



EXPERTS LIVE

KENYA

26 TH JULY 2024
NAIROBI, KENYA



Breaking Security Silos Across Your Multi- Cloud Landscape with Microsoft Defender & Microsoft Sentinel

Jacklyne Mbuthia,
Cloud Security Engineer, Cyber Guard Africa

Agenda

- Rise of Cloud Adoption & Multi-Cloud Adoption
- Challenges Facing Multi-Cloud Adoption
- Silos & BlindSpots in Multi-Cloud Challenges Posed by Security Silos
- Strategies to Break Down Security Silos
- Tools and Technologies



ADOPTION OF MULTI-CLOUD

o o o o

The rise of cloud computing marked the beginning of a new era of innovation, enabling organizations to quickly scale and seize new opportunities. Nowadays, multi-cloud environments have become the standard approach for conducting business.

Approximately 86% of organizations have already adopted a multi cloud approach thanks to its benefits

ADOPTION OF MULTI-CLOUD

A multi-cloud environment refers to the use of multiple cloud computing services from different providers within a single architecture.

Why are businesses distributing workloads across multiple clouds?

- Avoiding Vendor Lock-In
- Optimizing Costs
- Enhancing Resilience and Reliability
- Leveraging Best-of-Breed Services
- Innovation and Agility
- Flexibility and Scalability
- Risk Mitigation



UNDERSTANDING SILOS IN MULTI-CLOUD SECURITY

In multi-cloud environments, silos refer to isolated and disjointed security practices and controls across different cloud platforms. These silos can occur when each cloud provider's security solutions and policies operate independently of others, creating gaps and inefficiencies in the overall security posture.

Examples of security silos:

- Fragmented Monitoring and Logging
- Inconsistent Incident Response Procedures
- Diverse Security Tools and Technologies
- Isolated Data Protection Measures
- Separate Security Policies

SECURITY SILOS IN MULTI-CLOUD

CHALLENGES

- Identity & Access management
- Complexity
- Inconsistent Security Policies
- Inefficient Threat Response
- Products/technologies to leverage
- Fragmented Visibility
- Securing cloud-native applications and infrastructure throughout the full lifecycle.

VS

STRATEGIES

- Cross-Cloud IAM Solutions
- Unified Security Management
- Consistent Security Policies
- Integrated Monitoring and Logging
- Unified Threat Detection and Response
- Leveraging Multi-Cloud Management Platforms
- Employee Training Programs

TOOLS AND TECHNOLOGIES

FACTORS TO CONSIDER

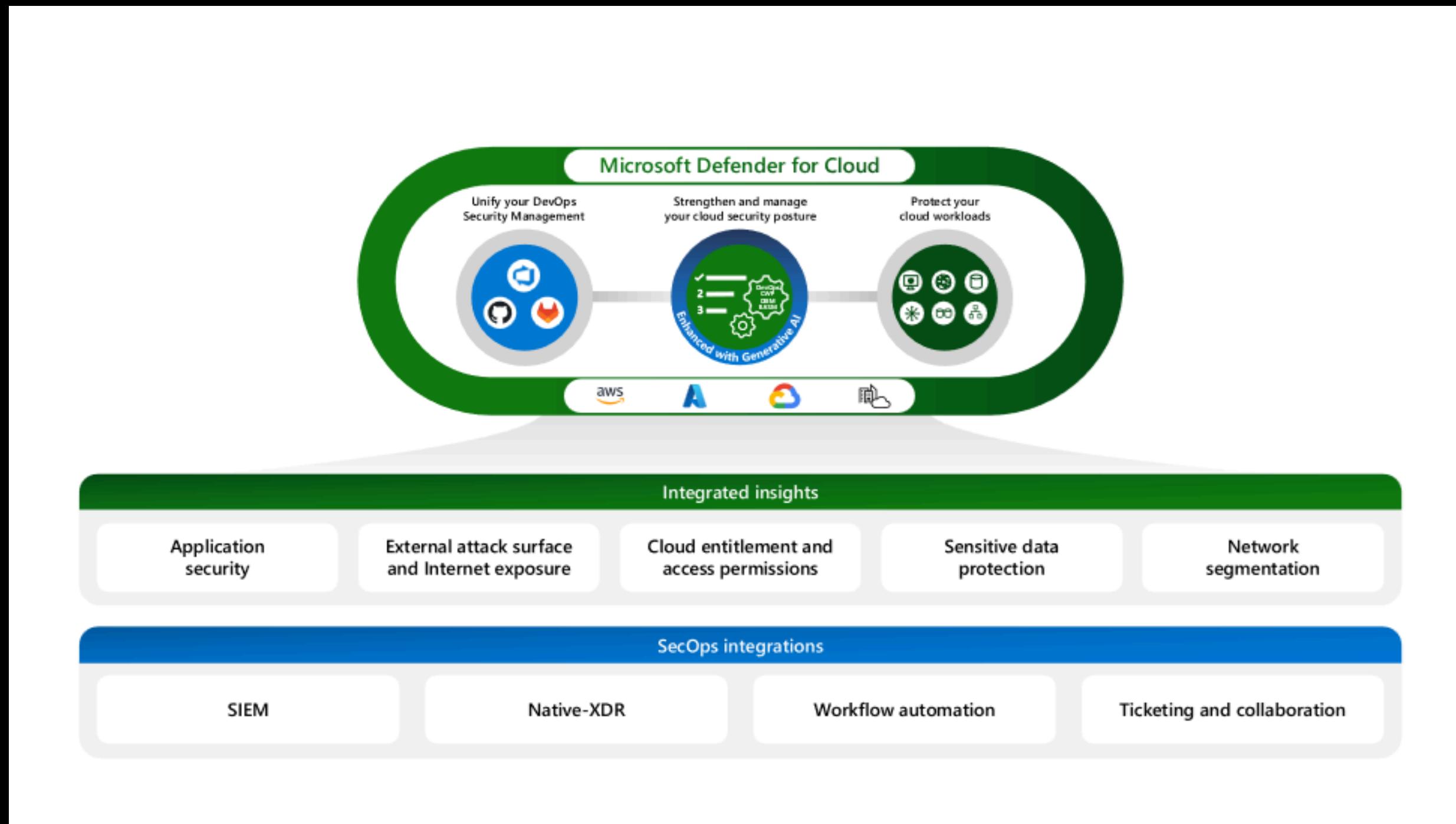
- Integration capabilities
- Scalability
- Automation & Orchestration
- Flexibility & Customization
- User friendliness
- Value for money

VS

TOOLS TO LEVERAGE

- Security incidents and events managements(SIEM)
- Cloud-native application platform protection (CNAPP)
- Cloud security posture management (CSPM)
- Multi-Cloud Management Platforms

MICROSOFT DEFENDER as MICROSOFT CNAPP SOLUTION



MICROSOFT DEFENDER as MICROSOFT CSPM SOLUTION

Microsoft Defender for Cloud | Overview

Showing 2 subscriptions

Search Subscriptions What's new

General

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

Azure subscriptions: 2

AWS accounts: 9

GCP projects: 10

Assessed resources: 34065

Attack paths: 114

Security alerts: 681

Security posture

- Critical recommendations: 212
- Attack paths: 114
- Overdue recommendations: 0/0

Environment risk and secure score

All recommendations by risk (20508): Critical 212, High 299, Medium 1086, Low 18894, Not evaluated 17

Total secure score: 53% (Azure 57%, AWS 19%, GCP 42%)

[Explore your security posture >](#)

Regulatory compliance

Microsoft cloud security benchmark: 10 of 64 controls passed

Lowest compliance standards by controls passed

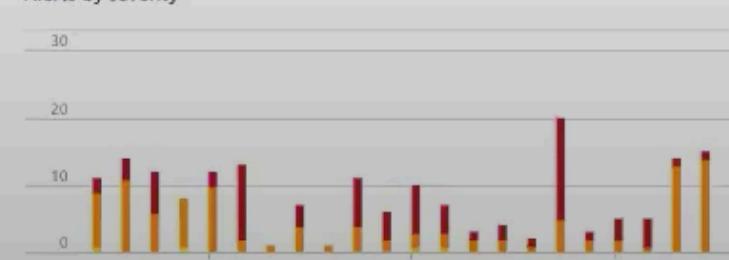
- AWS Well Architected Framework (Preview): 0/2
- AWS GDPR (Preview): 0/4
- AWS California Consumer Privacy Act (CCPA) (Preview): 0/1

[Improve your compliance >](#)

Workload protections

Resource coverage: 99% (For full protection, enable 3 resource plans)

Alerts by severity



Inventory

Unmonitored VMs: 59 (To better protect your organization, we recommend installing agents)

Total Resources: 34065

Unhealthy (13911), Healthy (19857), Not applicable (297)

New threat protection for AI workloads (preview)

Protect your GenAI workloads using Azure OpenAI Service. Integrated with Azure AI Content Safety prompt shields and Microsoft threat intelligence, threat protection for AI workload detects attacks on your AI workloads and provides evidence-based security alerts, such as jailbreak, credentials theft and more.

[Apply here to participate | Learn more](#)

Posture and threat detection

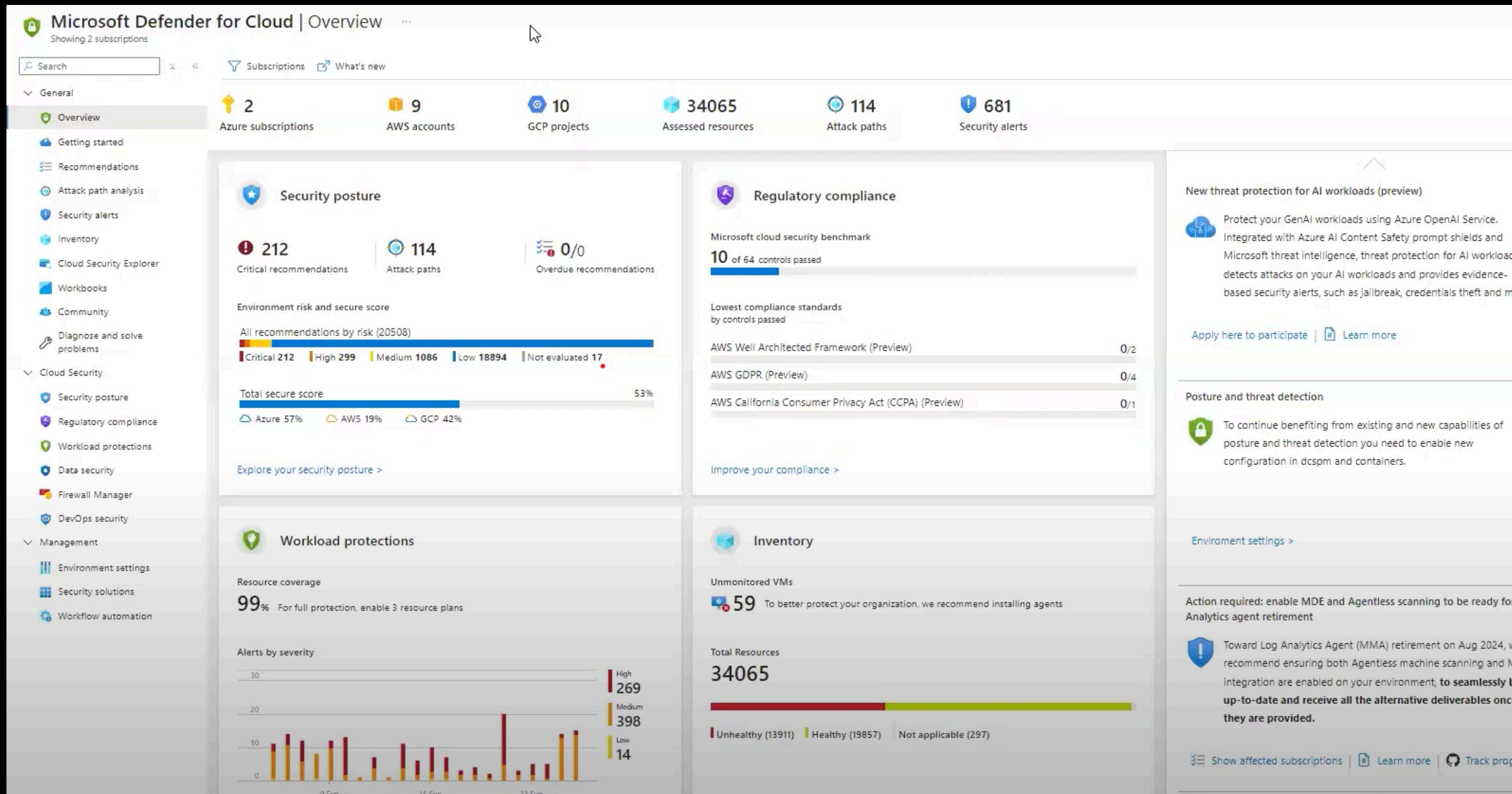
To continue benefiting from existing and new capabilities of posture and threat detection you need to enable new configuration in dcspm and containers.

Environment settings >

Action required: enable MDE and Agentless scanning to be ready for Analytics agent retirement

Toward Log Analytics Agent (MMA) retirement on Aug 2024, we recommend ensuring both Agentless machine scanning and MMA integration are enabled on your environment, to seamlessly be up-to-date and receive all the alternative deliverables once they are provided.

Show affected subscriptions | Learn more | Track progress



Microsoft Defender for Cloud | Attack path analysis

Showing 2 subscriptions

Search Learn more Guides & Feedback Open query Download CSV report

You are seeing partial data in certain environments as Defender CSPM is not enabled. Enable Defender CSPM on all environments to get full data visibility. [Learn more >](#)

General

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

Attack path analysis

114 Total attack paths 166 Affected resources 24 Active recommendations

Risk level

Critical (55)	High (42)	Medium (17)	Low (0)
---------------	-----------	-------------	---------

Search Add Group by: None

Risk level	Title	Entry point	Target	Enviro...	Risk F...	Affected resou...
Critical	Critical Internet exposed and publicly accessible Azure blob storage container with sensitive data	vms	vms	Azure	Critical re	2
Critical	Critical Internet exposed and publicly accessible Azure blob storage container with sensitive data	file	file	Azure	Critical re	2
Critical	Critical Internet exposed and publicly accessible Azure blob storage container with sensitive data	uploaded	uploaded	Azure	Critical re	2
Critical	Critical Internet exposed and publicly accessible Azure blob storage container with sensitive data	xdrsiem	xdrsiem	Azure	Critical re	2
Critical	Critical Internet exposed and publicly accessible Azure blob storage container with sensitive data	contosohotels123	contosohotels123	Azure	Critical re	2
Critical	Critical Internet exposed and publicly accessible Azure blob storage container with sensitive data	contosovisitorsdataarchive	contosovisitorsdataarc	Azure	Critical re	2
Critical	Critical Internet exposed and publicly accessible Azure blob storage container with sensitive data	contosohrstorage1con	contosohrstorage1list	Azure	Critical re	2
Critical	Critical Internet exposed and publicly accessible Azure blob storage container with sensitive data	contosohrstorage1list2con	contosohrstorage1list	Azure	Critical re	2
Critical	Critical Internet exposed and publicly accessible Azure blob storage container with sensitive data	xdrsentinel	xdrsentinel	Azure	Critical re	2
Critical	Critical Publicly accessible GCP storage bucket with sensitive data	contosogcp-standard-sensitive-public	contosogcp-standardarc	GCP	Critical re	1
Critical	Critical AWS RDS DB with excessive internet exposure and basic authentication (local user/password) and sensitive data	backofficedb2	backofficedb2	AWS	Critical re	1
Critical	Critical AWS RDS DB with excessive internet exposure and basic authentication (local user/password) and sensitive data	backoffice-instance-1	backoffice-instance-1	AWS	Critical re	1
Critical	Critical AWS RDS DB with excessive internet exposure and basic authentication (local user/password) and sensitive data	backofficedb1-instance-1	backofficedb1-instan	AWS	Critical re	1
Critical	Internet exposed EC2 instance has high severity vulnerabilities and read permission to a KMS	aws-ec2-instance (i-0148e2702d5e19484)	1ebbcd2a-1111-473c	AWS	Internet	5
Critical	Internet exposed EC2 instance has high severity vulnerabilities and read permission to a KMS	aws-ec2-instance (i-0148e2702d5e19484)	8dd41815-062d-43d	AWS	Internet	5
Critical	Internet exposed EC2 instance has high severity vulnerabilities and high permission to an account	aws-ec2-instance (i-0148e2702d5e19484)	735530032416	AWS	Internet	4
Critical	Internet exposed EC2 instance has high severity vulnerabilities and read permission to a KMS	aws-ec2-instance (i-02285a1b9773aa18b)	8dd41815-062d-43d	AWS	Internet	5
Critical	Internet exposed EC2 instance has high severity vulnerabilities and read permission to a KMS	aws-ec2-instance (i-02285a1b9773aa18b)	1ebbcd2a-1111-473c	AWS	Internet	5

Attack Path analysis is a feature on Defender that allows companies to be able to identify risk in their environment, prioritise how to mitigate them and it's how to refactor it

Internet exposed Azure VM with high severity vulnerabilities allows lateral movement to Critical Azure storage account with sensitive data

i Defender CSPM for GCP was released to General Availability! [Learn more >](#)

Critical 2 Active Recommendations Azure

Description

An Azure Virtual Machine is reachable from the internet and has high severity vulnerabilities allowing remote code execution. The Azure VM can authenticate as an Azure Managed Identity. The managed identity has permissions to read data from an Azure st... [Show more](#)

Attack story

1. Attacker can exploit the vulnerabilities via the internet and gain control on the VM
2. Attacker can authenticate as the managed identity
3. Attacker can use the identity to read data from the storage account
4. Attacker can read s...

[Show more](#)

Resource types

- Virtual machine (1)
- Managed identity (1)
- Storage account (1)

[Show more](#)

Risk factors

CRITICAL RESOURCE INTERNET EXPOSURE VULNERABILITIES LATERAL MOVEMENT

◀ ▶

MITRE ATT&CK® tactics



Collection [Read more](#)

Code Repositories (T1213/003)

[Show more](#)



Attack Path analysis allows you to analyse at a granular level

Internet exposed Azure VM with high severity vulnerabilities allows lateral movement to Critical Azure storage account with sensitive data

Defender CSPM for GCP was released to General Availability! [Learn more >](#)

Critical 2 Active Recommendations Azure

Attack path Remediation

Resolve the following security recommendations to mitigate the attack path:

Recommendations Unhealthy resources

Machines should have vulnerability findings resolved 1 of 1 Virtual machine

Permissions of inactive identities in your Azure subscription should be revoked 1 of 1 microsoft.security/pricings/securityentitydata

Permissions of inactive identities in your Azure subscription should be revoked

> Additional recommendations

Description

An Azure Virtual Machine is reachable from the internet and has high severity vulnerabilities allowing remote code execution. The Azure VM can authenticate as an Azure Managed Identity. The managed identity has permissions to read data from an Azure st... [Show more](#)

Attack story

1. Attacker can exploit the vulnerabilities via the internet and gain control on the VM
2. Attacker can authenticate as the managed identity
3. Attacker can use the identity to read data from the storage account
4. Attacker can read s...
[Show more](#)

Resource types

Virtual machine (1)
Managed identity (1)
Storage account (1)
[Show more](#)

Risk factors

CRITICAL RESOURCE INTERNET EXPOSURE VULNERABILITIES LATERAL MOVEMENT

MITRE ATT&CK® tactics

Collection [Read more](#)
Code Repositories (T1213/003)

Show more

Actionable recommendations are provided for issues identified

Microsoft Defender for Cloud | Environment settings

Showing subscription 'Azure subscription 1'

Search Add environment Refresh Create custom recommendation Guides & Feedback Cost estimator Defender Plans Coverage

Security alerts Inventory Cloud Security Explorer Workbooks Community Diagnose and solve problems

Cloud Security

- Security posture
- Regulatory compliance
- Workload protections
- Data security
- Firewall Manager
- DevOps security

Management

- Environment settings**
- Security solutions
- Workflow automation

Amazon Web Services Google Cloud Platform GitHub Azure DevOps GitLab

Data sensitivity Set the sensitivity of your organization's resources based on info type or sensitivity labels

Direct onboarding Onboard non-Azure servers directly with Defender for Endpoint

ServiceNow integration Connect your environment to ServiceNow ITSM for bi-directional sync

Resource criticality (preview) Define your critical assets (resources), to better protect your crown jewels

Containers drift policy (preview) Set your scope and conditions for applying drift detection

1 Azure subscriptions 0 AWS accounts 0 GCP projects 0 GitHub connectors 0 AzureDevOps connectors 0 GitLab connectors

0 Total issues

GCP Projects 0 AWS Accounts 0 AzureDevOps ADO 0

Search by name Environments == All Standards == All Coverage == All Connectivity status == All

Expand all

Name ↑ Total resources ↑ Connectivity status Defender coverage ↑

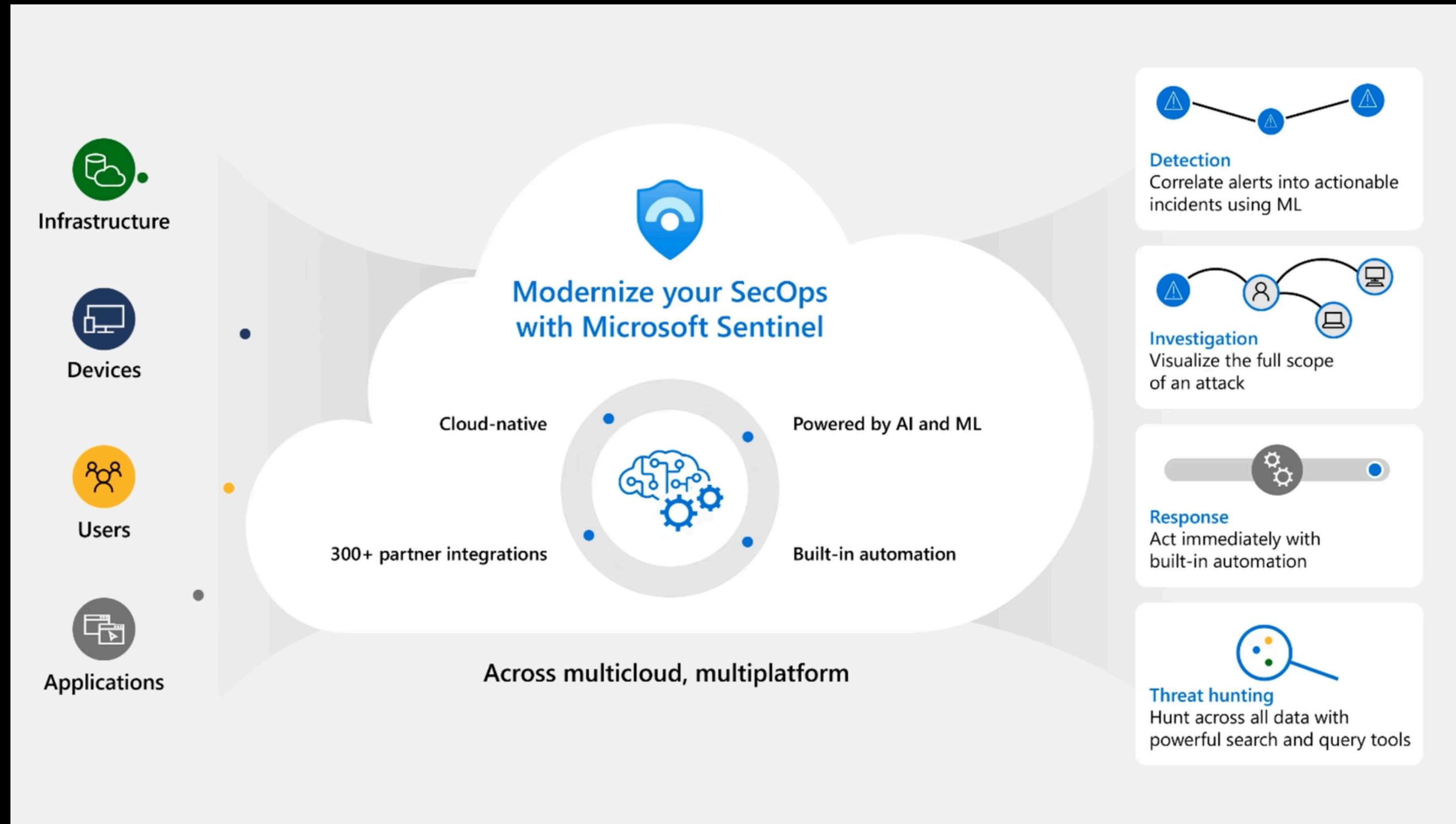
Azure

11/12 plans

The screenshot shows the Microsoft Defender for Cloud Environment settings page. The left sidebar has 'Environment settings' selected. The main area displays connectivity status for various platforms: Azure subscriptions (1), AWS accounts (0), GCP projects (0), GitHub connectors (0), AzureDevOps connectors (0), and GitLab connectors (0). It also shows 0 total issues and connectivity status filters. A modal for 'Data sensitivity' is open.

Adding CSPs and development platforms to Microsoft Defender

MICROSOFT SIEM SOLUTION - MICROSOFT SENTINEL



Microsoft Sentinel | Data connectors

Selected workspace: 'expertsivelaw'

Search Refresh Guides & Feedback

General

- Overview
- Logs
- News & guides
- Search

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)
- SOC optimization

Content management

- Content hub
- Repositories (Preview)

6 Connectors 0 Connected More content at Content hub

Search by name or provider Providers : All Data Types : All Status

Status	Connector name ↑
	Amazon Web Services S3 Amazon
	Azure Activity Microsoft
	Microsoft Entra ID Microsoft
	Subscription-based Microsoft Defender for Cloud (Legacy) Microsoft
	Threat intelligence - TAXII Microsoft
	Threat Intelligence Platforms - BEING DEPRECATED (Preview) Microsoft

Sentinel uses data connectors to enable you to integrate to your environments

Microsoft Sentinel | Data connectors

Selected workspace: 'expertslivelaw'

Search Refresh Guides & Feedback

6 Connectors 0 Connected More content at Content hub

Search by name or provider Providers : All Data Types : All Status

Status Connector name ↑

aws	Amazon Web Services S3
Status	Amazon Provider
Last Log Received	
Description	
This connector allows you to ingest AWS service logs, collected in AWS S3 buckets, to Microsoft Sentinel. The currently supported data types are:	
<ul style="list-style-type: none">AWS CloudTrailVPC Flow LogsAWS GuardDutyAWSCloudWatch	
For more information, see the Microsoft Sentinel documentation .	
Last data received	
Open connector page	

Amazon Web Services S3
Amazon

Azure Activity
Microsoft

Microsoft Entra ID
Microsoft

Subscription-based Microsoft Defender for Cloud (Legacy)
Microsoft

Threat intelligence - TAXII
Microsoft

Threat Intelligence Platforms - BEING DEPRECATED (Preview)

General

- Overview
- Logs
- News & guides
- Search

Threat management

- Incidents
- Workbooks
- Hunting
- Notebooks
- Entity behavior
- Threat intelligence
- MITRE ATT&CK (Preview)
- SOC optimization

Content management

- Content hub

Identify what the connector will capture to plan out your environment

Conclusion

Multi cloud security is growing,
we have to grow in how we are
approaching security as well !



Session Feedback

Session Track: Security

Session Name: Breaking Security Silos Across Your
Multi- Cloud Landscape with Microsoft Defender &
Microsoft Sentinel

Experts Live KE 2024 Attendee
Feedback



THANK YOU

Speaker Name: Jacklyne Mbuthia

Speaker Title: Senior Cloud Security Engineer,
Cyber Guard Africa

Speaker Social Media/links:
X: @bugsandbags_



THANK YOU TO OUR SPONSORS!

