

Securing Multi-Clouds Part 2

Azure Arc
Microsoft Defender for Cloud
Microsoft Sentinel

Poll - <https://aka.ms/SecuringMVC2-Poll>



Meet the Team



Cassandra Browning
Cloud Solutions Architect
Security / Azure



Richard Diver
Technical Business Strategy
Manager



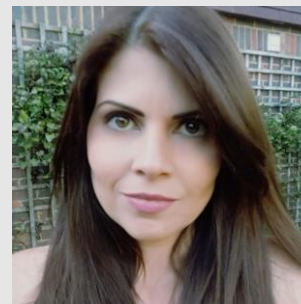
Nick Lines
Security Product
Marketing Manager



Darren Small
Cloud Solutions Architect
Azure Infrastructure



Ally Turnbull
Cloud Solutions Architect
Security / Compliance



Luciana Blanchard
Cloud Solutions Architect
Identity



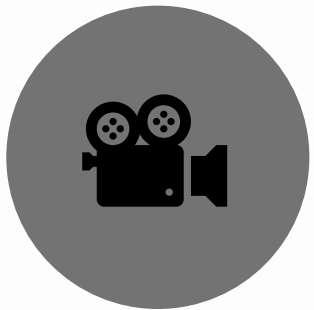
Housekeeping



There will be breaks & speaker changes throughout



This is a one-way speaker to attendees audio, so please ask any questions in the Q&A



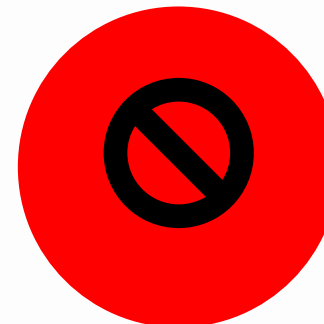
This will be recorded and links sent to you (*current delay on recordings being sent*)



Feedback – aka.ms/SecuringMVC2-Feedback



These Resources will be shared with you (to share with others at your company)



All content is under your partnership NDA

Today's Agenda (GMT)

14:00 - Intro and Housekeeping – Cassandra Browning

14:05 - Opening Keynote – Nick Lines

14:15 - Azure Arc – Darren Small

15:20 - Break 10 mins

15:30 – Microsoft Defender for Cloud – Cassandra Browning

16:40 – Break 10 mins

16:50 – Microsoft Sentinel - Ally Turnbull

17:20 – Wrap Up + Live Q&A

17:30 – Event ends



In case you missed part 1 MVC – Identity



- **On-Demand Recording** – coming soon
- **Slides & Labs** – <https://aka.ms/SecuringMVC-Repo>

Keynote

Nick Lines
Security PMM





BUSINESSES AND USERS
ARE GOING TO
EMBRACE TECHNOLOGY
ONLY IF THEY CAN
TRUST IT.

SATYA NADELLA



For the eighth time, the American tech conglomerate has been regarded as a reputable brand.

Microsoft, which is worth more than US\$1 trillion, is the only software company listed in the top 10 for 2021.

The successful business scored 77.1 overall, giving it a Strong Reputation.



Microsoft on the Front Lines

Protecting

650K organizations
in 120 countries

Analyzing

24T threat signals
every day

Tracking

40+ nation-state actors &
140+ threat groups

Blocked

32B email threats
last year



Microsoft Security

Comprehensive visibility, automation, and intelligence



Protect
everything



Simplify
the complex



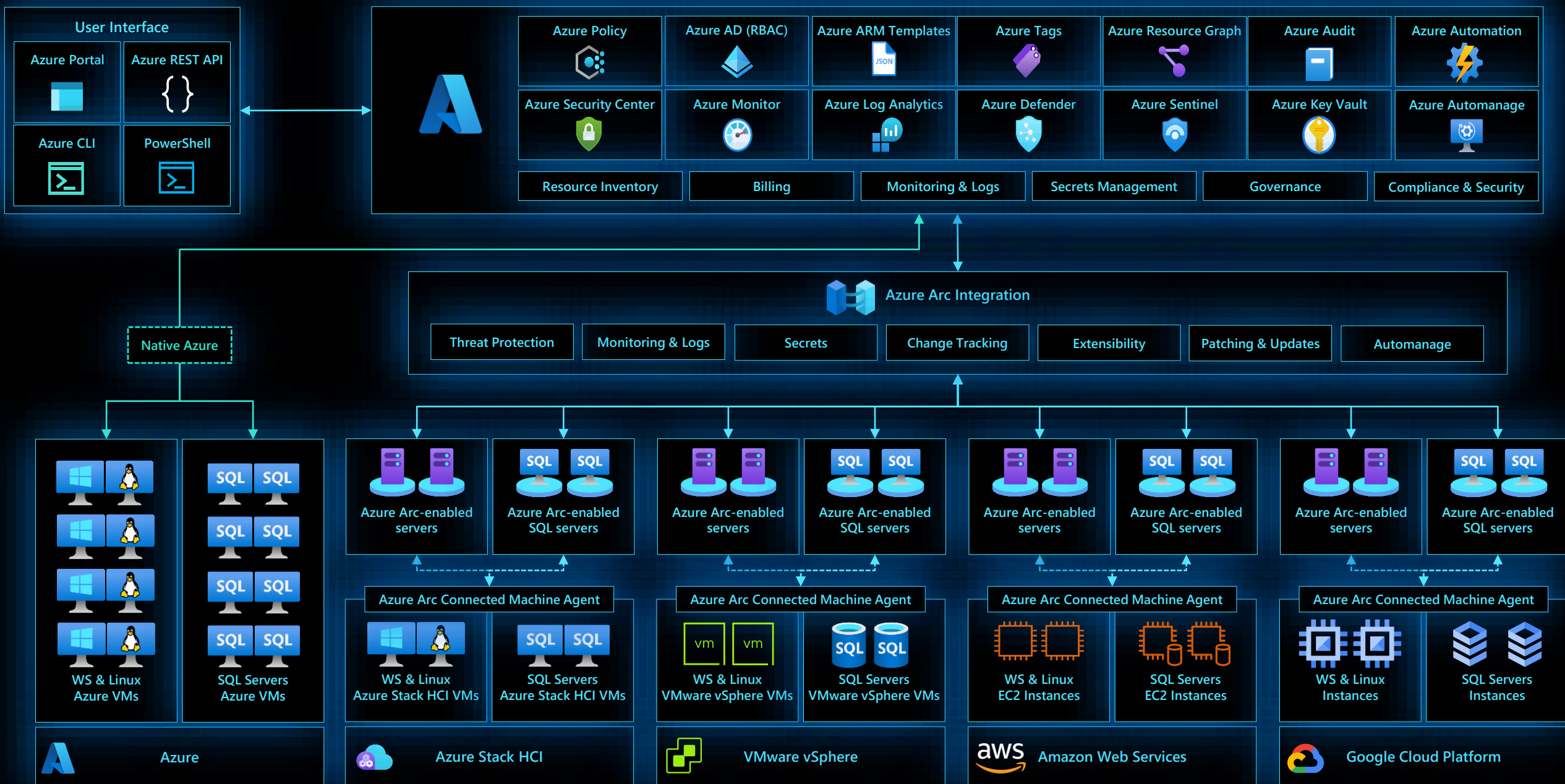
Catch
what others miss



Grow
your future

Azure Arc-enabled servers & Azure Arc-enabled SQL server

On-premises and multi-cloud integration

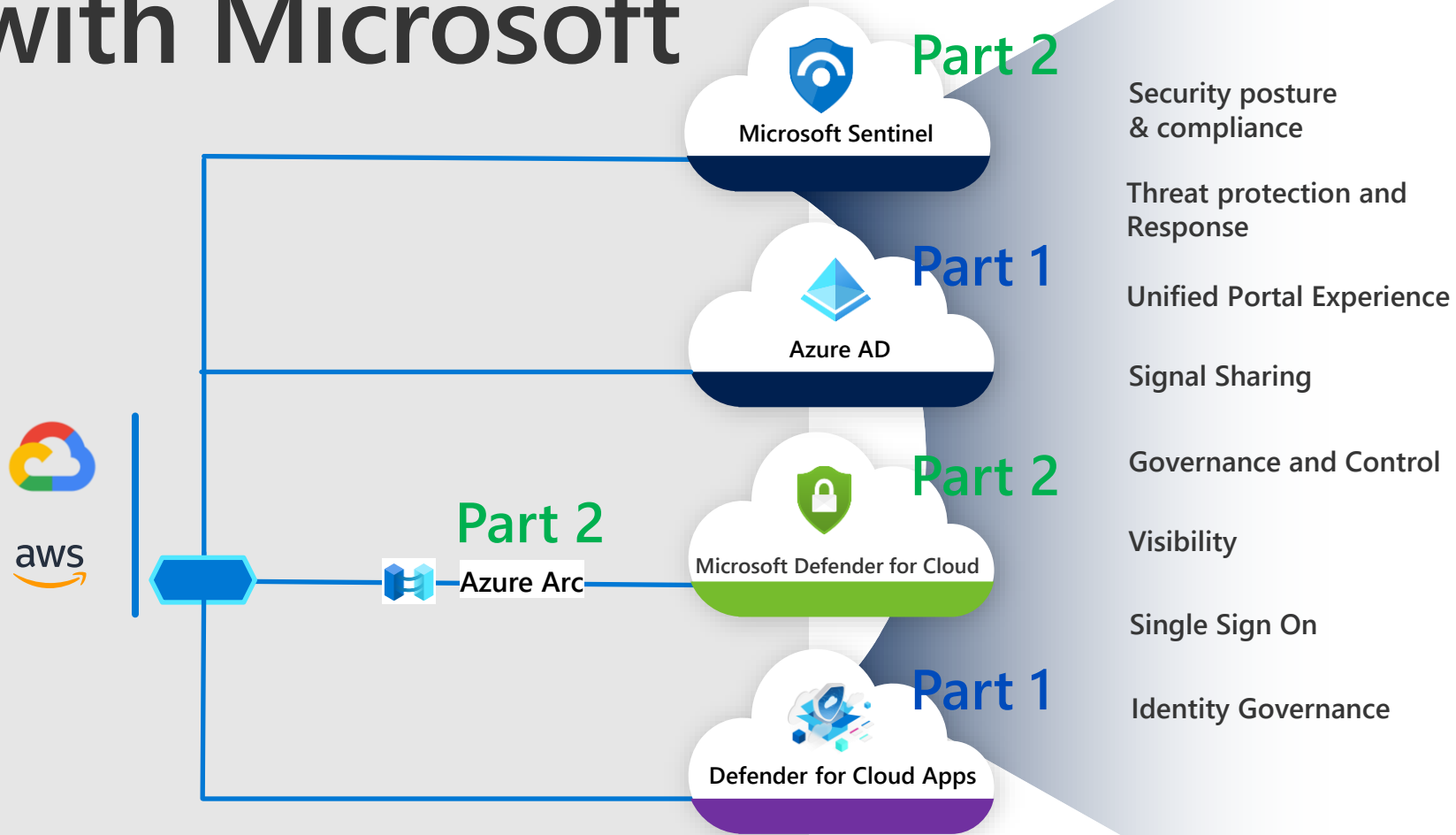


Why care?

- Revenue growth of 50% YoY for past 3 years
 - Azure Security growing faster...
- Strategic growth pillar for Microsoft
- 715k customers relying on Microsoft Security
- Market for managed security services growing beyond license/service spend
- Gartner predicts
"By 2025, 50% of enterprises will be using MDR"
- Whitespace of \$2Bn+ in UK alone



Securing AWS and GCP with Microsoft



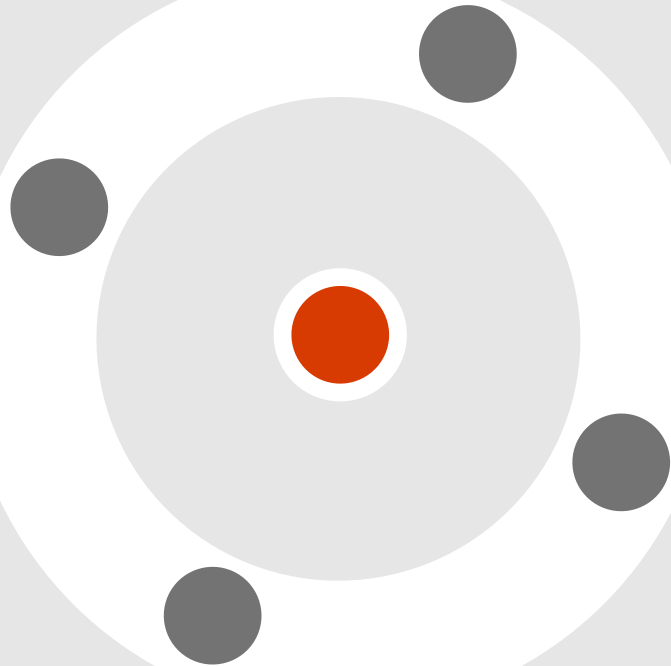
Azure Arc

Darren Small



Microsoft Defender for Cloud

Cassandra Browning



Cloud Security from Microsoft

Integrated protection for your multi-cloud resources, apps and data



Get your security posture in order

Microsoft Defender for Cloud



Defend against evolving threats

Microsoft Defender for Cloud



Control access to critical apps & resources

Microsoft Defender for Cloud Apps

Azure Network Security

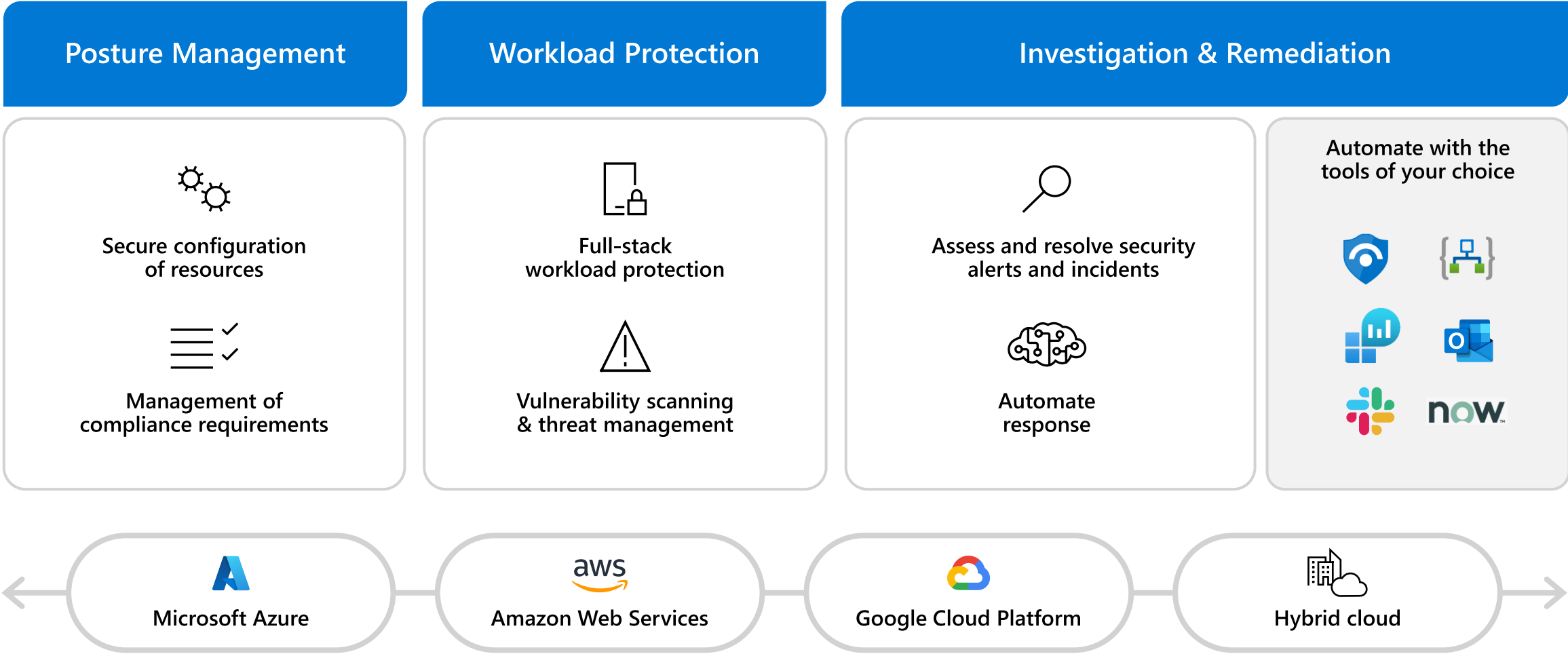
CloudKnox



Build secure apps from the start

GitHub Advanced Security

Microsoft Defender for Cloud



Cloud-Native Security



Built-in with Azure

- No deployment, just enable
- Built into the resource provisioning process
- Broadest protection coverage
- Identify sensitive data



Multi-cloud and hybrid support

- Agentless onboarding for AWS and GCP posture management
- Auto protection provisioning for new resources
- Onboard on-prem resources with Azure Arc



Advanced Threat Detection

- Deterministic, AI, and anomaly-based detection mechanism
- Leverages the power of Microsoft Threat Intelligence



Easy remediation and automation

- Remediate with the tools and workflows of your choice
- Native SIEM integration for automatic logging and easy management of incidents.
- Out-of-the box reporting

Posture Management

Birds-eye view with Secure Score

- Get an all-in-one view of your security posture and vulnerabilities across clouds
- Assess and implement best practices for security and compliance
- Improve your Secure Score in minutes and manage it over time

Out-of-the-box and custom recommendations

- 450+ out-of-the-box recommendations
- Support for security and regulatory compliance standards
- Create custom recommendations to meet organizational requirements

Easy remediation and automation

- Use “Quick fix” to remediate with a single click
- Create auto-remediation workflows using Azure Logic Apps

[Attackers Exploit Poor Cyber Hygiene to Compromise Cloud Security Environments | CISA](https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report)
<https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report> (p.124)

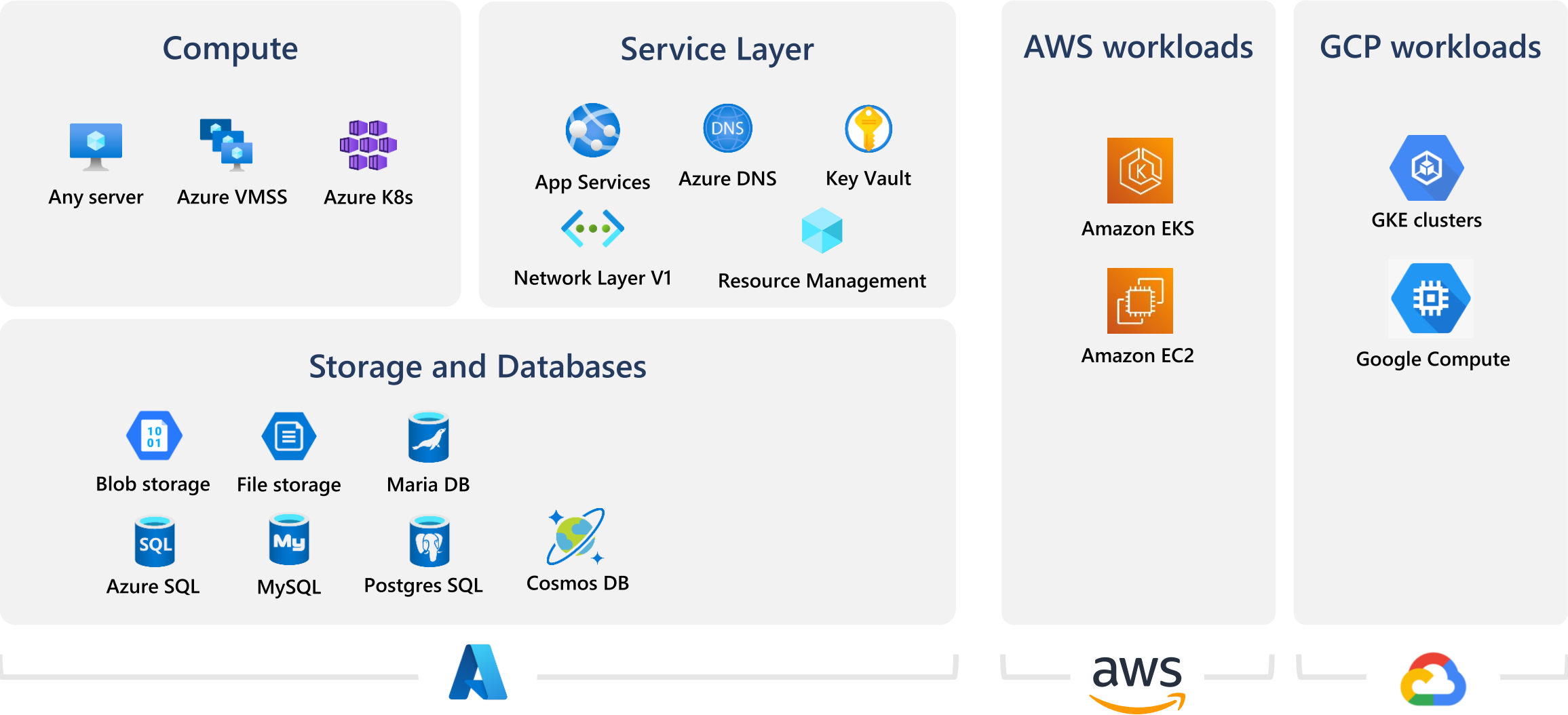


Workload Protection

- Protect cloud and on-premises resources against threats in one place
- Reduce your attack surface further by continuously scanning workloads to identify and manage vulnerabilities
- Automatically apply threat protection as soon as new workloads are deployed



Broad threat protection coverage



Microsoft Defender for Servers

Threat protection for servers

Protect Linux, Windows, EC2, and Google Compute

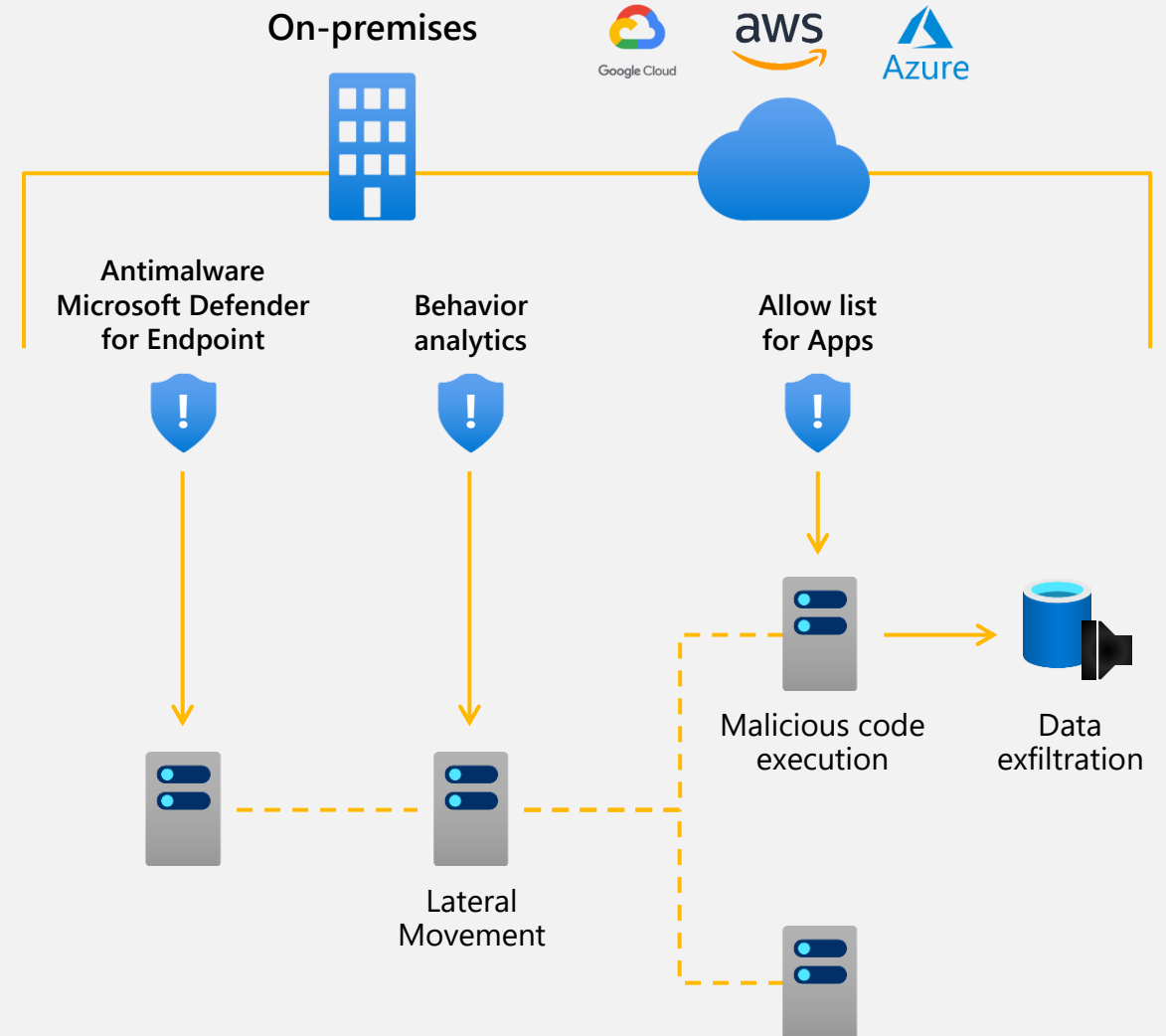
Reduce open network ports (Azure)

- Use Just-in-Time VM to control access to commonly attacked management ports
- Limit open ports with adaptive network hardening

Block malware with adaptive application controls

Protect Windows and Linux servers with the integration of Microsoft Defender for Endpoint

[Microsoft Defender for Cloud's servers features according to OS, machine type, and cloud | Microsoft Docs](#)



Assess your VMs for vulnerabilities

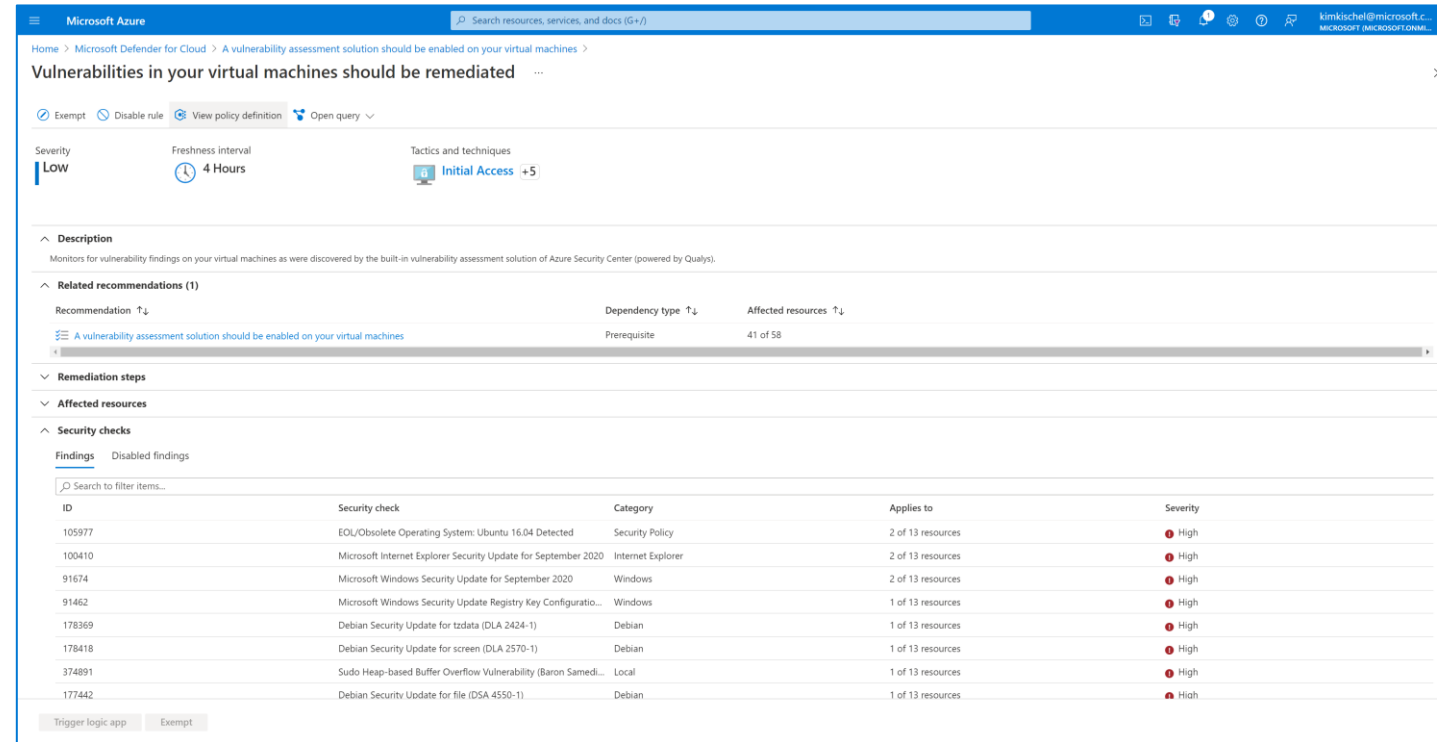


Automated deployment of the vulnerability scanner

Continuously scans installed applications to find vulnerabilities for Linux and Windows VMs

Visibility to the vulnerability findings in Security Center portal and APIs

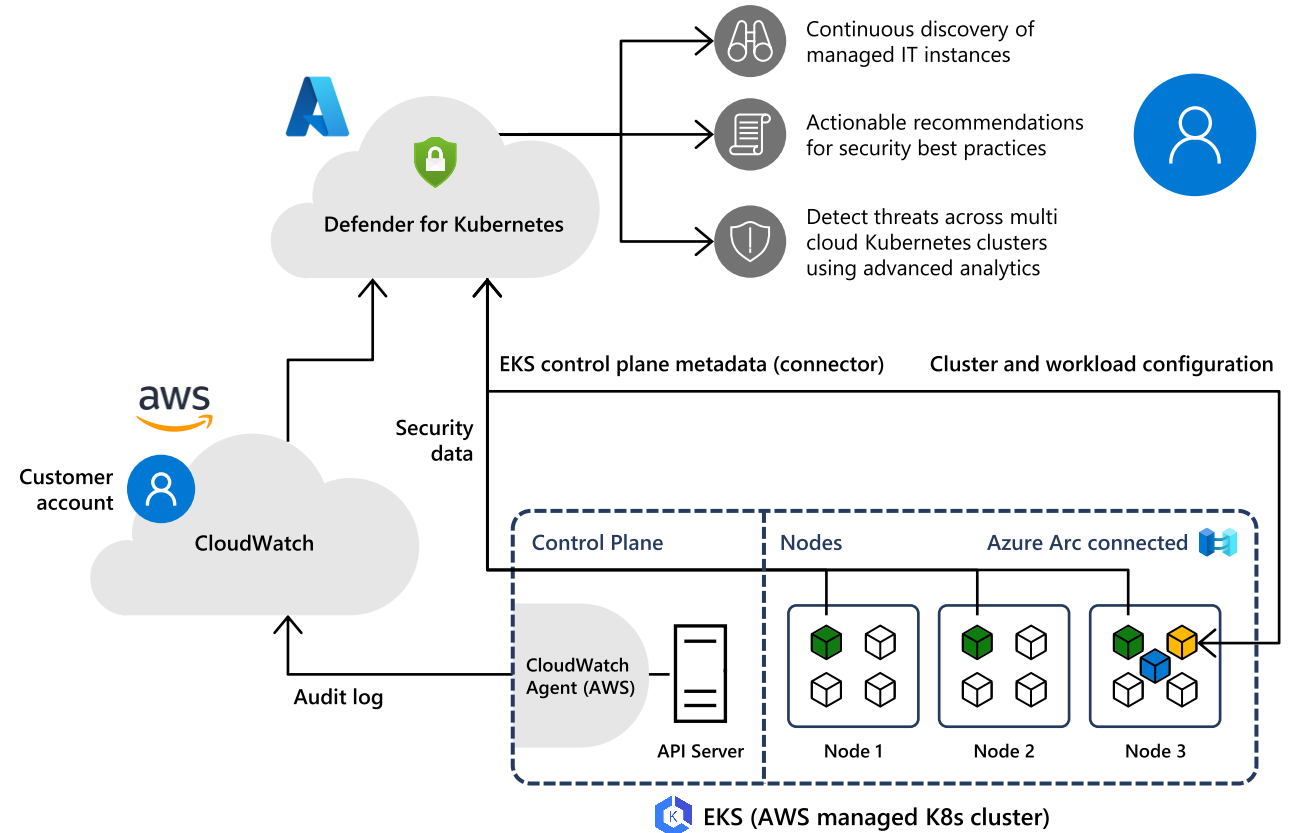
Choose between Qualys and Microsoft's threat and vulnerability management capabilities.



Microsoft Defender for Containers

Protect hybrid and multi-cloud Kubernetes deployments, leveraging Azure Arc for Kubernetes

- Cloud-native technology
- Multi-cloud and hybrid support
 - Amazon EKS and Google GKE
 - Kubernetes on-premises / IaaS
- Discovery and visibility of clusters
- Management and workload visibility
- Kubernetes-aware threat detection
- Kubernetes behavioral analytics and anomaly detection



[Microsoft Defender for Containers feature availability](#)
[| Microsoft Docs](#)

- Defender for Cloud extension
- Arc-enabled Kubernetes
- Gatekeeper, Azure Policy

Workflow Automation

- Apply Quick Fixes to recommendations
- Automate responses with Logic Apps
- Continuously export to Event Hub and Log Analytics
- Export to CSV



Break
Please return at 15:15pm GMT

Please complete the poll if you haven't already

<https://aka.ms/SecuringMVC2-Poll>



Microsoft Defender for Cloud – AWS



Microsoft Defender for Cloud | Recommendations

Showing subscription 'Microsoft Azure Sponsorship 2'

Search (Ctrl+F) Download CSV report Guides & Feedback

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Secure Score
- Regulatory compliance
- Workload protections
- Firewall Manager

Management

- Environment settings
- Security solutions
- Workflow automation

Secure score recommendations

All recommendations

Completed recommendations (by severity)

High	Medium	Low
45/56	18/40	19/56

Resource health

Unhealthy (152) Healthy (46) Not applicable (1)

Use these recommendations to harden your resources. Each one has a description, steps to take, and the affected resources. [Learn more >](#)

For the full details of a recommendation, select it from the list.

Search recommendations

Recommendation status: 2 Selected Recommendation maturity: All Severity: All Resource type: All Response actions: All

Contains exemptions: All Environment: AWS Tactics: All Initiative: All

Recommendation	Unhealthy resources	Resource health	Initiative	Actions
S3 buckets should have cross-region replication enabled	1 of 1 AWS S3 Buckets	AWS PCI DSS 3.2.1 (preview)		
Password policies for IAM users should have strong configurations	1 of 1 AWS accounts	AWS PCI DSS 3.2.1 (preview)		
MFA should be enabled for all IAM users	1 of 1 AWS IAM users	AWS PCI DSS 3.2.1 (preview)		
Hardware MFA should be enabled for the "root" account	1 of 1 AWS accounts	AWS CIS 1.2.0 (preview), AWS Foun...		
MFA should be enabled for the "root" account	1 of 1 AWS accounts	AWS CIS 1.2.0 (preview), AWS PCI ...		
Ensure a log metric filter and alarm exist for AWS Management Console authentication failures	1 of 1 AWS accounts	AWS CIS 1.2.0 (preview)		
Ensure AWS Config is enabled in all regions	17 of 17 AWS resources	AWS CIS 1.2.0 (preview), AWS Foun...		
Ensure a log metric filter and alarm exist for CloudTrail configuration changes	1 of 1 AWS accounts	AWS CIS 1.2.0 (preview)		
Ensure a log metric filter and alarm exist for disabling or scheduled deletion of customer create...	1 of 1 AWS accounts	AWS CIS 1.2.0 (preview)		
Ensure a log metric filter and alarm exist for AWS Config configuration changes	1 of 1 AWS accounts	AWS CIS 1.2.0 (preview)		
Ensure a log metric filter and alarm exist for security group changes	1 of 1 AWS accounts	AWS CIS 1.2.0 (preview)		
Ensure a log metric filter and alarm exist for route table changes	1 of 1 AWS accounts	AWS CIS 1.2.0 (preview)		
VPC's default security group should restricts all traffic	17 of 17 AWS EC2 security gr...	AWS CIS 1.2.0 (preview), AWS Foun...		
Amazon EC2 should be configured to use VPC endpoints	17 of 17 AWS EC2 VPC's	AWS Foundational Security Best Pr...		
GuardDuty should be enabled	17 of 17 AWS resources	AWS Foundational Security Best Pr...		
Lambda functions should have a dead-letter queue configured	1 of 1 AWS Lambda Functions	AWS Foundational Security Best Pr...		

Native AWS support using the AWS API

Policy management

Vulnerability management

Embedded Endpoint Detection and Response (EDR)

Detection of security misconfigurations

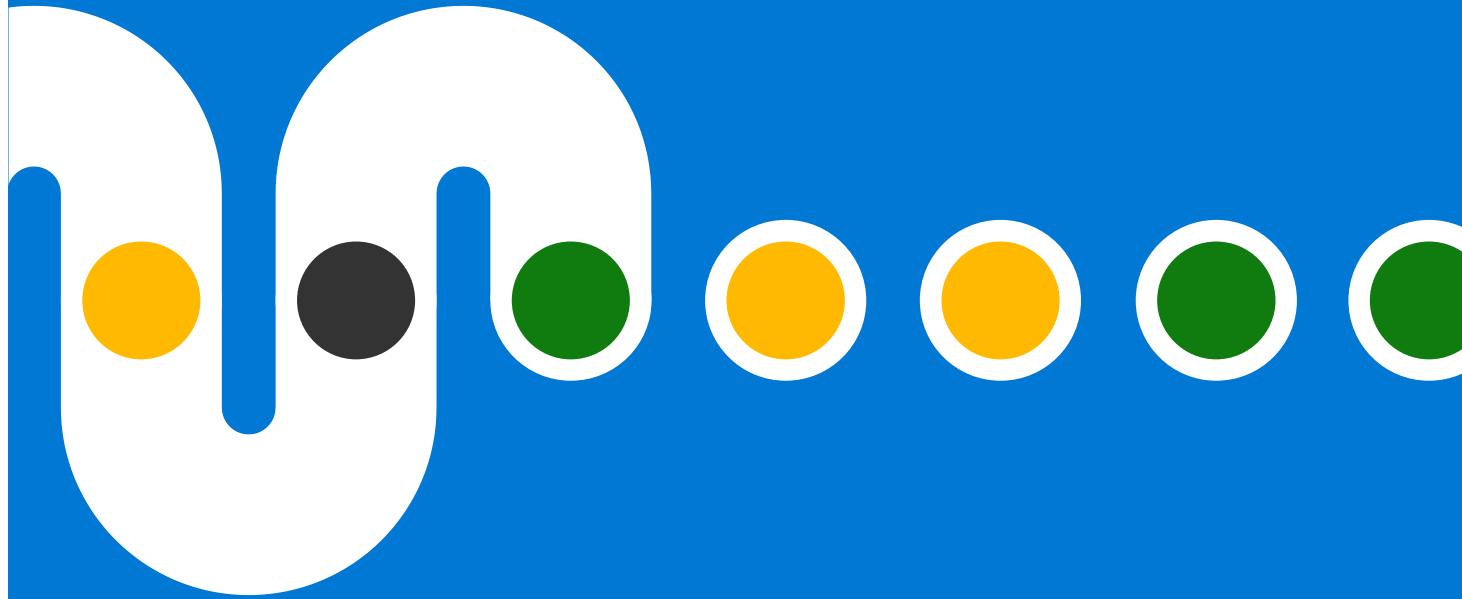
Protect Amazon EKS clusters and AWS EC2 workloads

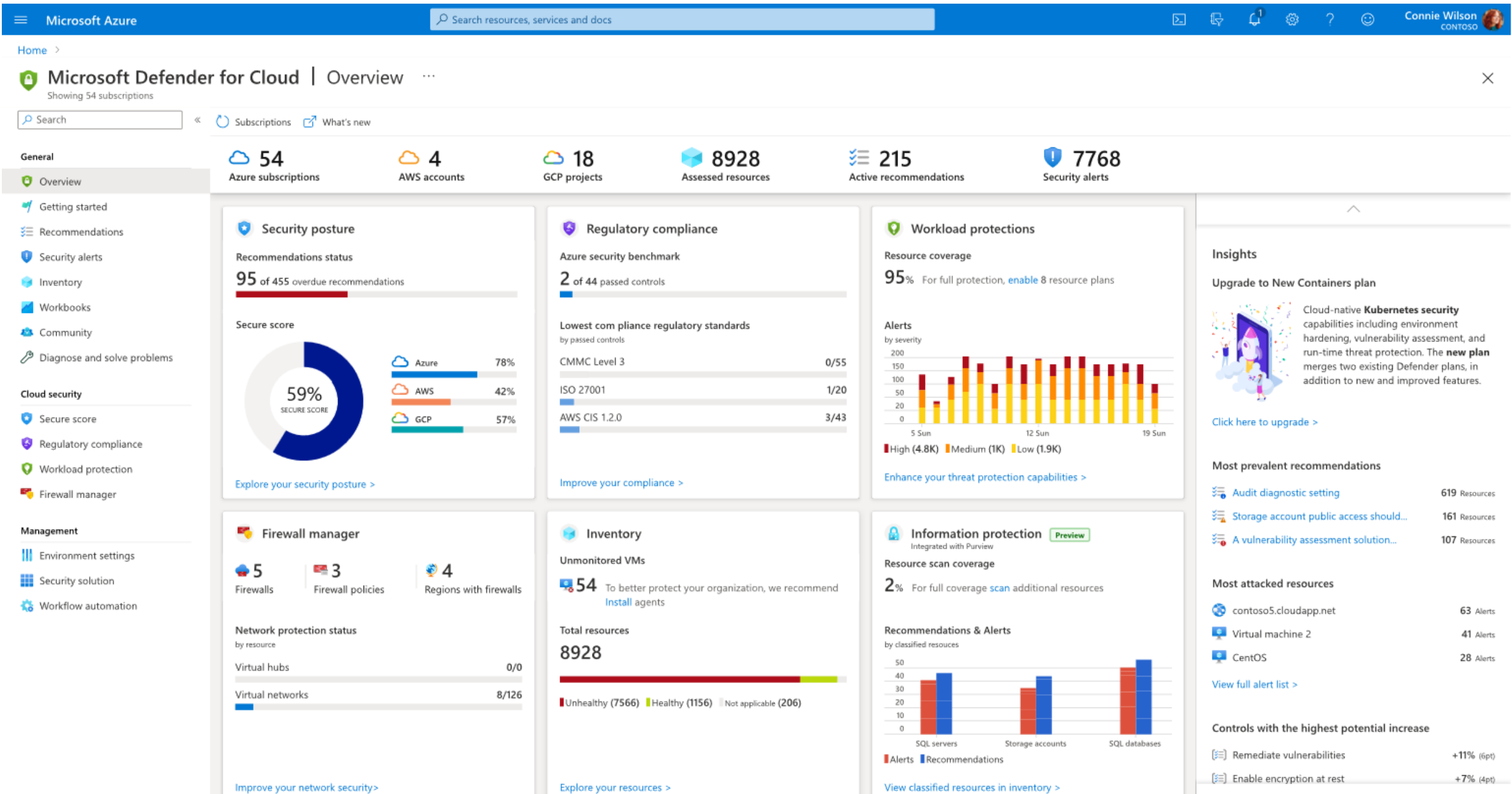
Incorporation of your AWS resources into MDfC's secure score calculations

160+ out of the box recommendations, CIS, PCI & AWS Foundational Security Best Practices support


Removed dependencies on AWS Security hub; native integration into the environment and recommendations

AWS Demo







AWS – MDfC Environment Settings

 Microsoft Azure

Search resources, services, and docs (G+)



Home > Microsoft Defender for Cloud

 Microsoft Defender for Cloud | Environment settings ...

Showing subscription 'Microsoft Azure Sponsorship 2'

Search (Ctrl+)

«

+ Add environment ▾

SQL Information Protection

Refresh

Guides & Feedback

General

Overview

Getting started

Recommendations

Security alerts

Inventory

Workbooks

Community

Diagnose and solve problems


Cloud Security


Secure Score


Regulatory compliance


Workload protections

Firewall Manager

 Amazon Web Services (preview)

 Google Cloud Platform (preview)

 1
AWS accounts

 1
GCP projects

Multi-cloud account management page (preview). To switch back to the classic cloud connectors experience, [click here](#).



Search by name

Environments == All

Standards == All

Coverage == All

Expand all

Name ↑↓	Total resources ↑↓	Defender coverage ↑↓	Standards
▼ Azure			
> [A] Tenant Root Group (1 of 1 subscriptions)	208		
▼ AWS (preview)			
 [REDACTED]	139	3/4 plans <div><div></div></div>	AWS C
▼ GCP (preview)			
 [REDACTED]	45	3/3 plans <div><div></div></div>	GCP C

Microsoft Defender for Cloud – GCP



Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Recommendations

Showing subscription 'ASC DEMO'

Search (Ctrl+/) «

Download CSV report Guides & Feedback

General

- Overview
- Getting started
- Recommendations
- Security alerts
- Inventory
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security

- Secure Score
- Regulatory compliance
- Workload protections
- Firewall Manager

Management

- Environment settings
- Security solutions
- Workflow automation

Secure score recommendations All recommendations

Active recommendations (by severity)

High	Medium	Low
49/132	38/178	40/215

Resource health

Unhealthy (7951)	Healthy (1320)	Not applicable (43)
------------------	----------------	---------------------

Use these recommendations to harden your resources. Each one has a description, steps to take, and the affected resources. [Learn more >](#)

For the full details of a recommendation, select it from the list.

Search recommendations

Recommendation status: 2 Selected Recommendation maturity: All Severity: All Resource type: All Response actions: All

Contains exemptions: All Environment: GCP Tactics: All Initiative: All

Recommendation	Unhealthy resources	Resource health	Initiative	Actions
Ensure that Service Account has no Admin privileges	7 of 7 Cloud resource manager projects		GCP CIS 1.1.0 (preview), GCP Defa...	
Ensure oslogin is enabled for a Project	7 of 7 Compute projects		GCP CIS 1.1.0 (preview), GCP Defa...	
Ensure that the 'log_lock_waits' database flag for Cloud SQL PostgreSQL instance is set to 'on'	7 of 7 Sql admin instances		GCP CIS 1.1.0 (preview), GCP Defa...	
Ensure that the 'log_min_messages' database flag for Cloud SQL PostgreSQL instance is set to 'on'	7 of 7 Sql admin instances		GCP CIS 1.1.0 (preview), GCP Defa...	
Ensure that the 'log_temp_files' database flag for Cloud SQL PostgreSQL instance is set to '0'	7 of 7 Sql admin instances		GCP CIS 1.1.0 (preview), GCP Defa...	
Ensure that the 'log_min_duration_statement' database flag for Cloud SQL PostgreSQL instance is...	7 of 7 Sql admin instances		GCP CIS 1.1.0 (preview), GCP Defa...	
Ensure that the 'contained database authentication' database flag for Cloud SQL on the SQL Serv...	2 of 2 Sql admin instances		GCP CIS 1.1.0 (preview), GCP Defa...	
Ensure that Cloud SQL database instances do not have public IPs	14 of 14 Sql admin instances		GCP CIS 1.1.0 (preview), GCP Defa...	
Ensure 'remote access' database flag for Cloud SQL SQL Server instance is set to 'off'	2 of 2 Sql admin instances		GCP Default	
Ensure Firewall Rules for instances behind Identity Aware Proxy (IAP) only allow the traffic from ...	284 of 285 Firewalls		GCP Default	
Ensure 'skip_show_database' database flag for Cloud SQL Mysql instance is set to 'on'	5 of 5 Sql admin instances		GCP Default	
Ensure 'log_duration' database flag for Cloud SQL PostgreSQL instance is set to 'on'	7 of 7 Sql admin instances		GCP Default	
Ensure 'log_hostname' database flag for Cloud SQL PostgreSQL instance is set appropriately	7 of 7 Sql admin instances		GCP Default	
Ensure 'log_min_error_statement' database flag for Cloud SQL PostgreSQL instance is set to 'Error...	7 of 7 Sql admin instances		GCP Default	
Ensure 'log_planner_stats' database flag for Cloud SQL PostgreSQL instance is set to 'off'	7 of 7 Sql admin instances		GCP Default	
Ensure 'user connections' database flag for Cloud SQL SQL Server instance is set as appropriate	2 of 2 Sql admin instances		GCP Default	

Native GCP support using the Google APIs

Policy management

Vulnerability management

Embedded Endpoint Detection and Response (EDR)

Detection of security misconfigurations

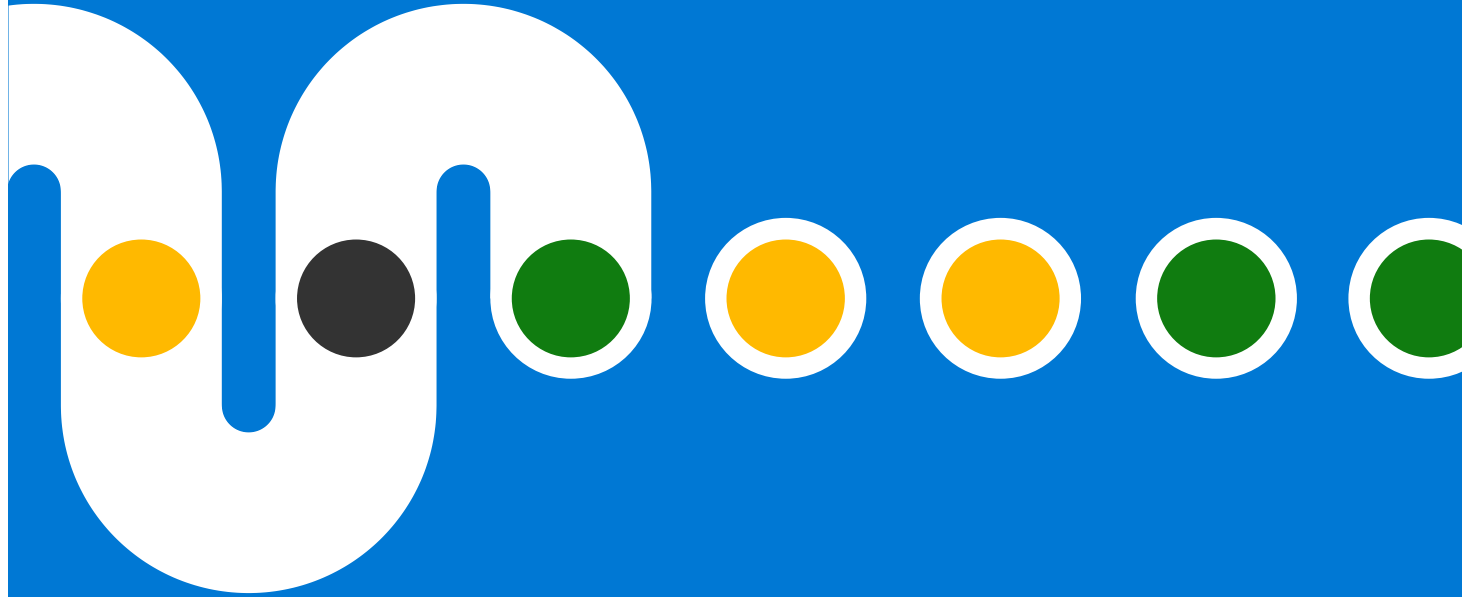
Protect Google GKE clusters and GCE workloads

Incorporation of your GCP resources into MDfC's secure score calculations

80+ out of the box recommendations aligned to industry standards and best practices such as CIS Benchmark for Google Cloud

Removed dependencies on Google Command Center; native integration into the environment and recommendations

GCP Demo



GCP – Environment settings

Microsoft Azure (Preview)

Search resources, services, and docs (G+)

Microsoft Defender for Cloud | Environment settings

Showing subscription 'ASC DEMO'

Search (Ctrl+)

+ Add environment

Refresh

Guides & Feedback

General

Overview

Getting started

Recommendations

Security alerts

Inventory

Workbooks

Community

Diagnose and solve problems

Cloud Security

Secure Score

Regulatory compliance

Workload protections

Firewall Manager

Management

Environment settings

Security solutions

Workflow automation

1

Azure subscriptions

7

AWS accounts

7

GCP projects

Welcome to the new multi-cloud account management page (preview). To switch back to the classic cloud connectors experience, [click here](#).

Search by name

Environments == All

Standards == All

Coverage == All

Expand all

Name ↑↓	Total resources ↑↓	Defender coverage ↑↓	Standards ↑↓
▼ Azure			
> 72f988bf-86f1-41af-91ab-2d7cd011db47 (1 of 4 subscriptions)	9352		⚠ Limited permissions
▼ AWS (preview)			
> 098881452406 (MDC_Containers_demo)		3/4 plans	AWS Foundational Security Best Practices (...)
> 371992567628 (AwsManagementAccount)		1/4 plans	Amit test standard, CustomRecommendati...
> 102614528198 (securityConnector)	39	3/4 plans	AWS CIS 1.2.0 (preview), AWS Foundational...
▼ GCP (preview)			
764670276399 (GcpProdConnector)		1/3 plans	Amit test standard, GCP CIS 1.1.0 (preview)...
205639119396 (DetectionProd)		2/3 plans	GCP Default
682450190097 (GCP-Containers-AP)		3/3 plans	GCP Default
922372707509 (mdc-containers-demo2)		3/3 plans	GCP Default

Microsoft Defender for Cloud



- Centrally secure and protect resources across the three major cloud providers and hybrid environments
- Ensure the secure and compliant configuration of cloud resources
- Detect vulnerabilities and threats to protect against malicious attacks

We always welcome feedback about our products! Please use User voice if you have ideas, suggestions, or feedback: <https://aka.ms/MDFCUserVoice>

If you're a customer as well as a partner, we have this link for feature requests: <https://aka.ms/CxESubmitFR>

Microsoft Defender for Cloud and Azure Arc Resources

- Microsoft Defender for Cloud Ninja Training – <http://aka.ms/ascninja>
- Microsoft Defender for Cloud Community Repository – <https://github.com/Azure/Microsoft-Defender-for-Cloud>
- SC-200 – Security Operations Analyst Associate - <https://docs.microsoft.com/en-us/learn/certifications/security-operations-analyst/>
- Defender for Cloud 'In the Field' YouTube series – <https://www.youtube.com/hashtag/mdfcinthe field>
- Microsoft Security Community – <http://aka.ms/SecurityCommunity>
- Azure Arc Jumpstart – <https://azurearcjumpstart.io/overview/>
- Must Learn KQL – <http://aka.ms/mustlearnkql>

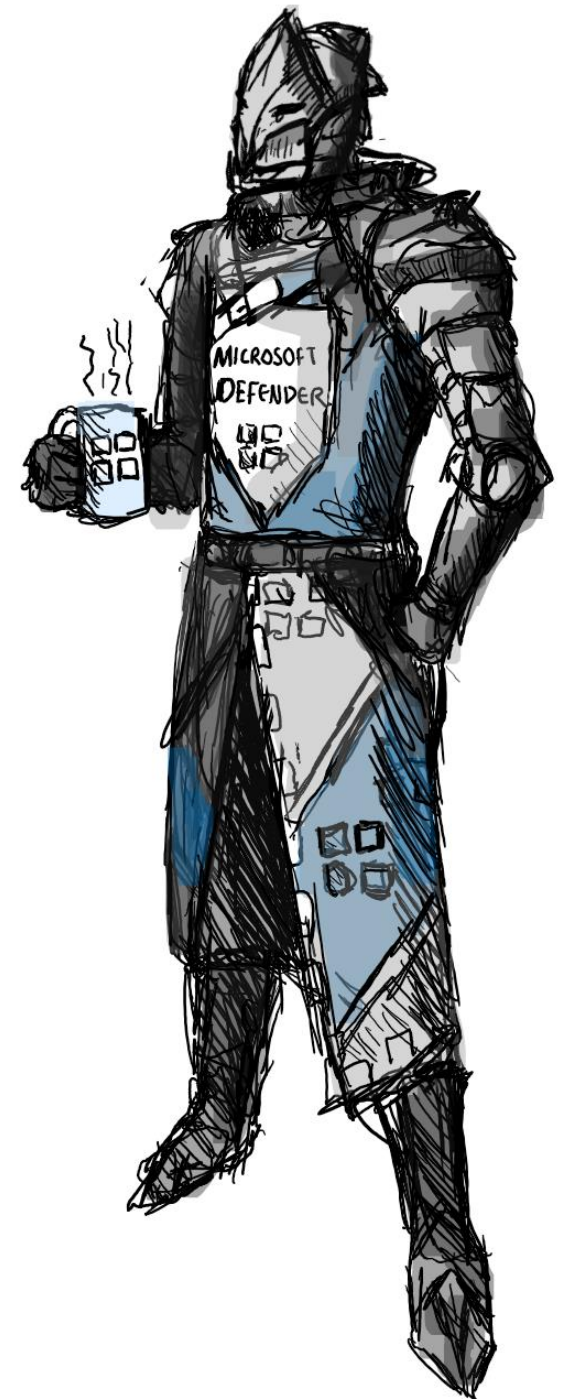


Break

Please return at 16:35pm GMT

Please complete the poll if you haven't already

<https://aka.ms/SecuringMVC2-Poll>

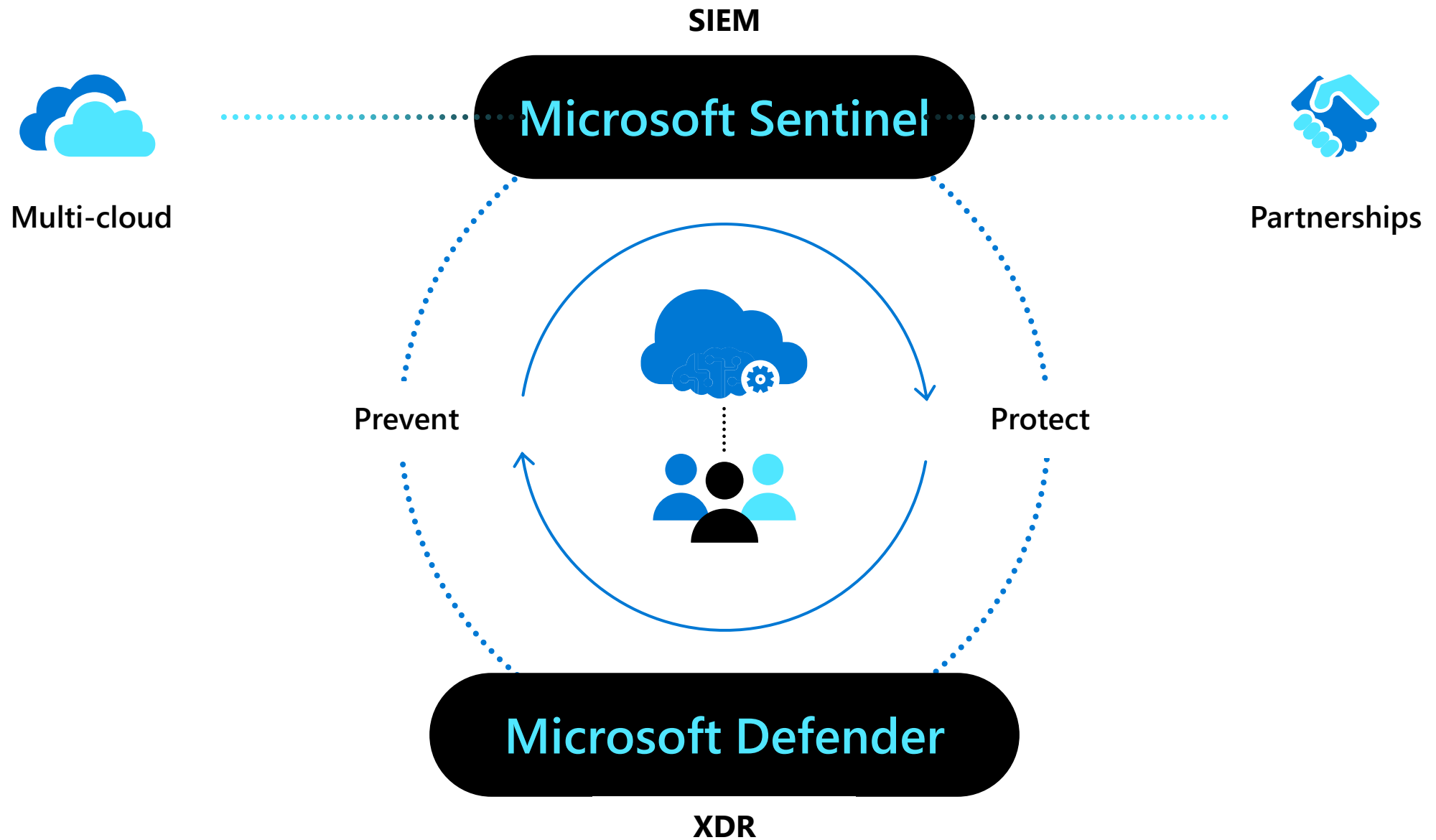


How does Microsoft Sentinel support Multi-Cloud?

Ally Turnbull

Partner SCI Cloud Solution Architect UK





Microsoft Sentinel

An end-to-end solution for security operations



Powered by community + backed by Microsoft's security experts



Collect



Visibility

Detect



Analytics



Hunting



Intelligence

Investigate



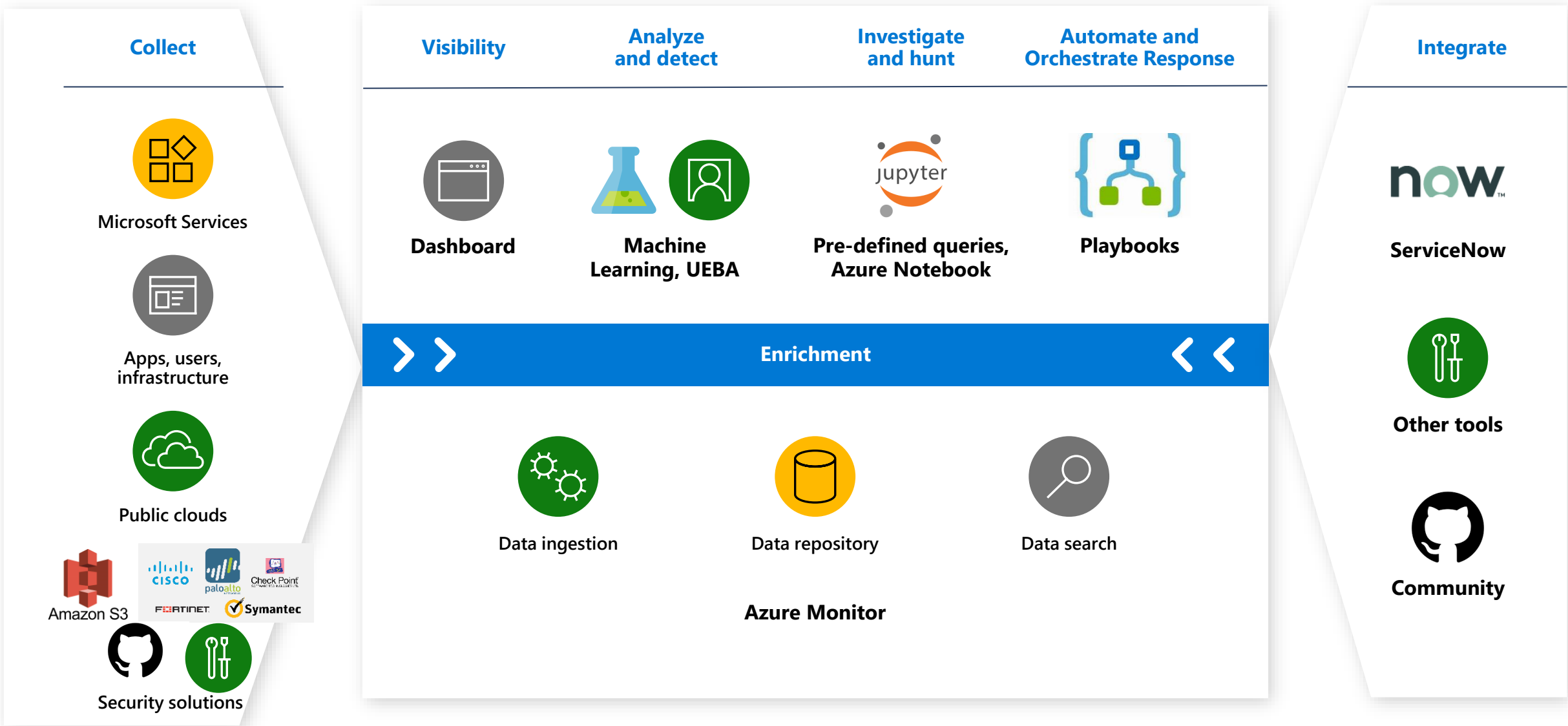
Incidents

Respond

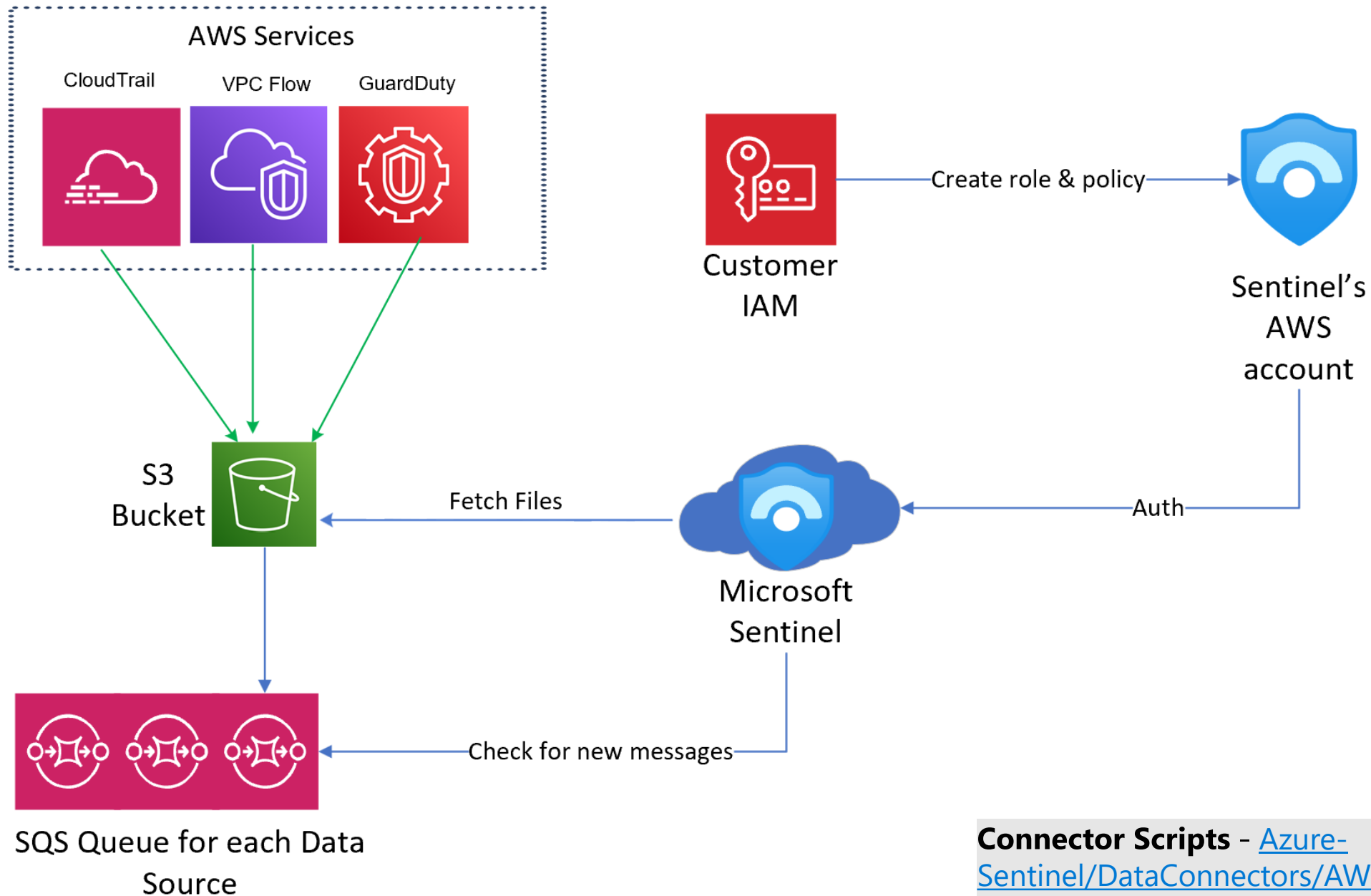


Automation

How it works

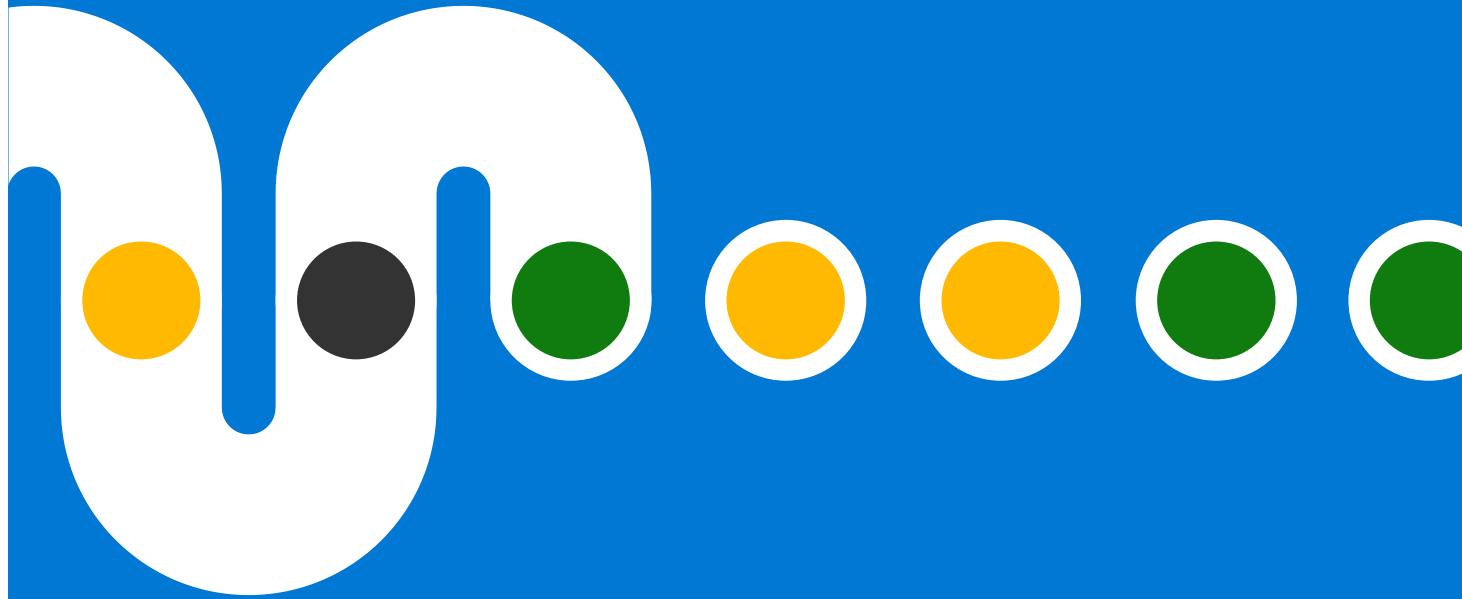


AWS S3 Microsoft Sentinel Connector Architecture



Connector Scripts - [Azure-Sentinel/DataConnectors/AWS-S3 at master · Azure/Azure-Sentinel \(github.com\)](https://github.com/Azure/Azure-Sentinel/tree/master/DataConnectors/AWS-S3)

AWS S3 Demo



PowerShell Scripts

Connector Scripts - [Azure-Sentinel/DataConnectors/AWS-S3 at master · Azure/Azure-Sentinel \(github.com\)](https://github.com/Azure/Azure-Sentinel/tree/master/DataConnectors/AWS-S3)

←

→

↺

https://github.com/Azure/Azure-Sentinel/tree/master/DataConnectors/AWS-S3

<> Code

Issues 97

Pull requests 97

Actions

Projects

Wiki

Security

Insights

master

Azure-Sentinel / DataConnectors / AWS-S3 /

Go to file

Add file

...

sivanguetta

AWS S3 connector- update AWS S3 connector permissions policies

✓ ea5baef 12 days ago

History

..

Utils

AWS S3 connector- Limit IAM role permissions (#4184)

22 days ago

AwsRequiredPolicies.md

AWS S3 connector- update AWS S3 connector permissions policies

12 days ago

ConfigAwsConnector.ps1

[Data connectors] Aws S3 Script- Add Sentinel tag when creating a new...

4 months ago

ConfigAwsS3DataConnectorScripts.zip

AWS S3 connector- Limit IAM role permissions (#4184)

22 days ago

ConfigCloudTrailDataConnector.ps1

AWS S3 connector- Limit IAM role permissions (#4184)

22 days ago

ConfigGuardDutyDataConnector.ps1

AWS S3 connector- Limit IAM role permissions (#4184)

22 days ago

ConfigVpcFlowDataConnector.ps1

[Data connectors] Aws S3 Script- Add Sentinel tag when creating a new...

4 months ago

ConfigVpcFlowLogs.ps1

[Data connectors] Aws S3 Script- Add Sentinel tag when creating a new...

4 months ago

README.md

[Data connectors] Aws S3 Script- Add Sentinel tag when creating a new...

4 months ago

Auto refresh: Off

Subscription
CyberSecSOC

Workspace
CyberSecuritySOC

Time Range
Last 90 days

Help
Yes No Change Log

CloudTrail GuardDuty VPCFlow Table Status

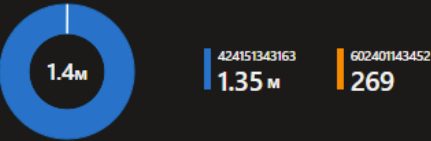
Group: CloudTrail

Overview User Network

Data flow over Time. TimeRange selected: Last 90 days with Automatic Time Grain of: 2d



Account IDs



EventSource list

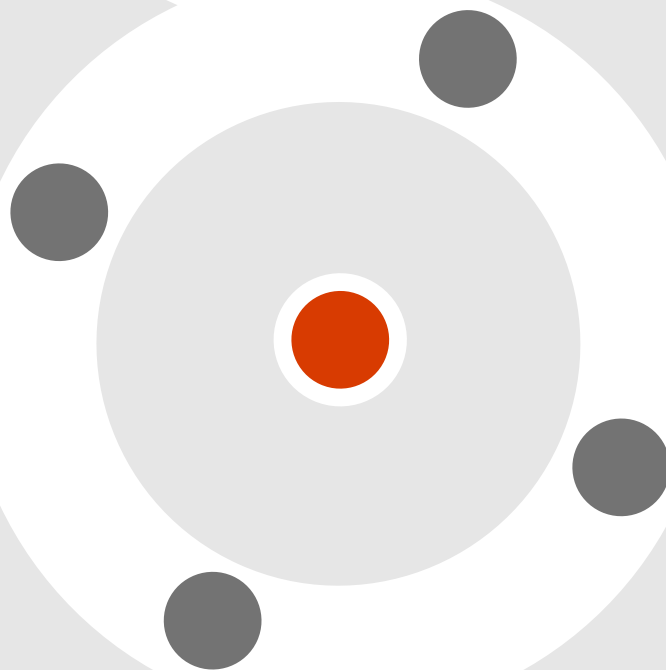
EventSource	count
iam.amazonaws.com	1220437
sts.amazonaws.com	781910
s3.amazonaws.com	721779
cloudtrail.amazonaws.com	329357
ec2.amazonaws.com	251484
kms.amazonaws.com	159942
ssm.amazonaws.com	68582
config.amazonaws.com	49972
elasticloadbalancing.amazonaws.com	34616

Microsoft Sentinel Resources



- Codeless connectors - [The Codeless Connector Platform - Microsoft Tech Community](#)
- Sentinel Github Data Connectors - [Azure-Sentinel/DataConnectors at master · Azure/Azure-Sentinel \(github.com\)](#)
- Ninja Training - [The Ninja Training 2021 edition is out! - Microsoft Tech Community](#)
- Sentinel Learning Path - [https://docs.microsoft.com/en-us/learn/paths/security-ops-sentinel/](#)
- SC-200 – Security Operations Analyst Associate - [https://docs.microsoft.com/en-us/learn/certifications/security-operations-analyst/](#)
- Sentinel Tech community – Blogs – [https://techcommunity.microsoft.com/t5/azure-sentinel/bg-p/AzureSentinelBlog](#)
- What's new in Microsoft Sentinel - [https://docs.microsoft.com/en-us/azure/sentinel/whats-new](#)
- How to deploy Microsoft Sentinel as a managed security services provider - [http://aka.ms/azsentinelmssp](#)

Wrap Up





Product	Feature	Theme	Capabilities	AWS Requirments	Deployment Effort	Additional Costs
Defender for Cloud Apps	Security Auditing	Visibility, Detection, Response	UEBA, Threat Detection, Investigation, AWS Activity	CloudTrail, GuardDuty	Minimal, Easy to Configure	Microsoft: E5 License AWS: CloudTrail and GuardDuty
Defender for Cloud Apps	Security Configuration	Visibility	Visibility, Inventory, Misconfiguration, CIS Benchmark for AWS	Security Hub	Minimal, Easy to Configure	Microsoft: E5 License AWS: Security Hub
Defender for Cloud Apps	Conditional Access App Control	Visibility, Detection, Prevention	Session Visibility and Control , Governance Controls	None	Moderate, Integration with IDP	Microsoft: E5 License
Defender for Cloud	Cloud Security Posture Management	Visibility	Visibility , Inventory , Misconfiguration , Hardening Guidance	None	Minimal, Easy to Configure	None
Defender for Cloud	Defender for Servers Defender for Endpoint	Detection, Prevention, Response	EDR , Regulatory Compliance Scanning , Threat Detection, Vulnerability Assessment , FIM , Adaptive Application Controls	Systems Manager	Moderate, Requires Agents	Microsoft: \$0.02/Server/hour AWS: Systems Manager
Defender for Cloud	Defender for Containers – EKS	Detection, Prevention, Response	Real-time threat protection	CloudWatch, S3, Kinesis, SQS	Minimal, Easy to Configure	Microsoft: \$0.00268/vCore/hour AWS: CloudWatch, S3, Kinesis, SQS
Microsoft Sentinel	N/A	Visibility, Detection, Prevention, Response	SIEM, SOAR, UEBA , ML Threat Detection , SOC-ML	CloudWatch, GuardDuty, VPC Flow Logging, S3, SNS	Moderate, Requires AWS component configuration	Microsoft: Charged for Data Ingestion and Retention AWS: CloudWatch, GuardDuty, VPC Flow Logging, S3, SNS
Azure Active Directory	Conditional Access , SSO, Identity Protection, Privileged Identity Management	Detection, Prevention, Protection, Zero Trust	Risk based access , threat detection , Identity Governance	None	Moderate, Requires migrating to Azure AD for SSO	Microsoft: Azure AD P2 / E5 / EMS License

Capabilities Matrix



Product	Feature	Theme	Capabilities	GCP Requirments	Deployment Effort	Additional Costs
Defender for Cloud Apps	Security Auditing	Visibility, Detection, Response	UEBA, Threat Detection, Investigation, GCP Activity	Cloud Audit Logs	Minimal, Easy to Configure	Microsoft: E5 License GCP: Google Cloud's operations suite (formerly Stackdriver)
Defender for Cloud Apps	Security Configuration	Visibility	Visibility, Inventory, Misconfiguration, CIS 1.1 Benchmark	Security Command Center	Minimal, Easy to Configure	Microsoft: E5 License GCP: Security Health Analytics (potentially)
Defender for Cloud Apps	Conditional Access App Control	Visibility, Detection, Prevention	Session Visibility and Control , Governance Controls	None	Moderate, Integration with IDP	Microsoft: E5 License
Defender for Cloud	Cloud Security Posture Management	Visibility	Visibility , Inventory , Misconfiguration , Hardening Guidance	None	Minimal, Easy to Configure	None
Defender for Cloud	Defender for Servers Defender for Endpoint	Detection, Prevention, Response	EDR , Regulatory Compliance Scanning , Threat Detection, Vulnerability Assessment , FIM , Adaptive Application Controls	OS config agent (for autoprovisioning)	Moderate, Requires Agents	Microsoft: \$0.02/Server/hour GCP: VM Agent (for autoprovisioning)
Defender for Cloud	Defender for Containers – GKE	Detection, Prevention, Response	Real-time threat protection	None	Minimal, Easy to Configure	Microsoft: \$0.00268/vCore/hour GCP: None beyond GKE
Microsoft Sentinel	N/A	Visibility, Detection, Prevention, Response	SIEM, SOAR, UEBA , ML Threat Detection , SOC-ML	GCP: Cloud Logging, Cloud Monitoring	Moderate, Requires AWS component configuration	Microsoft: Charged for Data Ingestion and Retention GCP: Cloud Logging + Cloud Monitoring
Azure Active Directory	Conditional Access , SSO, Identity Protection, Privileged Identity Managment	Detection, Prevention, Protection, Zero Trust	Risk based access , threat detection , Identity Governance	None	Moderate, Requires migrating to Azure AD for SSO	Microsoft: Azure AD P2 / E5 / EMS License

Labs and demo guidance



- **On-Demand Recording** - coming in the near future after this event
- **Slides & Labs** - <http://aka.ms/securingmvc2-repo>

Cloud skills challenge

<https://aka.ms/SecuringMVC2-CSC>

For more info and how to claim
your badge, visit

<https://aka.ms/SecuringMVC2-CSC>



Silver – Complete cloud skills challenge **and** be registered for the event.



Gold – Completed cloud Skills Challenge + registered for the event + pass the SC-200 exam.



Security, Compliance, Identity Enablement Guide for Partners

Access the latest partner-facing version here:

<https://aka.ms/scipartnerenablement>

Simplified Guide to SCI Partner training resources for the role-based exams, learning journeys across Security, and other key resources to support you and your organization on your skilling journey.

Security, Compliance, Identity Certifications and Exams

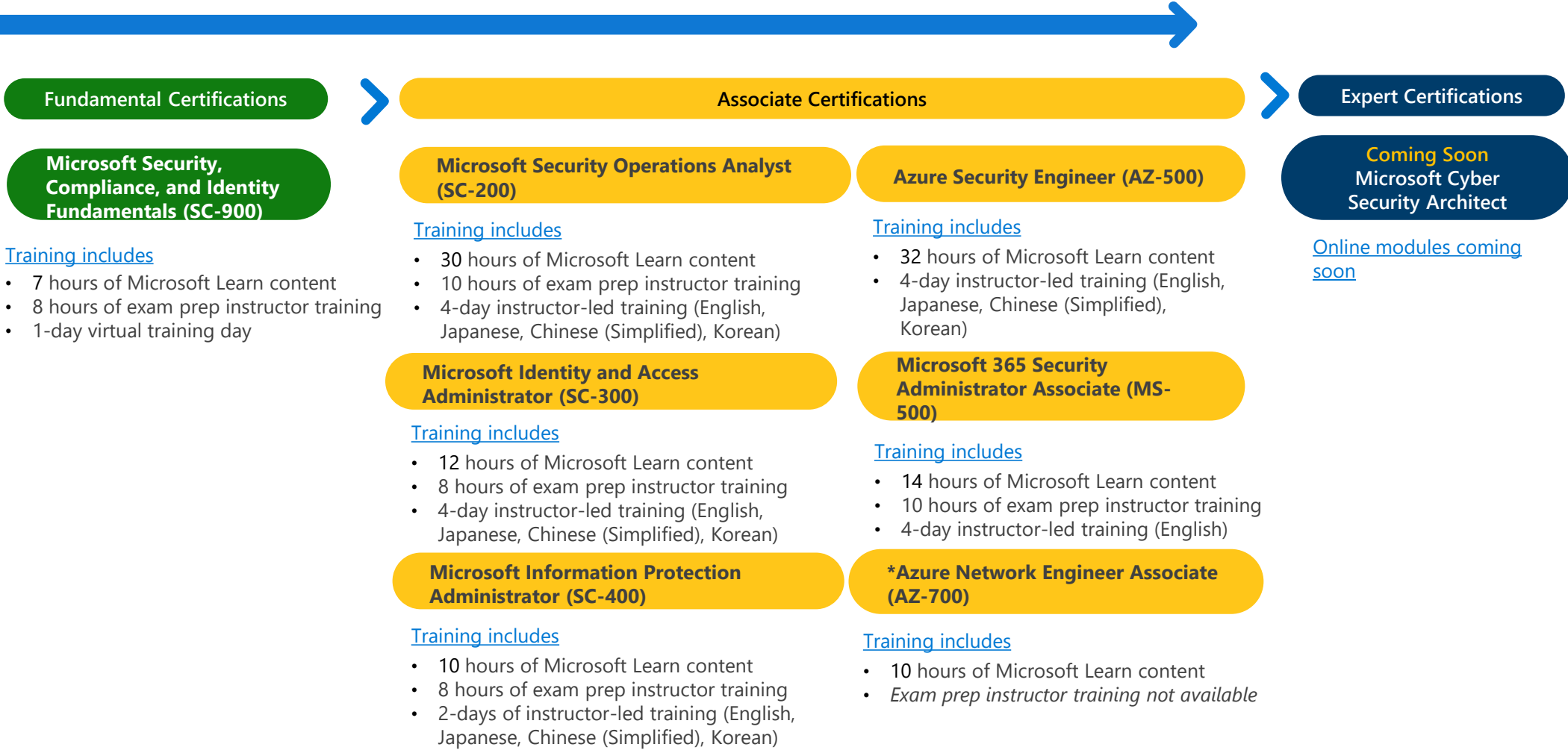
This page lists the certifications and exams that are recommended for partners looking to build and extend their Microsoft security, compliance, and identity practices.

The [Microsoft Security, Compliance, and Identity certification portfolio](#) includes the following certifications:

- Microsoft Security, Compliance, and Identity Fundamentals
- Microsoft Security Operations Analyst
- Microsoft Identity and Access Administrator
- Microsoft Information Protection Administrator
- Azure Security Engineer
- Microsoft 365 Security Administrator
- Microsoft Cybersecurity Architect

*Azure Network Engineer Associate is categorized in the Azure certification portfolio and is also relevant to our partners.

Go here for the latest certification roadmap [Microsoft training and certifications](#).



• Go here for the latest certification roadmap [Microsoft training and certifications](#).

Security workshops

	Threat protection	Microsoft Sentinel	Hybrid cloud security
Methodology	Discover threats in a customer's M365 cloud environment by using the Threat Check license , and provide recommendations to mitigate threat.	Discover threats in a customer's M365 cloud environment by using Microsoft Sentinel and Threat Check license , and provide recommendations to mitigate threat.	Discover threats and vulnerabilities in a customer's Azure, hybrid, and multi-cloud environment. Provide recommendations to mitigate.
Outcome	Create intent for purchasing and deploying M365 E5 Security.	Create intent for purchasing and deploying Microsoft Sentinel.	Create intent for purchasing and deploying Microsoft Defender for Cloud and Network Security products.
Customer eligibility	800+ AADP PAUs* 250+ monthly active units (MAU) for EXO, SPO, or Teams	800+ AADP* paid available units (PAU*) 250+ MAU* for EXO*, SPO*, or Teams	Annual Azure consumption for servers, SQL, and storage must be >\$150,000 USD. Defender for Cloud consumption is <4% of total Azure consumption.
Funding	Up to \$5,000 per workshop	Up to \$2,500 per workshop	Up to \$5,000 per workshop

To find out more: aka.ms/PartnerAccelerators

*PAU – Paid Available Units

*MAU – Monthly Active Usage

*EXO – Exchange Online

*SPO – SharePoint Online

*AADP – Azure Active Directory Premium

*Azure AD – Azure Active Directory

Microsoft Cybersecurity Reference Architectures

We are excited to announce an **update to the Microsoft Cybersecurity Reference Architectures (MCRA)**. The MCRA describes Microsoft cybersecurity capabilities. The diagrams describe how Microsoft security capabilities integrate with Microsoft platforms and third-party platforms such as Microsoft 365, Microsoft Azure, third-party apps such as ServiceNow and Salesforce, and third-party platforms such as Amazon Web Services (AWS) and Google Cloud Platform (GCP).

[View the update and download the file here.](#)

Capabilities

What cybersecurity capabilities does Microsoft have?



Build Slide



Azure Native Controls

What native security is available?



Attack Chain Coverage

How does this map to insider and external attacks?

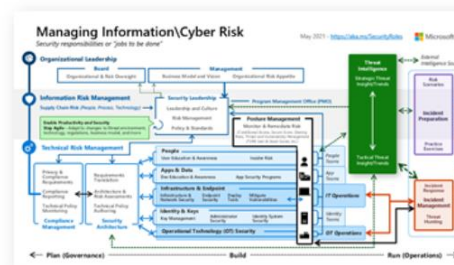


Build Slide



People

How are roles & responsibilities evolving with cloud and zero trust?



Multi-Cloud & Cross-Platform

What clouds and platforms does Microsoft protect?



Zero Trust User Access

How to validate trust of user/devices for all resources?



Security Operations

How to enable rapid incident response?



Operational Technology

How to enable Zero Trust Security for OT?





- Complete the [Cloud Skills Challenge](#)
- Pass the **SC-200 Microsoft Security Operations Analyst exam**
- [Cloud Accelerator](#) for Hybrid Cloud Security and Microsoft Sentinel Workshops
- **Share the training** and materials with others at your organization
- **Help your customers** with their security needs across the Microsoft security stack

Contact your local GPS Team to get started!
UK – protectanddefend@microsoft.com

Share your thoughts, **feedback** via our survey!
<https://aka.ms/SecuringMVC2-Feedback>



Thank you! Feedback:

<https://aka.ms/SecuringMVC2-Feedback>