Data and AI security
- Network security
- DevOps security

Management
- Environment settings
- Workflow automation

Share query link | Download CSV report | Guides & Feedback

What would you like to search?

Query builde

Select resource types

Start creating a query

Use the Cloud Security Explorer query builder to easily run graph-based queries and proactively hunt for security risks in your cloud environment.

Learn more

Scope : All

Search

Query templates

ADO and Github containing a vulnerability

ADO and Github repositories containing code vulnerable to Apache Parquet vulnerability CVE-2025-30065

Open query >

Container images vulnerable to Apache Parquet vulnerability CVE-2025-30065

Returns all container images which are vulnerable to Apache Parquet vulnerability CVE-2025-30065

Open query >

Internet exposed VMs

Returns all internet exposed virtual machines

Open query >

Internet exposed VMs with high severity vulnerabilities

Returns all internet exposed virtual machines that have high severity vulnerabilities

Open query >

VMs vul vulneral

Returns a machines vulnerab

Open qu

Internet exposed SQL servers with managed identity

VMs with MDE agent health issues

Returns all the Azure virtual machines

AI workloads and models in use

Returns all AI workloads and artifacts

Generative AI vulnerable code repositories that provision Azure OpenAI

Containe images w vulnerabi

Understand gaps in your cloud compliance posture

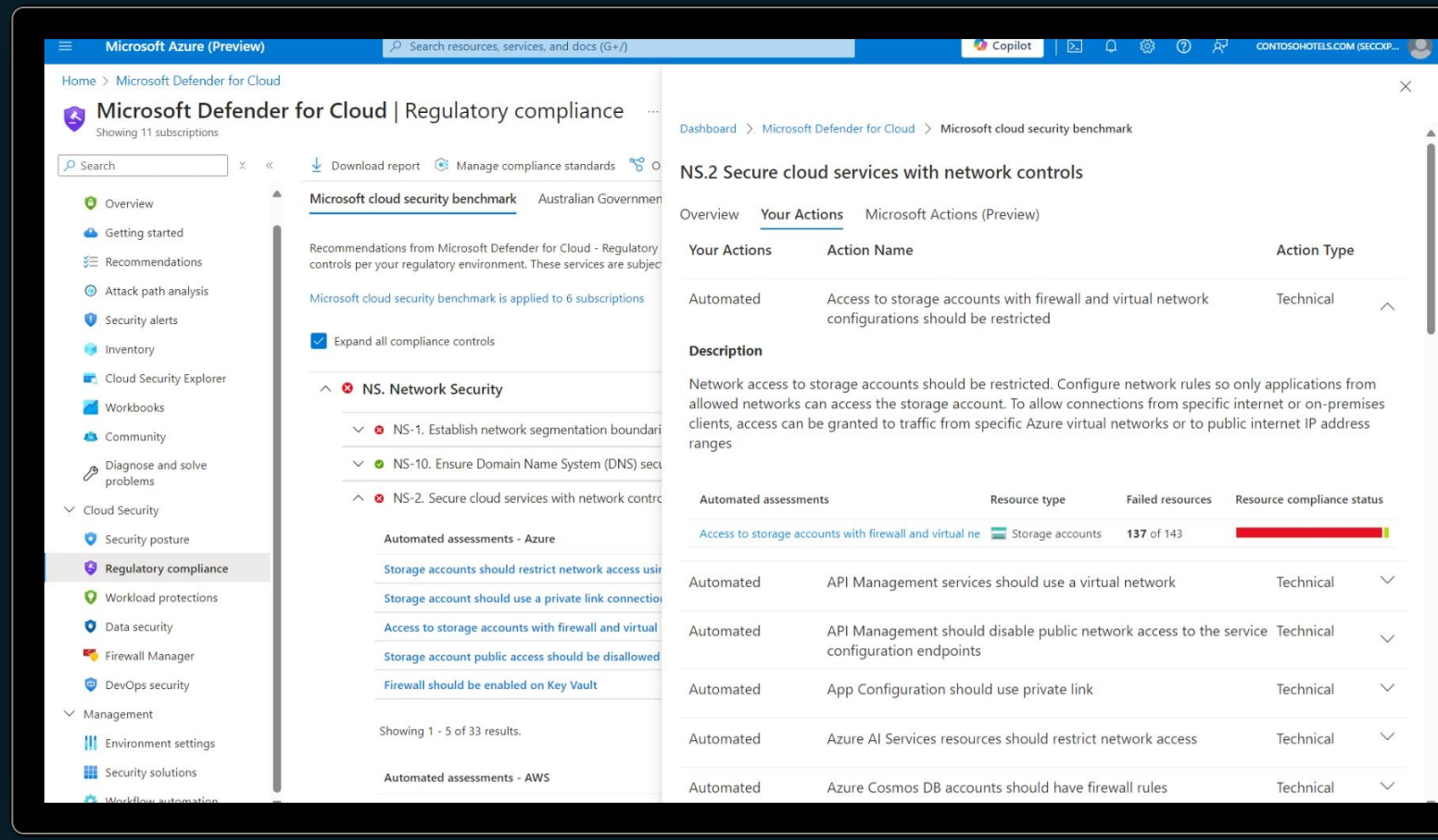
Assess and manage your cloud security compliance

Continuously assess your cloud resources across AWS, Azure, and GCP in a single, integrated dashboard

- Summary and custom reports
- Track compliance over time
- Integrate your cloud compliance posture with Purview Compliance Manager

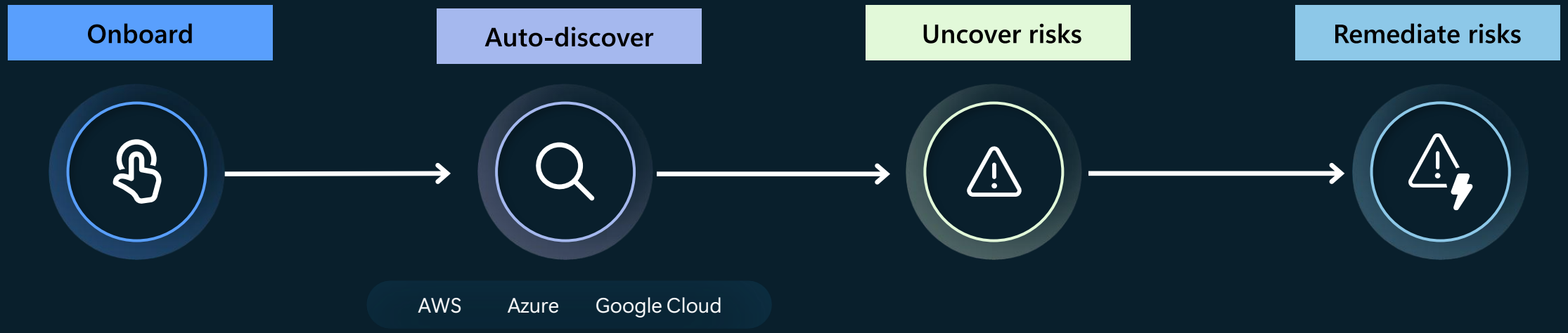
Supported (among others):

- ✓ CIS
- ✓ SOC 2
- ✓ HIPAA
- ✓ PCI DSS
- ✓ ISO 2700
- ✓ NIST 800-53r5
- ✓ Local/national compliance standards
- ✓ Microsoft cloud security benchmark
- ✓ AWS foundational security best practices



Data-aware security posture

Strengthen cloud data security posture by uncovering the cloud data estate and risks to data breaches



Agentless onboarding of multicloud data resources, one-click enablement

Automatically discover your cloud data estate to surface accessibility, sensitive data, and data flows

Uncover risks to your data resources through the cloud security explorer and attack path analysis

Strengthen your cloud data security posture with built-in insights, recommendations, and quick fixes

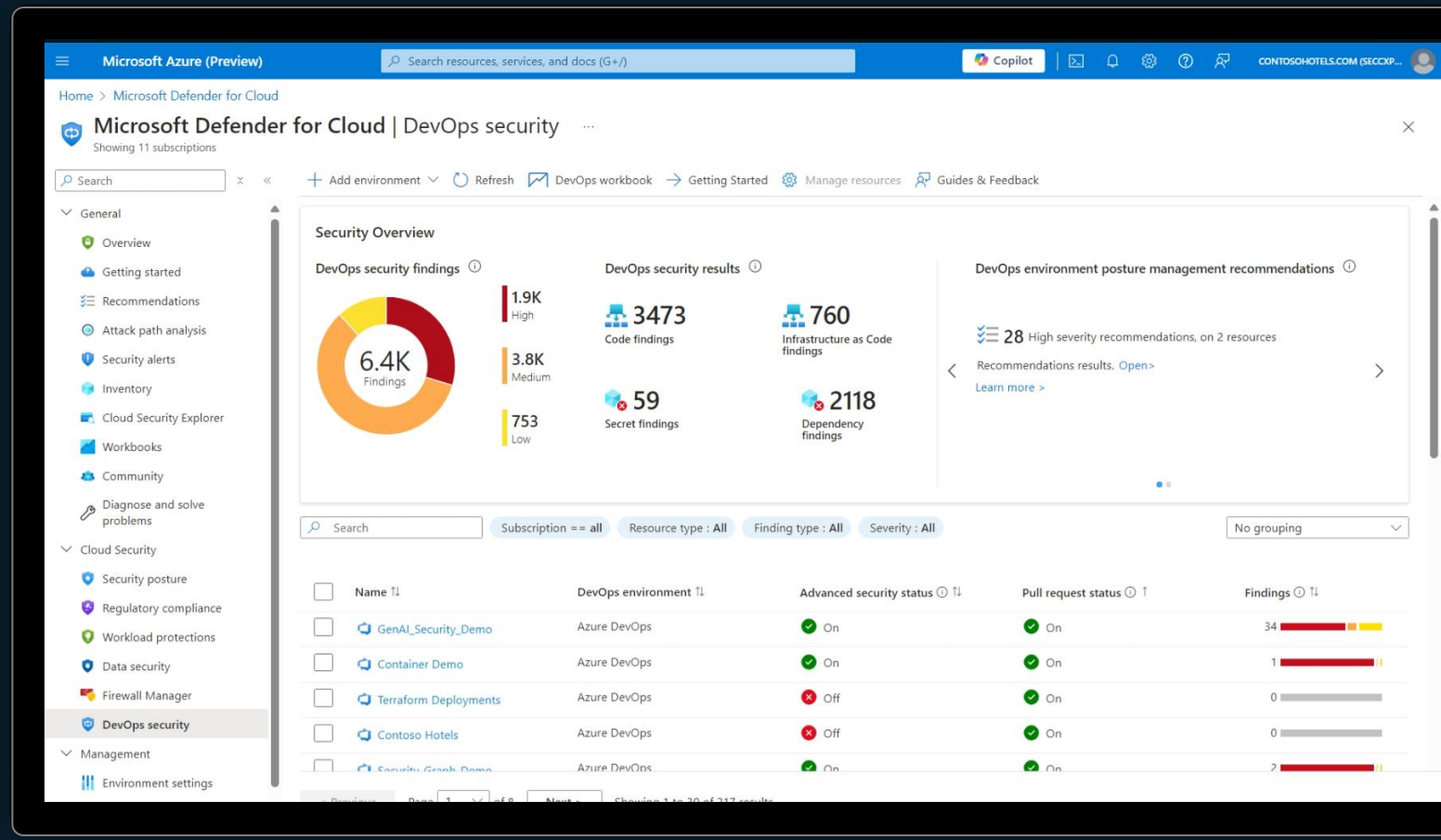
Unify visibility into application security posture

Discover DevOps resources across multicloud and multi-pipeline environments

- GitHub
- Azure DevOps
- GitLab

Connect to DevOps environments for ongoing deep analysis into resources

- Code scanning*
- End-to-end secrets scanning*
- Open-source dependency scanning*
- API security testing**
- AI infused DevSecOps* (preview)

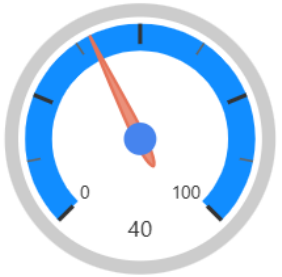


*Requires GitHub Advanced Security on GitHub, Azure DevOps, or GitLab Ultimate
**Enabled through integration with Azure Marketplace partner ecosystem

Subscription Name

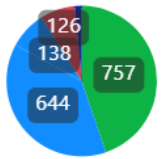
ME-MngEnvMCAP482351-sdrinkenburg-1
ME-MngEnvMCAP482351-sdrinkenburg-2

Secure Score %



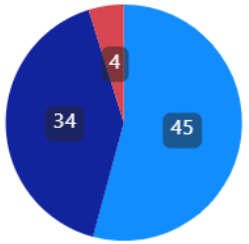
Risk Level Recommendations

Low Medium High Critical Unknown



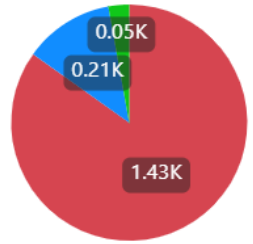
18 Attack Paths

Medium High Critical



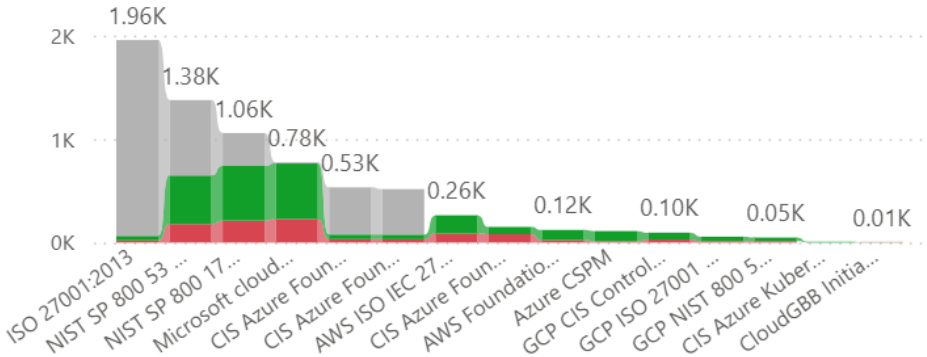
Remediation Completion

Unassigned Overdue OnTime



Compliance

Failed Passed Skipped

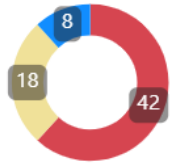


Top Resource at Risk

Resource Name	Resource Type	Score
WebSrv-UB-01	virtualmachines	689
WebSrv-UB-02	virtualmachines	175
CloudGBB-Container	repos	138
WebSrv-INT-UB-01	virtualmachines	129
eks-01-eks-group-Node	ec2instance	101
eks-01-eks-group-Node	ec2instance	67
DEVSrv-UB-01	virtualmachines	53
gke-websrv-01-3855242620296627854	machines	51
WebSrv-AWS-01	ec2instance	47
cloudgbbcontainer	securityentitydata	44
DEVWks-WIN-02	virtualmachines	41

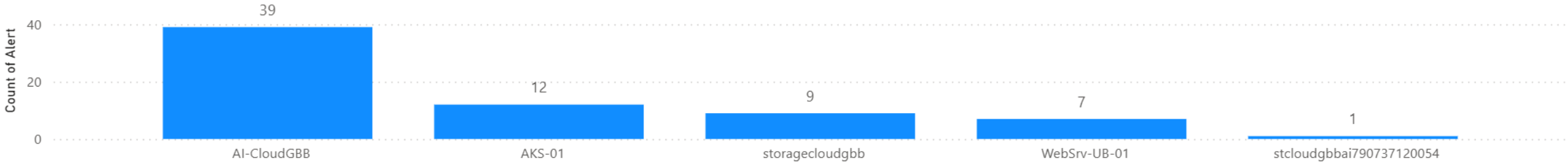
Alert Distribution

High Medium Low



Active

Alert by Resource



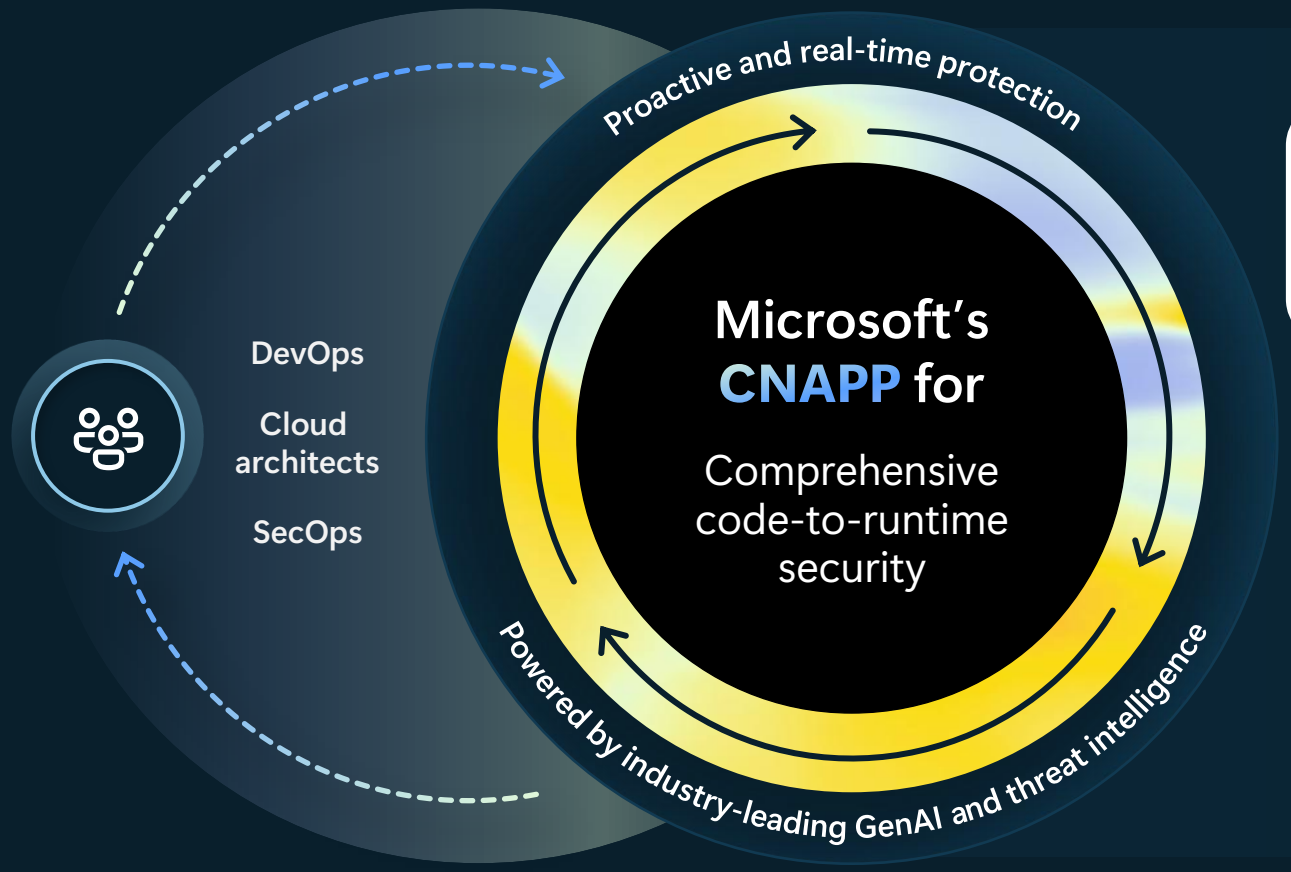
Foundational CSPM vs Microsoft Defender CSPM

Feature	Foundational CSPM (free)	Defender CSPM (billing applies)	Cloud coverage		
			Azure	AWS	GCP
Security recommendations (across infrastructure, data, DevOps, network, permissions, 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 (Azure only)	●	●	●		
Infrastructure as code (IaC) security		●			
Code-to-cloud mapping for containers		●			
PR annotations		●			
Internet exposure analysis		●	●	●	●
KQL based recommendation customization (multicloud)		●	●	●	●
Regulatory compliance assessments		●	●	●	●
Governance (including ServiceNow integration)		●	●	●	●
Critical assets protection		●	●	●	●
Cloud infrastructure entitlement management		●	●	●	●

Foundational CSPM vs Microsoft Defender CSPM, cont.

Feature	Foundational CSPM (free)	Defender CSPM (billing applies)	Cloud coverage		
			Azure	AWS	GCP
AI security posture management (AI models and AI agents)		●	●	●	●
Attack path analysis		●	●	●	●
Risk prioritization		●	●	●	●
Risk hunting with cloud security explorer		●	●	●	●
EASM insights in network exposure		●	●	●	●
Agentless vulnerability assessments for compute (using Microsoft Defender Vulnerability Management)		●	●	●	●
Agentless VM secrets scanning		●	●	●	●
Agentless discovery for Kubernetes		●	●	●	●
Agentless vulnerability assessments for container images, including registry scanning		●	●	●	●
Data security posture for storage and databases		●	●	●	●
API security posture management		●	●		
Azure Kubernetes Service security dashboard (preview)		●	●		
Agentless misconfiguration and vulnerability assessments for Serverless resources (preview)		●	●	●	
Agentless code scanning (integration with GitHub Advanced Security) (preview)		●	●	●	●
CLI-based scanning (using Microsoft Devender Vulnerability Management) (preview)		●	●	●	●
Code-to-runtime mapping (preview)		●	●	●	●
Multicloud log ingestion (preview)		●	●	●	●

Microsoft Defender for Cloud



- Unify security across the full app lifecycle
- Prioritize the risks that matter most
- Respond to cloud threats in near real-time

AWS | Azure | Google Cloud | Azure DevOps | GitHub | GitLab

Extend security into software development lifecycle

Security

- DevOps security posture management
- Infrastructure-as-code security
- Code-to-runtime visibility and remediation

Defender for Cloud
Integrated DevOps security insights from GitHub, Azure DevOps, and GitLab

Bridging the gap between DevOps and security teams

Alert prioritization

Native tool integration

Agentic remediation

Development

- Code security
- Dependencies security
- Embedded secrets protection
- Developer remediation

GitHub Advanced Security
Native code security with GitHub and Azure DevOps

Prevent recurring risks with code-to-runtime remediation

Code-to-runtime contextualization

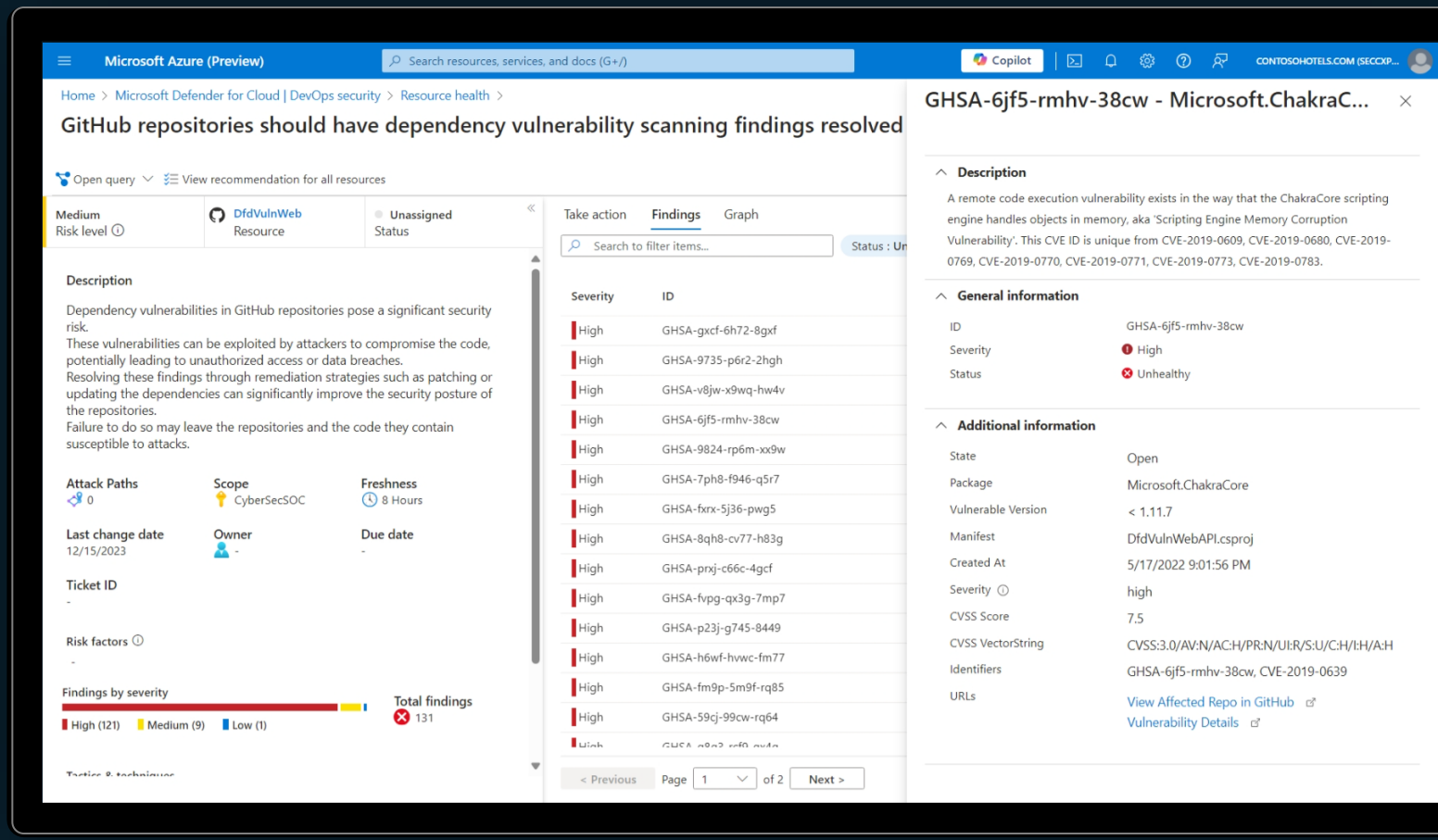
- Enrich cloud security graph with application code insights
- Automatically trace running containers and container images to source code origin

Identify critical attack paths with application code insights

- OSS vulnerabilities
- Exposed secrets
- Container image vulnerabilities

Drive remediation in code

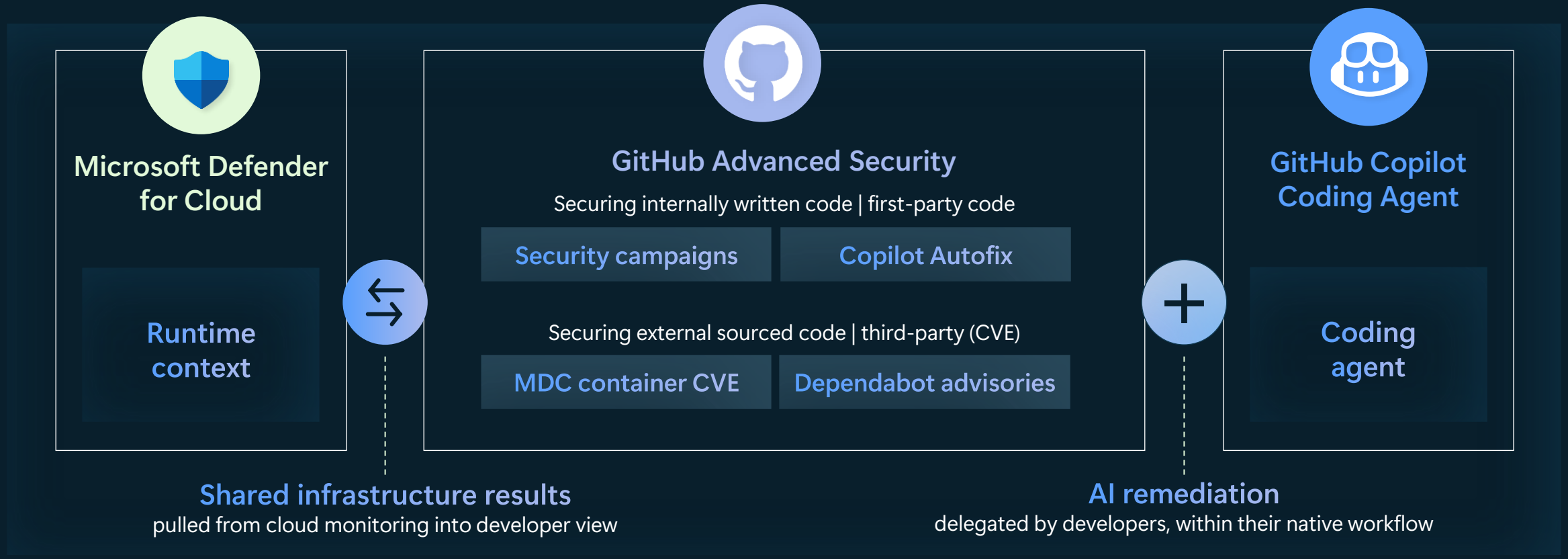
- Custom workflows for developer ownership assignments with SecOps initiated pull request annotations



Microsoft Defender for Cloud and GitHub Advanced Security

IN PREVIEW

Secure code-to-cloud with AI infused DevSecOps: unify developer and security workflows, pairing runtime context with agentic remediation, all in the preferred tools of developers and security admins



Alert prioritization

Connect runtime context to code to focus only on what's exploitable

Native tool integration

DevSecOps collaboration with native security and dev tool integration, bi-directional workflows and data

Agentic remediation

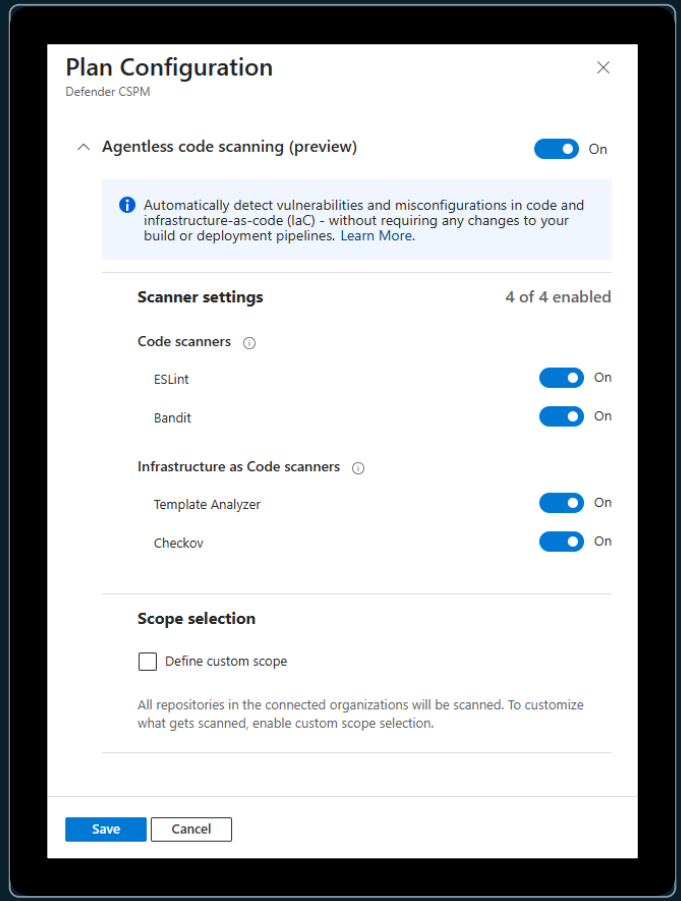
Reduce remediation time with AI suggested fixes with Copilot Autofix and GitHub Coding Agent

Detect misconfigurations in deployment

IN PREVIEW

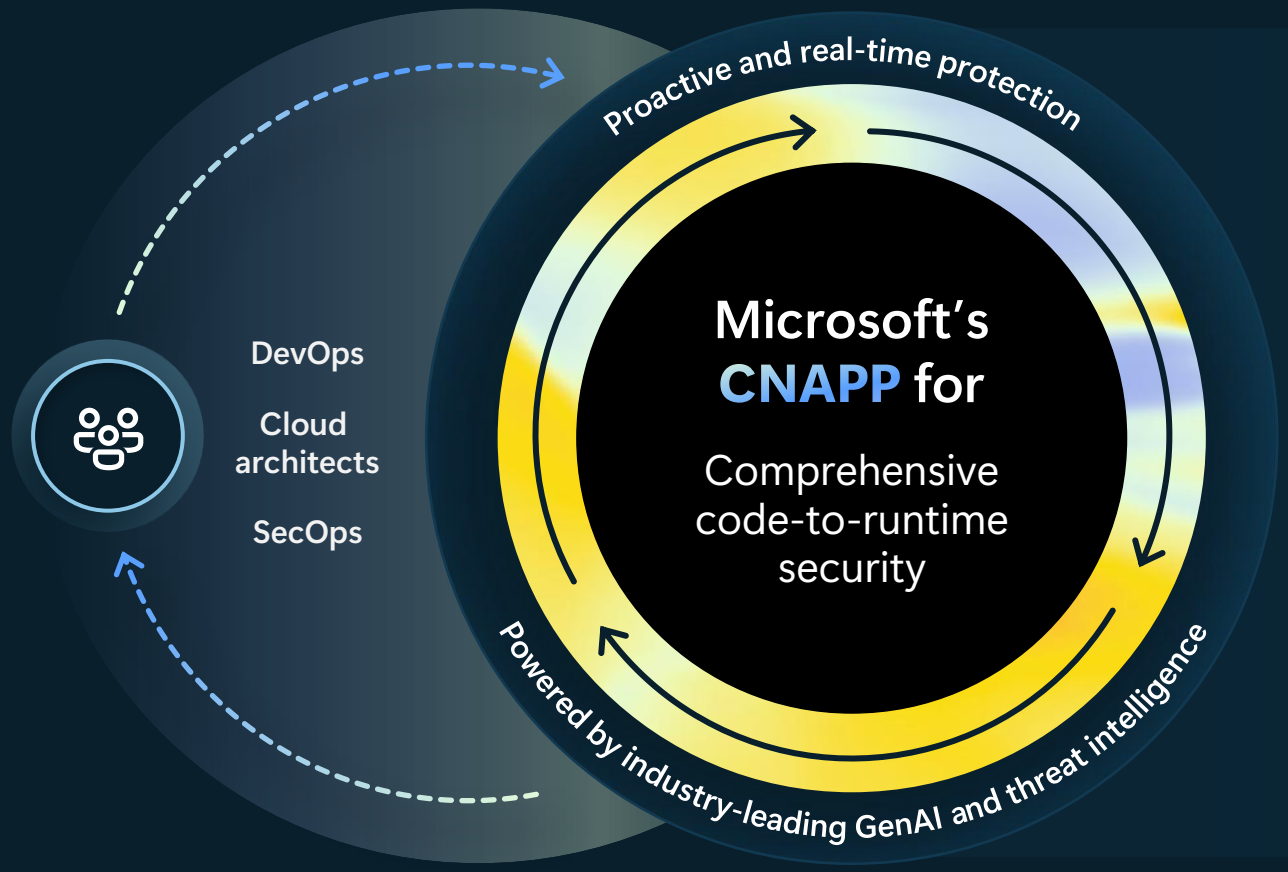
A seamless way to discover risks in code and respond faster

- **Frictionless onboarding**: no pipeline changes required
- **Enterprise-scale**: covers large environments with one connector
- **Quick remediation**: scan results delivered in under 60 minutes, reducing exposure time
- **Developer-independent, pipeline-friendly**: preserves developer velocity, doesn't impact pipeline speed



- Fix DevOps environment misconfigurations
- Fix code misconfigurations
- Fix IaC templates vulnerabilities

Microsoft Defender for Cloud



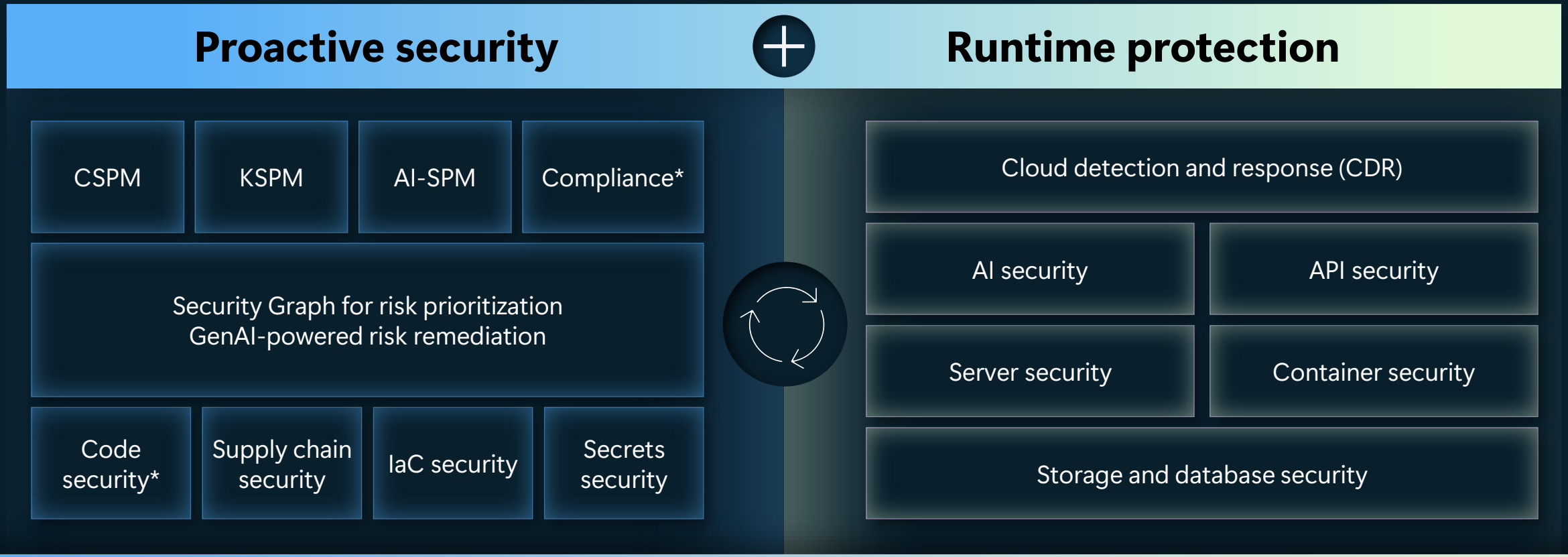
Unify security across the full app lifecycle

Prioritize the risks that matter most

Respond to cloud threats in near real-time

AWS | Azure | Google Cloud | Azure DevOps | GitHub | GitLab

Microsoft Defender offers unified cloud security



Unified platform across multicloud, multi-pipeline environments

Agent-based and agentless protections

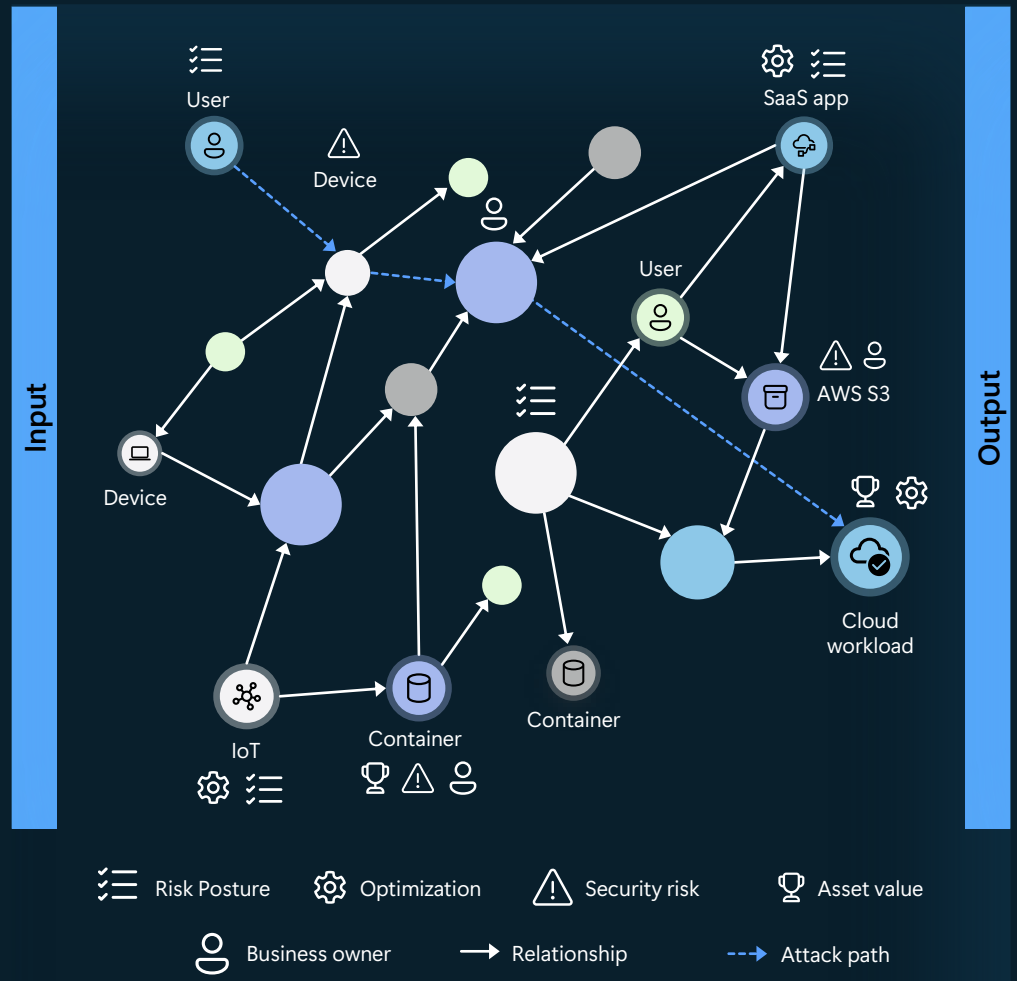
Built-in, natively integrated security controls

* Will be available soon in the unified experience
Looking ahead- Customers will soon be able to secure and manage new resources directly within the Defender portal.
Additionally, large organizations will be able to manage multiple-tenants from this unified experience as well.

XDR Integration

Extend posture management to the entire digital estate

- CMDB
- Vulnerability management
- Email security
- Identity security
- Endpoint security
- SaaS security
- **Application security**
- **Cloud security**
- External attack surface
- Threat intelligence



Attack surface management

Continuously discover, contextualize and manage an organization's assets to provide defenders with an attacker perspective

Attack path analysis

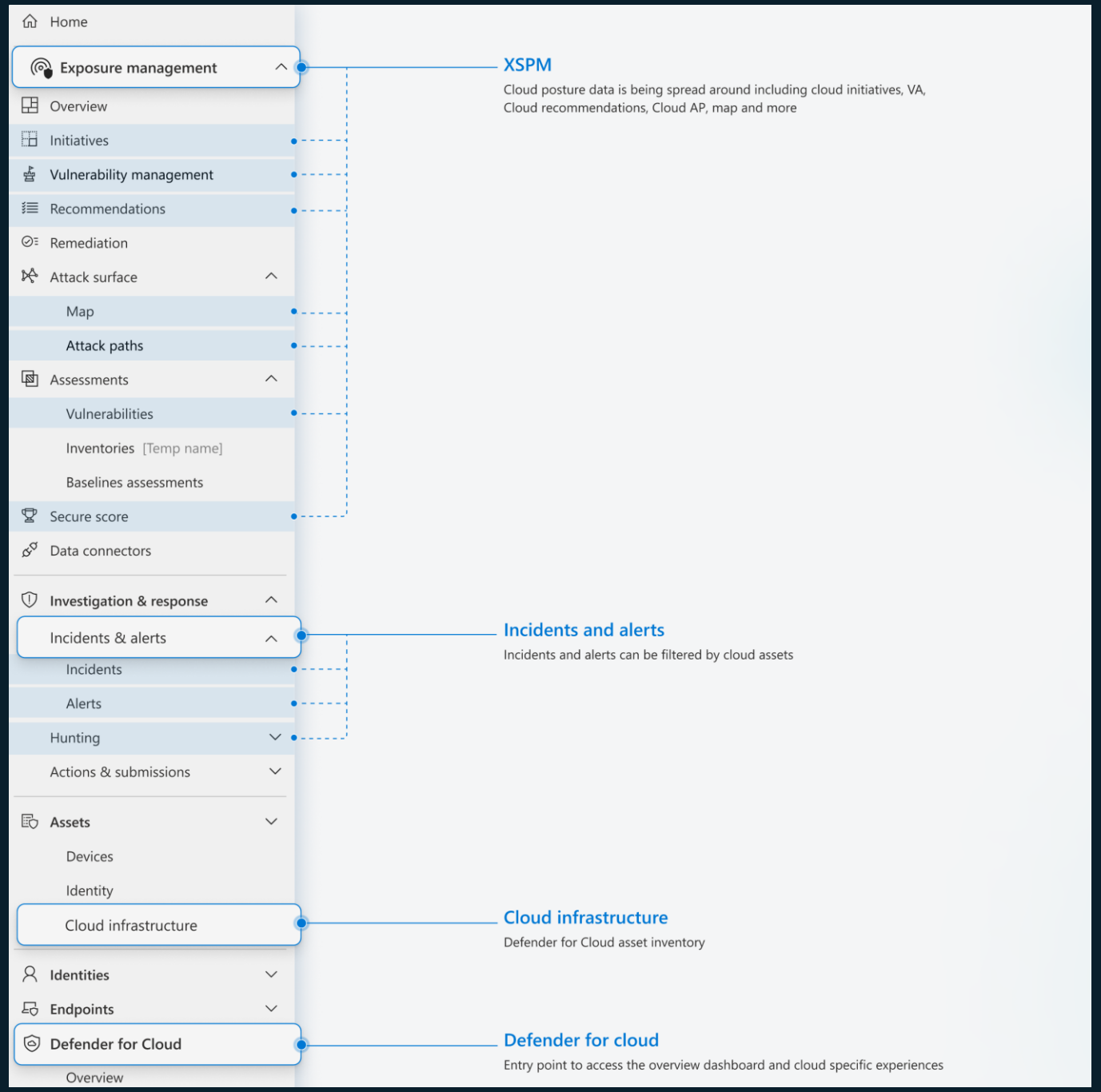
Prioritize weaknesses by considering the attacker's perspective, moving away from the traditional siloed approach

Unified exposure insights

Understand your security posture and proactively answer questions from key stakeholders using out-of-the-box insights

Microsoft Defender for Cloud integration with Microsoft Security Exposure Management

Cloud security: integrated across experiences



Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
Cloud infrastructure
Cases
SOC optimization
Reports
Learning hub
Trials
More resources
System
Data management
Permissions
Health
Settings
Customize navigation

Home

Dark mode

Explore the latest security solutions at Microsoft Ignite on November 18–20. Discover cutting-edge strategies for securing agentic AI in deep technical sessions and live demos. Learn more about Ignite

Defender Experts

Was this helpful?

3 incidents require your action

Incident name	Severity	Impacted assets	Pending actions
Multi-stage incident involving Privilege ...	High	632	1
ef0b1804-ac3c-403a-924a-3d1defe282fe...	Medium	14	2

See all incidents

In the last 30 days, Defender Experts resolved **99%** of your incidents.

Incidents investigated	Resolved	Resolved directly	Resolved with your help
2435	2414	1023	1391

View report

Guided tour | What's new ? | Community | Add cards

SOC optimization

Your optimization data

Optimization status

Active	In progress	Completed	Dismissed
96	0	300	0

Microsoft Sentinel automation

14 automation rules

Last 24 hours

Closed incidents	Time saved	Actions performed
0	N/A	0

Actions performed (0)

Severity (0) | Status (0) | Comments (0) | Owner (0)

Microsoft Sentinel data connectors

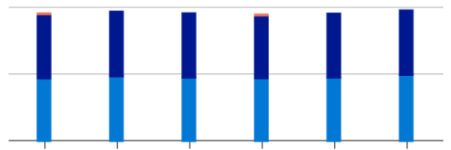
22 data connectors

Last 24 hours

Active connectors	Unhealthy connectors
21/22	1/22

TI by type (0)

Data received



ITDR Deployment Health

Protect your Identities and Identity Infrastructure with Microsoft Defender for Identity and Entra ID Protection.

Defender for Identity Deployment

Unable to determine ADCS and ADFS

Sensors deployment on ADCS	0 / 0
Sensors deployment on ADFS	0 / 0
Sensors deployment on Entra Connect	2 / 2
Sensors deployment on domain controllers	2 / 2
Health alerts	

Home
Exposure management
Investigation & response
Threat intelligence
Assets
Microsoft Sentinel
Threat management
Content management
Configuration
Data lake exploration
Identities
Endpoints
Email & collaboration
Cloud apps
Cloud infrastructure
Overview
Cases
SOC optimization
Reports
Learning hub

Guidance | Last 7 days | Environment Filter : Off | Scope filter : Off

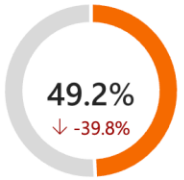
Defender for Cloud

Protects your cloud-native workloads from code to runtime.

Azure (4) AWS (3) GCP (6)
Azure DevOps (1) GitLab (6)
DockerHub (1) JFrog (3)

Security posture

Cloud secure score Moderate



View cloud initiative

Threat detection

Security alerts

High Medium 1 more

View alerts

Top actions

95 critical recommendations
Resolve critical recommendations to strengthen security posture.

79 high alerts
Resolve high security alerts to mitigate immediate threats.

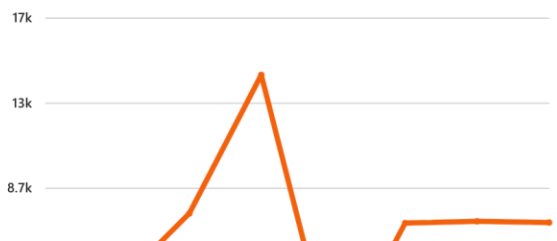
118 critical attack paths
Explore and investigate critical attack vectors.

Security posture

Cloud secure score

Security recommendations

Critical **95**
High **1921**
Medium **1723**
Low



Get Started Guide

Introducing Defender for Cloud

Learn how CNAPP now integrates across Defender portal to provide unified security insights across your multi-cloud and multi-pipeline environments

Take the full tour

Start here

Monitor Your Cloud Secure Score
Monitor how your cloud security posture improves over time. Use the secure score to identify trends, measure hardening efforts, and prioritize security recommendations.

Show me where I can find it on this page

Explore Security Alert Trends
Stay informed with a timeline view of security alerts. Understand threat patterns, investigate spikes, and assess the effectiveness of your incident response.

Show me where I can find it on this page

Learn more

Glossary

Risk-based recommendations | Attack path analysis | Cloud initiative | Investigation & response | Cloud secure score | Vulnerabilities | Cloud assets | Attack surface map | Advanced hunting | Cloud scopes | Unified RBAC

Cloud initiative

Understand your organization's cloud security posture, track changes over time, identify security issues, take

Home
Exposure management
Investigation & response
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
Cloud infrastructure
Overview
Cases
SOC optimization
Reports
Learning hub
Trials
More resources
System
Data management

Virtual machines

Asset summary and coverage

Virtual machine	Automation service	Serverless	More
461	143	49	32

Defender coverage

Covered Partially Covered Not Covered

View assets

Insights

Critical and high risk recommendations
619

Critical and high risk attack paths
10

Finding categories by risk level

Misconfigurations

Critical High Medium Low

Vulnerabilities

Critical High Medium Low

Secrets

Critical High Medium Low

Data

Asset summary and coverage

Object storage	Managed database	Hosted database	More
105	12	6	62

Defender coverage

Covered Partially Covered Not Covered

View assets

Insights

Critical and high risk recommendations
216

Critical and high risk attack paths
91

Assets with sensitive data

Object Storage
21

Managed Database
1

Containers

Home
Exposure management
Investigation & response
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
Cloud infrastructure
Overview
Cases
SOC optimization
Reports
Learning hub
Trials
More resources
System
Data management

Guidance | Last 7 days | Environment Filter : Off | Scope filter : Off

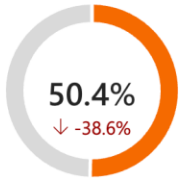
Defender for Cloud

Protects your cloud-native workloads from code to runtime.

Azure (4) AWS (3) GCP (6) Azure DevOps (1)
GitLab (6) DockerHub (1) JFrog (3)

Security posture

Cloud secure score Moderate



View cloud initiative

Threat detection

Security alerts

High Medium 1 more

View alerts

Defender coverage

Assets covered by posture and protection plans

Covered Partially Covered 1 more

View assets

Top actions

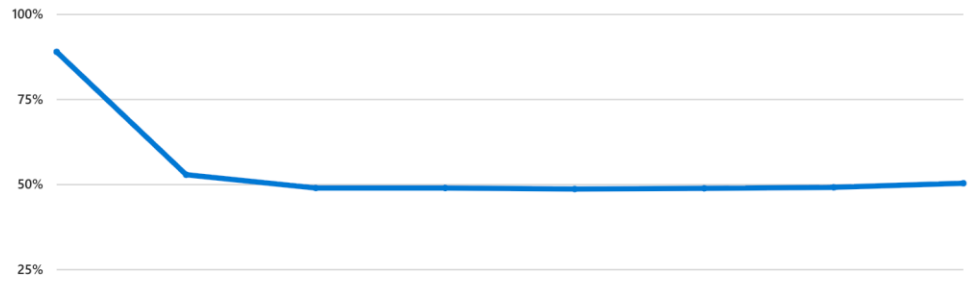
94 critical recommendations
Resolve critical recommendations to strengthen security posture.

79 high alerts
Resolve high security alerts to mitigate immediate threats.

106 critical attack paths
Explore and investigate critical attack vectors.

Security posture

Cloud secure score



Security recommendations

Critical **94**
High **1943**
Medium **1817**
Low **7502**

Home
Exposure management
Investigation & response
Incidents & alerts
Incidents
Alerts
Hunting
Actions & submissions
Partner catalog
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
Cloud infrastructure
Overview
Cases
SOC optimization
Reports

Alerts

Export | 1 Week

23 Alerts | Search for name or ID | Customize columns

Filter set:

Service/detection sources: Microsoft Defender for Cloud - ... | Add filter | Reset all

Alert name	Tags	Severity	Investigation state	Status	Category	Detection source	Product name	Impacted assets
Attestation failed on your virtual machine		Medium		New	Privilege escalation	Microsoft Defender for Ser...	Microsoft Defender for Clo...	Woodgrove-DC03
Attestation failed on your virtual machine		Medium		New	Privilege escalation	Microsoft Defender for Ser...	Microsoft Defender for Clo...	Woodgrove-DC03
Attestation failed on your virtual machine		Medium		New	Privilege escalation	Microsoft Defender for Ser...	Microsoft Defender for Clo...	Woodgrove-DC03
Attestation failed on your virtual machine		Medium		New	Privilege escalation	Microsoft Defender for Ser...	Microsoft Defender for Clo...	Woodgrove-DC03
Attestation failed on your virtual machine		Medium		New	Privilege escalation	Microsoft Defender for Ser...	Microsoft Defender for Clo...	Woodgrove-DC03
Attestation failed on your virtual machine		Medium		New	Privilege escalation	Microsoft Defender for Ser...	Microsoft Defender for Clo...	Woodgrove-DC03
Attestation failed on your virtual machine		Medium		New	Privilege escalation	Microsoft Defender for Ser...	Microsoft Defender for Clo...	Woodgrove-DC03
Attestation failed on your virtual machine		Medium		New	Privilege escalation	Microsoft Defender for Ser...	Microsoft Defender for Clo...	Woodgrove-DC03
Attestation failed on your virtual machine		Medium		New	Privilege escalation	Microsoft Defender for Ser...	Microsoft Defender for Clo...	Woodgrove-DC03
Attestation failed on your virtual machine		Medium		New	Privilege escalation	Microsoft Defender for Ser...	Microsoft Defender for Clo...	Woodgrove-DC03
Attestation failed on your virtual machine		Medium		New	Privilege escalation	Microsoft Defender for Ser...	Microsoft Defender for Clo...	Woodgrove-DC03
Attestation failed on your virtual machine		Medium		New	Privilege escalation	Microsoft Defender for Ser...	Microsoft Defender for Clo...	Woodgrove-DC03
Attestation failed on your virtual machine		Medium		New	Privilege escalation	Microsoft Defender for Ser...	Microsoft Defender for Clo...	Woodgrove-DC03
Attestation failed on your virtual machine		Medium		New	Privilege escalation	Microsoft Defender for Ser...	Microsoft Defender for Clo...	Woodgrove-DC03
Attestation failed on your virtual machine		Medium		New	Privilege escalation	Microsoft Defender for Ser...	Microsoft Defender for Clo...	Woodgrove-DC03
Attestation failed on your virtual machine		Medium		New	Privilege escalation	Microsoft Defender for Ser...	Microsoft Defender for Clo...	Woodgrove-DC03
Attestation failed on your virtual machine		Medium		New	Privilege escalation	Microsoft Defender for Ser...	Microsoft Defender for Clo...	Woodgrove-DC03
Attestation failed on your virtual machine		Medium		New	Privilege escalation	Microsoft Defender for Ser...	Microsoft Defender for Clo...	Woodgrove-DC03

Home
Exposure management
Investigation & response
Incidents & alerts
Incidents
Alerts
Hunting
Actions & submissions
Partner catalog
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
Cloud infrastructure
Overview
Cases
SOC optimization
Reports

Incidents

Email notification

Most recent incidents and alerts

Incidents addressed by agent
Out of the total incidents it can handle
3/3 Last 30 days

Incidents involving AI detection
Copilot powered detections
0 Last 30 days

Attack disruptions
Automated actions stopped attacks
None Last 30 days

Queue reduction
Shorter and more comprehensive view
69% Last 30 days

Export | Copy list link | Refresh | 1 Week | 7 Incidents | Search for name or ID | Customize columns

Filter set: Save

Status: **Active, In Progress** | Incident assignment: **Any** | Priority score: **15-100** | Tags: **Any** | Entities: **Any** | Product names: **Microsoft Defender for Cloud** | Add filter | Reset all

Incident name	Incident Id	Priority score	Tags	Severity	Investigation state	Categories	Impacted assets	Active alerts
Malicious file uploaded to storage account - Auto...	251852	30		High		Lateral movement	woodgrovetaxes	1/1
Malicious file uploaded to storage account - Auto...	251427	31		High		Lateral movement	woodgrovetaxes	2/2
Multi-stage incident involving Initial access & Dis...	251408	63	Critical asset +1	High		Initial access, Execution, Di...	aks-agentpool-33582328-vmss000006	5/5
Multi-stage incident involving Privilege escalation...	249917	25	Full Remediation	Medium	2 investigation states	Privilege escalation, Discov...	Woodgrove-DC03.woodgrove.net Wo	127/128
A Jailbreak attempt was blocked on an AI agent (...	251851	32		Medium		Privilege escalation	dev-project	1/1
Suspected brute-force attack attempt involving m...	251608	15		Medium		Initial access	8 Accounts woodgrove-database-post	8/8
Multi-stage incident involving Initial access & Co...	239225	100	Agent	Medium		Initial access, Execution, Pe...	aks-agentpool-33582328-vmss000006	11/12

Home
Exposure management
Investigation & response
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps
Cloud infrastructure
Overview
Cases
SOC optimization
Reports
Learning hub
Trials
More resources
System
Data management

Cloud Infrastructure

Environment Filter : Off
Scope filter : Off

All Assets | VMs | Data | Containers | AI | API | DevOps | Identity | Serverless

Total **12583**
Critical assets **1545**

Defender coverage

Covered | Partially Covered | Not Covered

Refresh | Export

12583 items | Search | Customize columns

Selected filter set: None | Save

Asset label: Any | Organization: Any | Project: Any | Repository: Any | Add filter

Name	Asset type	Asset label	Environment	Criticality level	Defender coverage	Recommendations	Attack Paths	Risk factors	Cloud tags	Last refr
pkendar62bzbq	Object storage	Azure Storage acco...	Azure	Very high	Covered	11	18	Sensitive Data +2	CreatedD... +7	Nov 3, 2
woodgroverg99b2	Object storage	Azure Storage acco...	Azure	Very high	Covered	9	1	Sensitive Data +2	CreatedD... +2	Nov 1, 2
sensdata	Object storage	Azure Storage acco...	Azure	Very high	Covered	9	1	Sensitive Data +2	Solution: jumps...	Nov 3, 2
adfs02.woodgrove.net	Virtual machine	Azure Virtual Mach...	Azure	None	Covered	298	2	Vulnerabilities +1	CreatedD... +3	Nov 3, 2
addcreatortags	Serverless	Azure Function App	Azure	None	Covered	3	0	Exposure to the Int... +1	CreatedD... +5	Nov 3, 2
hello-contoso	-	Kubernetes contain...	Other	Very high	Covered	27	8	Exposure to the Int... +4	-	Oct 29,
hello-contoso	-	Kubernetes contain...	Other	Very high	Covered	27	12	Exposure to the Int... +4	-	Oct 31,
hello-contoso	-	Kubernetes contain...	Other	Very high	Covered	23	8	Exposure to the Int... +4	-	Oct 30,
hello-contoso	-	Kubernetes contain...	Other	Very high	Covered	23	0	Lateral Movement +3	-	Oct 28,
hello-contoso	-	Kubernetes contain...	Other	Very high	Covered	23	8	Exposure to the Int... +4	-	Oct 28,
hello-contoso	-	Kubernetes contain...	Other	Very high	Covered	16	0	Lateral Movement +3	-	Nov 2, 2
ai-service	-	Kubernetes contain...	Other	Very high	Covered	16	8	Exposure to the Int... +4	-	Nov 1, 2
woodgrove-srv1	Virtual machine	Azure Virtual Mach...	Azure	Very high	Covered	115	55	Lateral Movement ... +6	CreatedD... +7	Nov 3, 2
wgverifiedemployee	Object storage	Azure Storage acco...	Azure	Very high	Covered	9	1	Sensitive Data +2	CreatedD... +3	Nov 3, 2
wdingestionservice7ecc9e	Object storage	Azure Storage acco...	Azure	Very high	Covered	8	1	Sensitive Data +2	-	Nov 1, 2

Home
Exposure management
Investigation & response
Incidents & alerts
Incidents
Alerts
Hunting
Actions & submissions
Partner catalog
Threat intelligence
Assets
Devices
Identities
Applications
Cloud infrastructure
AI Agents
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps

Cloud Infrastructure

All Assets | VMs | Data | Containers | AI | API | DevOps | Identity | Serverless

- Kubernetes clusters
- Kubernetes namespaces
- Kubernetes workloads
- Containers
- Kubernetes service accounts
- Kubernetes services
- Kubernetes ingress
- Kubernetes node pools
- Registries and repositories
- Images

Total **10** | Critical assets **10**

Defender coverage: Covered | Partially Covered | Not Covered

Refresh | Export

Selected filter set: None | Save

CVE ID: Any | Cluster name: Any | Cluster type: Any | Environment type: Any | Criticali

Cluster name	Cluster type	Environment type	Kubernetes version
woodgrove-k8-mdc	AKS Cluster	Azure	1.31.6
woodgrove-aks-inventory-mdc	AKS Cluster	Azure	1.31.11
hello-cluster	GKE Cluster	GCP	1.33.5-gke.1162000
attack-path-deployment-3-cluster	GKE Cluster	GCP	1.33.5-gke.1162000
exciting-country-duck	EKS Cluster	AWS	1.31
zava-fargate-cluster	EKS Cluster	AWS	1.33
exciting-country-duck-us-east-2-648887187133	ARC Cluster	Azure	1.31.13-eks-113cf36
zava-fargate-cluster-us-east-2-648887187133	ARC Cluster	Azure	-

woodgrove-k8-mdc

Very high

Open asset page | View in map | Go hunt | Configure settings | ...

Criticality level
Very high

Last refreshed
Nov 3, 2025, 5:23 AM

Cloud security details

Attack paths
16

Risk factors
Lateral Movement +3

Configuration

Kubernetes version
1.31.6

Number of node pools
2

Node pool versions
1.31.6

Workload identity enabled
true

Risk based recommendations

54 recommendations

Critical: 0 | High: 38 | Medium: 12 | Low: 4

Environment details

Cluster cloud ID
/subscriptions/ab48f397-fc82-4634-aa52-62dd91b3ebaa/resourcegroups/woodgrove-mdc-rg/providers/microsoft.containerservice/managedclusters/woodgrove-k8-mdc

Security insights

Home
Exposure management
Investigation & response
Incidents & alerts
Incidents
Alerts
Hunting
Actions & submissions
Partner catalog
Threat intelligence
Assets
Devices
Identities
Applications
Cloud infrastructure
AI Agents
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps

woodgrove-k8-mdc

Very high | CreatedDate: 5/23/2025 7:26:20 PM | Created By: Woodgrove-DevOps-MI | CreatorUPN: ad92369c000a42feac6578cd8026763c | Owner: dilake | +5

View in map | Go hunt | Configure settings | View

Overview | Incidents and alerts | Security recommendations | Attack paths | Linked assets

Essentials

Asset ID
88c1f7d7f8704f3d8ac04fab5dea2aec

Native ID
/subscriptions/ab48f397-fc82-4634-aa52-62dd91b3ebaa/resourcegroups/woodgrove-mdc-rg/providers/microsoft.containerservice/managedclusters/woodgrove-k8-mdc

Asset type
Kubernetes cluster

Asset label
AKS Cluster

Environment
Azure

Subscription ID
ab48f397-fc82-4634-aa52-62dd91b3ebaa

Resource group
woodgrove-mdc-rg

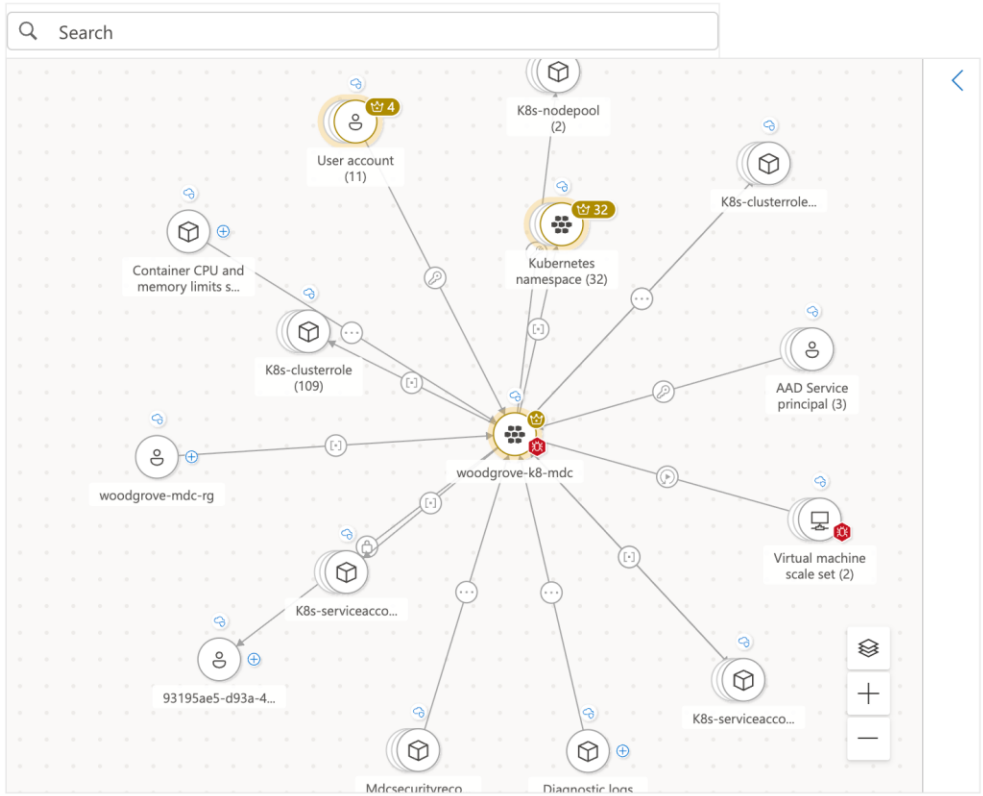
Region
eastus

Tags
CreatedDate: 5/23/2025 7:26:20 PM | +8

Criticality level
Very high

Last refreshed
Nov 3, 2025, 5:23 AM

Map



View in map

Threat protection

79 active alerts in 16 incidents

High (26) | Medium (42) | 2 more

Alert name	Severity	Status

View all incidents and alerts

Risk based recommendations

54 recommendations

Critical: 0 | High: 38 | Medium: 12 | 1 more

View recommendations

Home
Exposure management
Investigation & response
Threat intelligence
Assets
Microsoft Sentinel
Threat management
Content management
Configuration
Data lake exploration
Identities
Endpoints
Email & collaboration
Cloud apps
Cloud infrastructure
Cases
SOC optimization
Reports
Learning hub
Trials

Cloud Initiative: 49.2%

-39.8% • Your target score: 99% • Last updated: Nov 2, 2025 8:18:39 PM • 1547 Critical assets

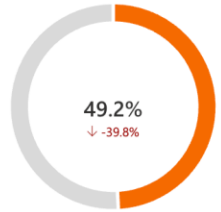
Last 7 days | Mark as favorite | Set target score | Environment Filter : Off | Scope filter

Overview | Security recommendations | Attack paths | History

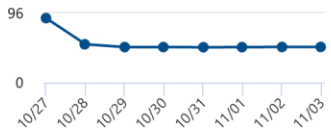
All
Misconfigurations
Vulnerabilities
Exposed secrets

Recommendations summary

Cloud secure score Moderate



Score history -39.8% Last 7 days



Recommendations by risk level

Critical
95

Critical | High | 2 more

How risk level is calculated?

Risk level
- Recommendation severity
- Asset risk factors
  - Defender CSPM

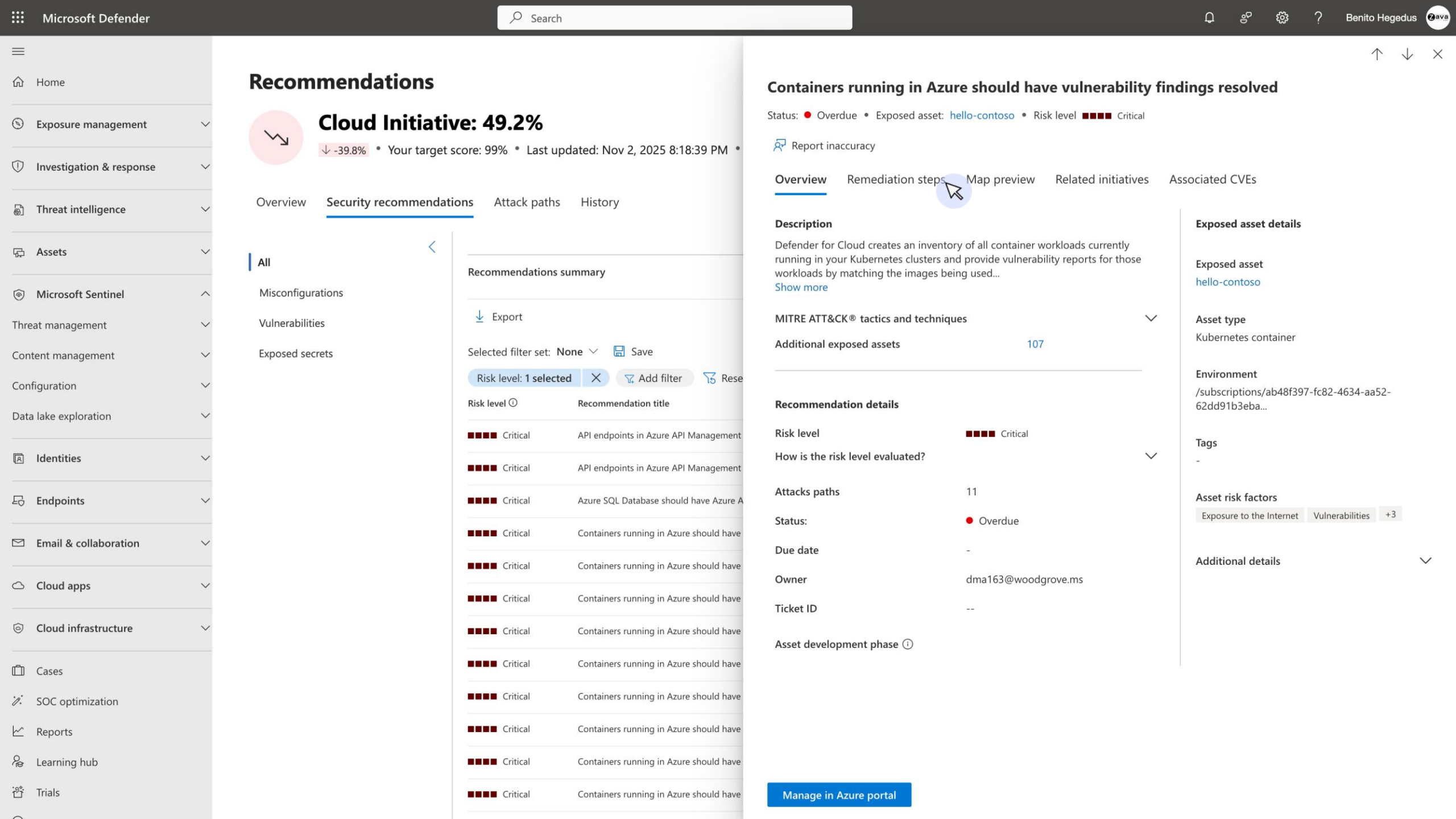
Learn about Defender CSPM trial

Export | 95 items | Search | Customize columns | View by: Recommendation per asset

Selected filter set: None | Save

Risk level: 1 selected | Add filter | Reset all

Risk level	Recommendation title		Exposed asset	Asset risk factors		Asset attack paths	Recommendation owner	Status
Critical	API endpoints in Azure API Management should be authenticated		createuser	Exposure to the Int...	+4	1	dilake	On tim
Critical	API endpoints in Azure API Management should be authenticated		createuser	Exposure to the Int...	+4	1	dilake	On tim
Critical	Azure SQL Database should have Azure Active Directory Only A...	Preview	woodgrove-database	Exposure to the Int...	+4	1	naha84@woodgrove.ms	Overdu
Critical	Containers running in Azure should have vulnerability findings ...	Preview	hello-contoso	Exposure to the Int...	+4	11	dma163@woodgrove.ms	Overdu
Critical	Containers running in Azure should have vulnerability findings ...	Preview	ai-service	Exposure to the Int...	+3	10	naha84@woodgrove.ms	Overdu
Critical	Containers running in Azure should have vulnerability findings ...	Preview	hello-contoso	Lateral Movement	+3	0	baka58@woodgrove.ms	Overdu
Critical	Containers running in Azure should have vulnerability findings ...	Preview	hello-contoso	Lateral Movement	+3	0	dma163@woodgrove.ms	Overdu


Microsoft Defender
Search
Benito Hegedus
Home
Exposure management
Investigation & response
Threat intelligence
Assets
Microsoft Sentinel
Threat management
Content management
Configuration
Data lake exploration
Identities
Endpoints
Email & collaboration
Cloud apps
Cloud infrastructure
Cases
SOC optimization
Reports
Learning hub
Trials
Recommendations
Cloud Initiative: 49.2%
-39.8% • Your target score: 99% • Last updated: Nov 2, 2025 8:18:39 PM •
Overview
Security recommendations
Attack paths
History
All
Misconfigurations
Vulnerabilities
Exposed secrets
Recommendations summary
Export
Selected filter set: None
Save
Risk level: 1 selected
Add filter
Rese
Risk level
Recommendation title
Critical API endpoints in Azure API Management
Critical API endpoints in Azure API Management
Critical Azure SQL Database should have Azure A
Critical Containers running in Azure should have
Critical Containers running in Azure should have
Critical Containers running in Azure should have
Critical Containers running in Azure should have
Critical Containers running in Azure should have
Critical Containers running in Azure should have
Critical Containers running in Azure should have
Critical Containers running in Azure should have
Critical Containers running in Azure should have
Critical Containers running in Azure should have
Containers running in Azure should have vulnerability findings resolved
Status: Overdue • Exposed asset: hello-contoso • Risk level Critical
Report inaccuracy
Overview
Remediation steps
Map preview
Related initiatives
Associated CVEs
Description
Defender for Cloud creates an inventory of all container workloads currently running in your Kubernetes clusters and provide vulnerability reports for those workloads by matching the images being used...
Show more
MITRE ATT&CK® tactics and techniques
Additional exposed assets 107
Recommendation details
Risk level Critical
How is the risk level evaluated?
Attacks paths 11
Status: Overdue
Due date -
Owner dma163@woodgrove.ms
Ticket ID --
Asset development phase
Exposed asset details
Exposed asset
hello-contoso
Asset type
Kubernetes container
Environment
/subscriptions/ab48f397-fc82-4634-aa52-62dd91b3eba...
Tags
-
Asset risk factors
Exposure to the Internet
Vulnerabilities
+3
Additional details
Manage in Azure portal

Home
Exposure management
Overview
Initiatives
Recommendations
Vulnerability management
Overview
Vulnerabilities
Inventories
Remediation
Baseline assessments
Attack surface
Secure score
Data connectors
Investigation & response
Threat intelligence
Assets
Microsoft Sentinel
Identities
Endpoints
Email & collaboration
Cloud apps

Vulnerability management

Email notifications settings
Scope filter : Off

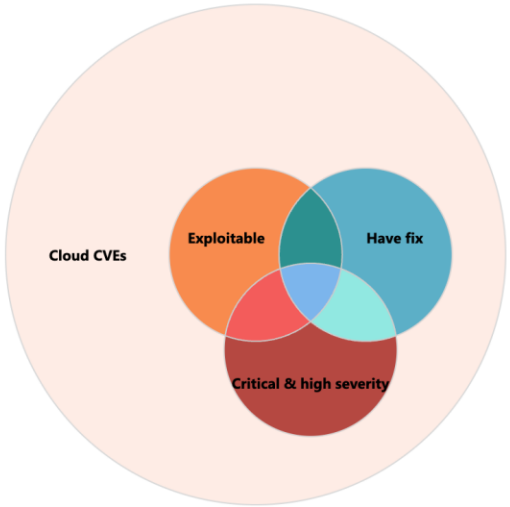
This dashboard provides a comprehensive summary of the vulnerability risks within your organization, covering both cloud and endpoint environments.

Scope filtering for device groups is only applied to the Endpoints tab and cloud scopes only to the Cloud tab.

Endpoint | Cloud

Vulnerabilities

Cloud vulnerabilities insights



View all vulnerabilities

Top cloud CVEs

Name	Severity	CVSS	Exposed assets	Exploits type
CVE-2025-10230	Critical	10	5	Remote
CVE-2024-12718	Critical	10	2	Remote
CVE-2025-62168	Critical	10	1	Remote

View all vulnerabilities

Vulnerabilities over time

Investigation & response
Threat intelligence
Assets
Microsoft Sentinel
Endpoints
Email & collaboration
Cloud apps
Cloud infrastructure
Cases
SOC optimization
Reports
Learning hub
Trials
More resources
System
Audit
Data management
Permissions
Health
Settings
Customize navigation

Learn more | Workload settings

Permissions and roles

Roles define what users can see and do in Microsoft Defender XDR. Assign only the permissions they need to stay secure.
Scopes help organize and control scoping groups. Use them to fine-tune access and limit permissions as needed.

Roles | Scopes

Export | Create cloud scope | Edit | Delete

2 items | Search

Scope name	Description	Environments	Assigned to	Last updated	Created by
Scope_UK		Azure Subscriptions	1 roles	Sep 3, 2025 10:28 AM	Rayan Daher
Scope_US		Azure Subscriptions	1 roles	Sep 3, 2025 10:29 AM	Qizhou(Ale...

Project Milestones and Deliverables

Launching at Ignite

Phase 1
Expanding cloud security posture capabilities in the Defender portal

- Posture capabilities can now be found in Exposure management

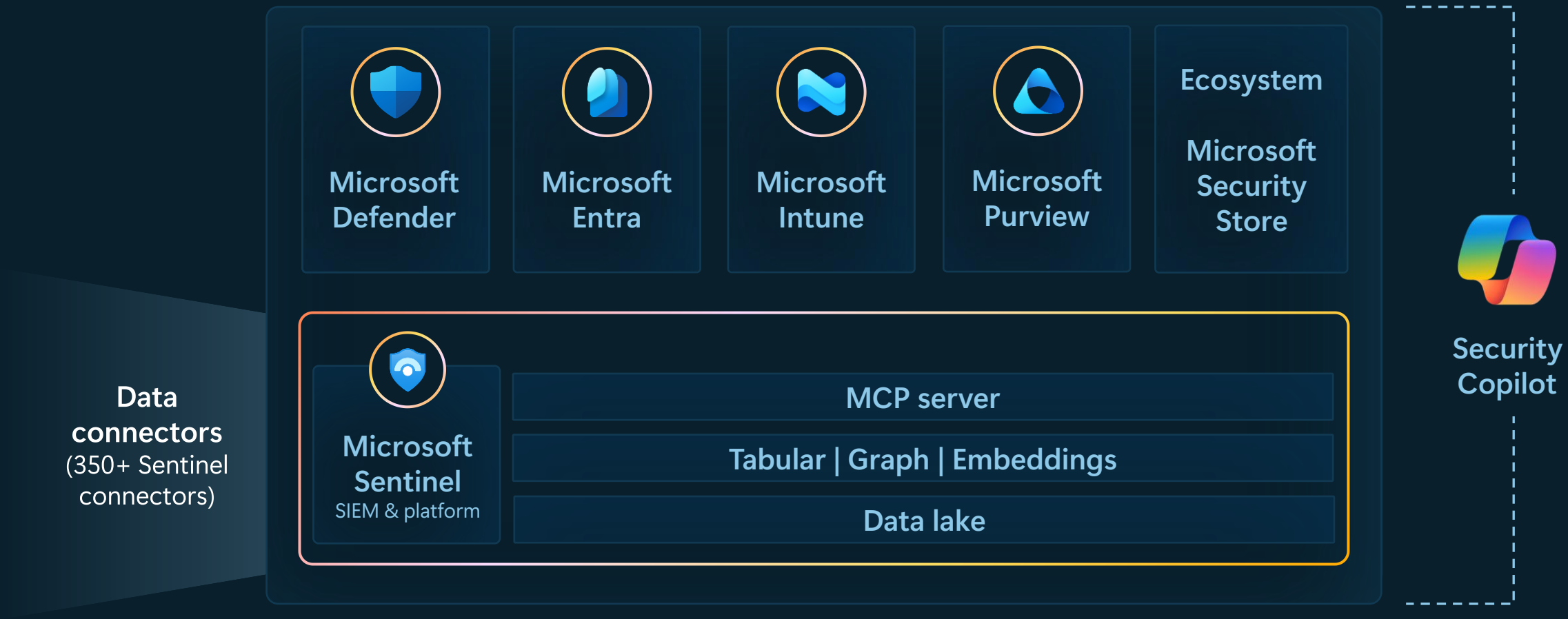
1. Overview (CNAPP) dashboard
2. Unified cloud asset inventory
3. Cloud vulnerabilities
4. Enhanced attack paths
5. Risk-based recommendations
6. Risk-based secure score
7. Granular RBAC

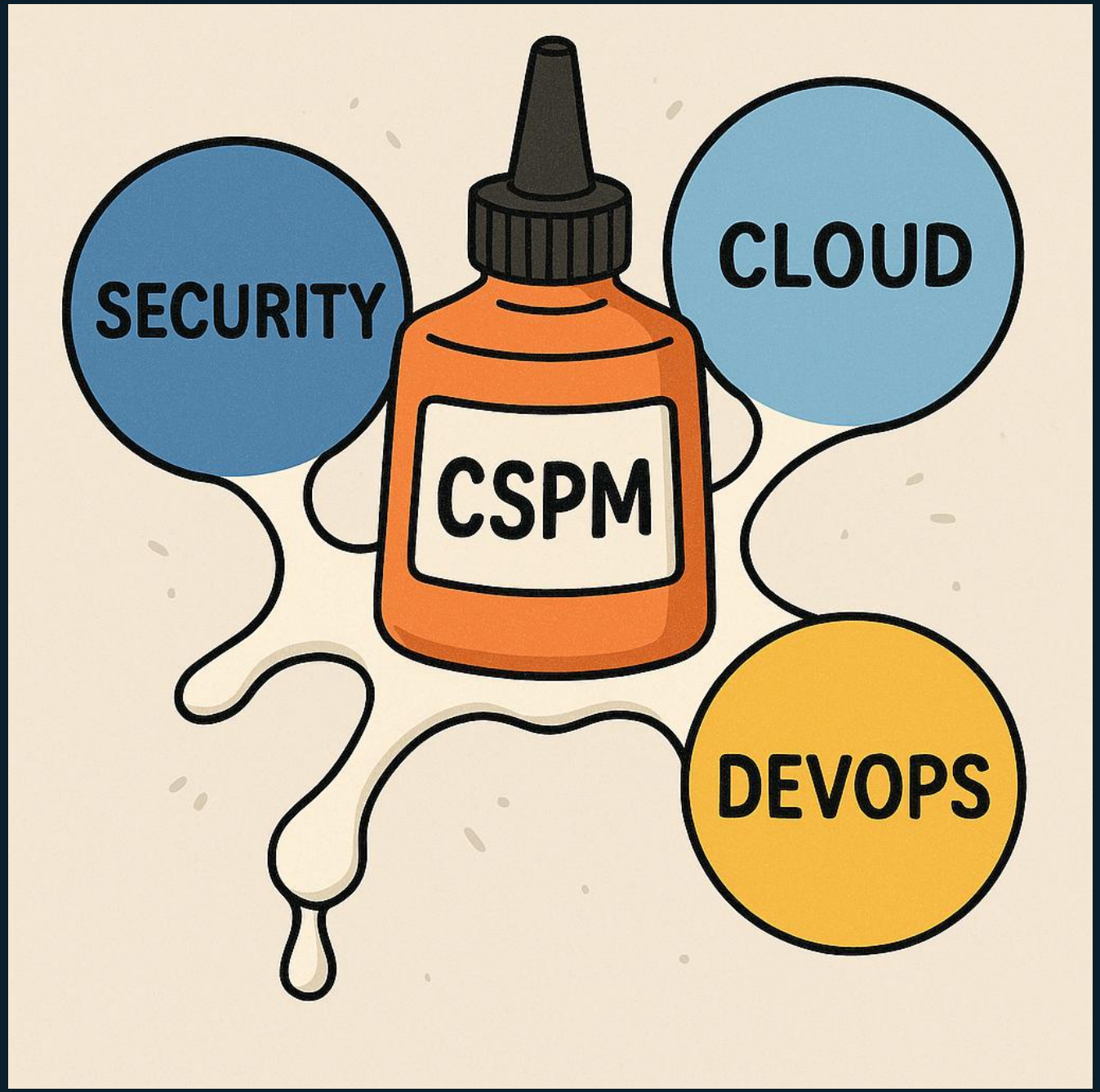
Phase 2
Expanding cloud security configuration & management capabilities

- Onboarding & Enablement
- Control/policy across all cloud sensors
- Go beyond the tenant boundary

1. Improved onboarding experience
2. Granular product settings
3. Security policies from posture to runtime
4. Multi-tenancy support
5. APIs and extensibility options
6. Automatic cloud risk reduction
7. Automatic cloud attack disruption

AI-first end-to-end security platform




SECURITY
CLOUD
CSPM
DEVOPS


RISKS
• Data Breaches
• Downtime
• Misconfigurations
• Access Control
SECURITY
DEVOPS
CLOUD
SECURITY
SECURITY
DEVOPS
CLOUD

Thank you!

Feedback