Microsoft Security

Microsoft Defender for Cloud Masterclass Part 1

18 May 2022 from 1300 BST

Poll: https://aka.ms/MDfCMasterclassP1-Poll

Today's Agenda (BST)

13:00 - Intro and Housekeeping – Cassandra Browning

13:05 - Microsoft Defender for Cloud Overview – Cassandra

13:30 - Extending Microsoft Defender for Cloud beyond Azure – Bojan Magusic

14:15 - Break 10 mins

14:25 - Creating and using custom regulatory compliance policies – Liana Tomescu and Cassandra Browning

15:10 - Break 10 mins

15:20 - Automation – Tom Janetscheck

15:50 - Wrap Up + Live Q&A

16:00 - Event ends

Meet the Team

Cassandra Browning
Cloud Solutions Architect
Azure and multicloud security

Bojan Magusic
Program Manager
Defender for Cloud

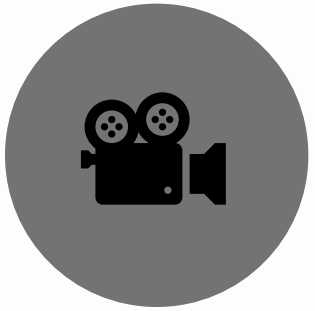
Tom Janetscheck
Senior Program Manager
Defender for Cloud Engineering

Liana Tomescu
Program Manager
Defender for Cloud

Housekeeping

There will be breaks & speaker changes throughout

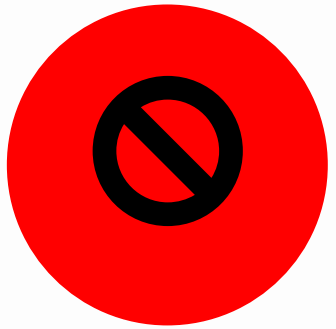
This is a one-way speaker to attendees audio, so please ask any questions in the Q&A



This will be recorded and links sent to you (typically within 24 hours of recordings being sent)

Feedback – https://aka.ms/MDfCMasterclassP1-Feedback

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



All content is under your partnership NDA

Microsoft Security

Microsoft Defender for Cloud Overview

Cassandra Browning

Microsoft Defender for Cloud

Posture Management

Secure configuration of resources

Management of compliance requirements

Workload Protection

Full-stack workload protection

Vulnerability scanning & threat management

Investigation & Remediation

Assess and resolve security alerts and incidents

Automate response

Automate with the tools of your choice

Microsoft Azure

Amazon Web Services

Google Cloud Platform

Hybrid cloud

How we're different

Built-in with Azure

- No deployment, just enable
- Built into the resource provisioning process
- Broad 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

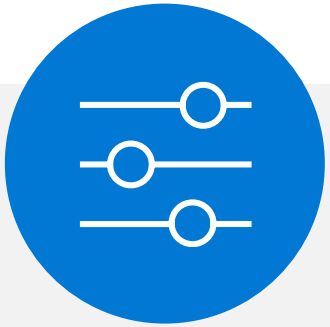
Advanced Threat Detection

- 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

Holistic management of your security posture in the cloud



Resource visibility

View and manage your cloud resource inventory

Secure Score

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

Compliance

Ensure your configurations align with key compliance standards and enforce organizational policies

Data security

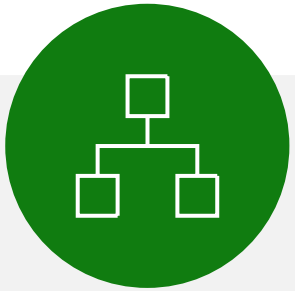
Identify sensitive data and prioritize critical resources

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

Threat protection for all layers of the cloud and on-prem

Threat detection

Prioritized alerts across compute, databases, the cloud service layer, and more



MITRE ATT&CK® framework mapping

Understand the effect across the adversary's attack lifecycle

Leading threat intelligence

Rely on highly sophisticated and resource-specific alerts based on Microsoft's global threat intelligence

Vulnerability management

Identify and remediate vulnerabilities before they are exploited

Alert correlation

Prioritize more easily with connected alerts that are grouped into incidents

Full-stack coverage with dedicated detections

Compute


Any server


Azure VMSS


App Services


Azure K8s

Service Layer

Azure DNS


Key Vault


Network Layer V1


Resource Manager

Databases and Storage

Blob storage


File storage


Maria DB


Azure Cosmos DB

Azure SQL

MySQL


Postgres SQL

AWS workloads


Amazon EKS


Amazon EC2

GCP workloads

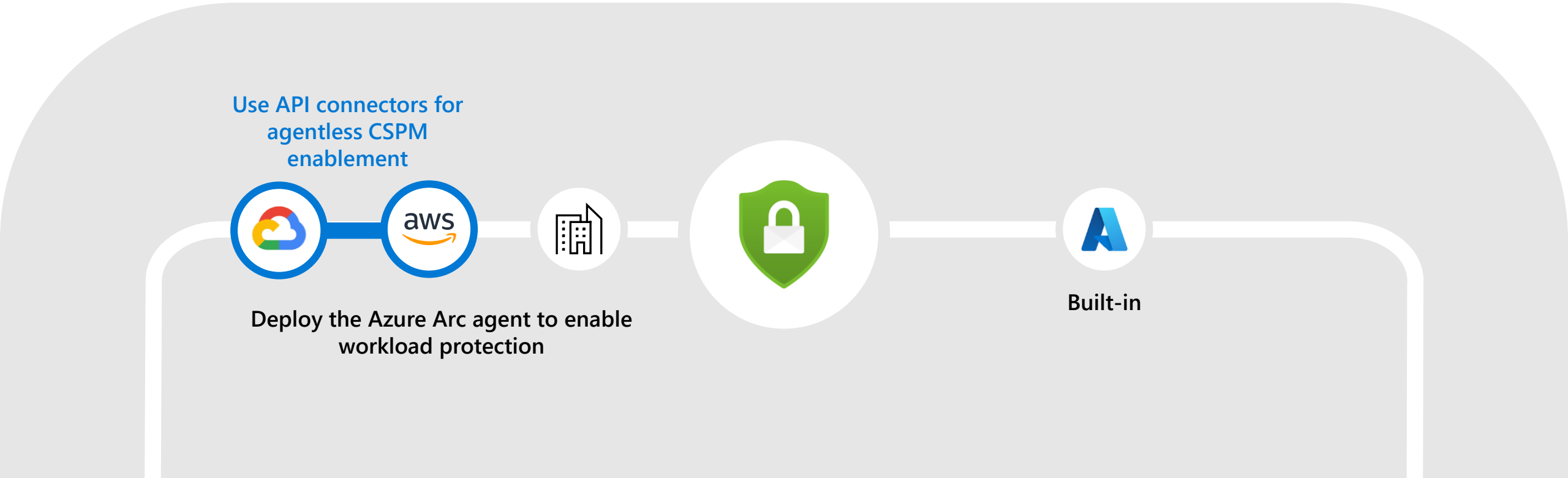

GKE clusters


Google Compute

[Microsoft Defender for Cloud Price Estimation Dashboard]

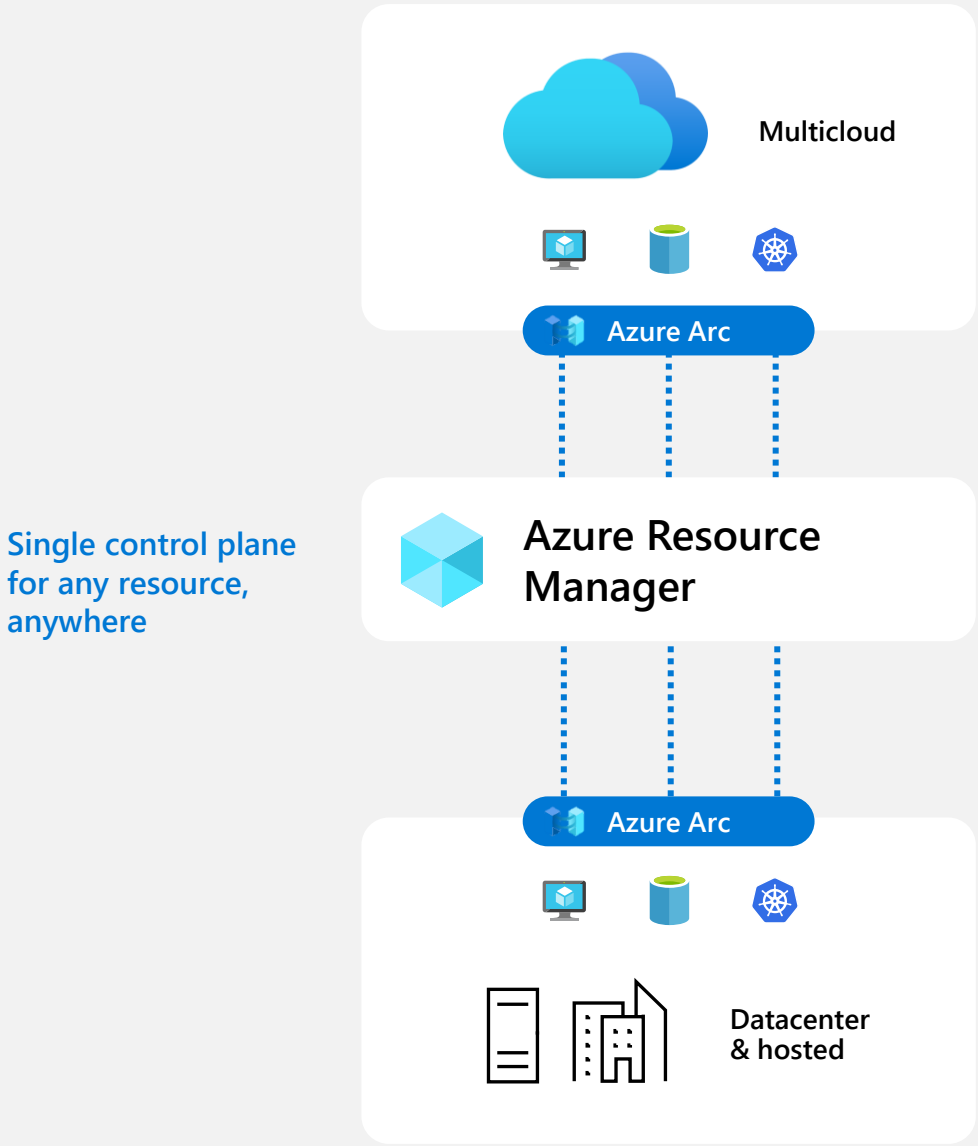
Multicloud and hybrid protection

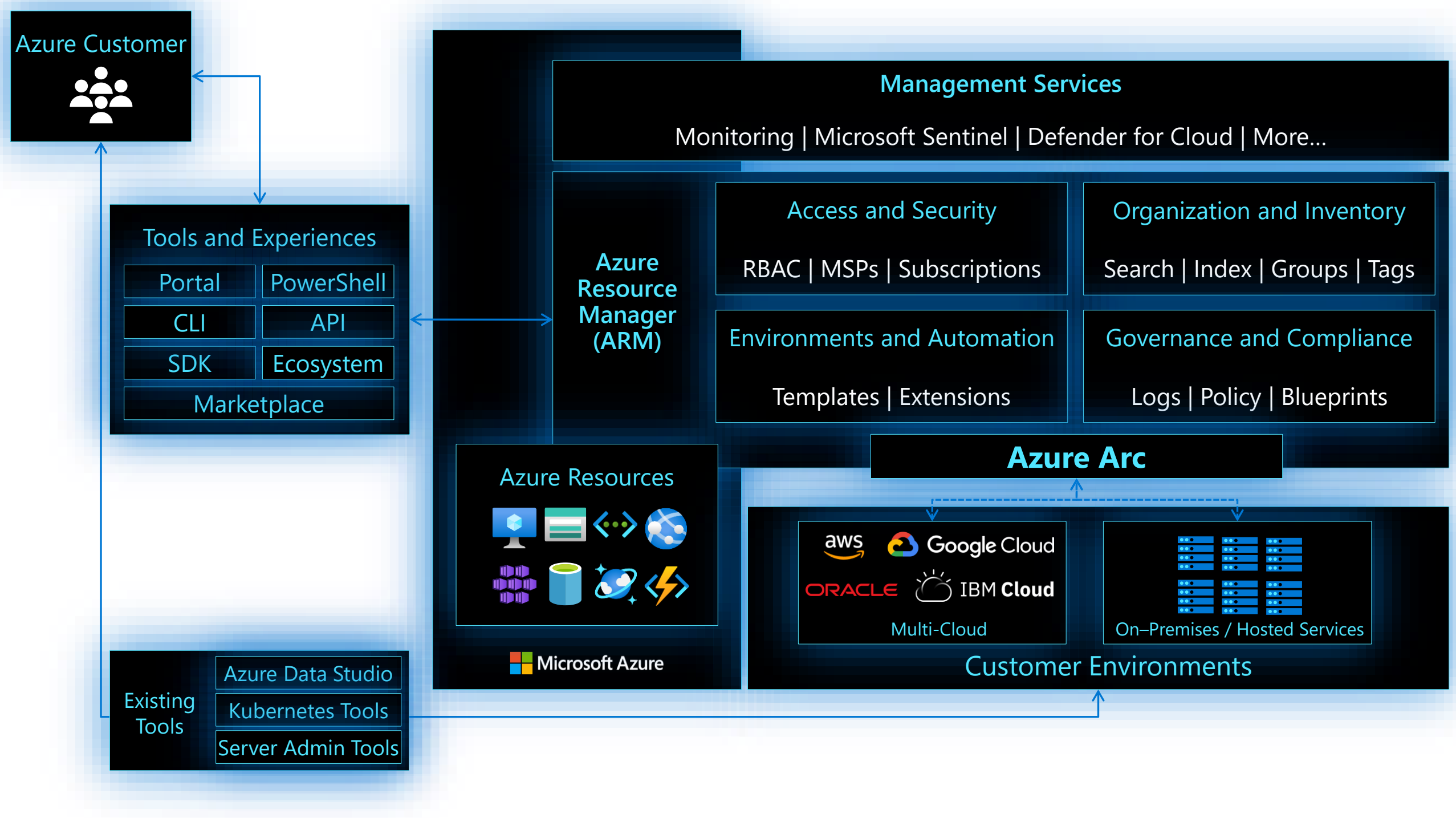
- Automatic onboarding for Azure subscriptions
- Use API connectors (**agentless**) to onboard AWS and GCP accounts to posture management capabilities.
- Use the Azure Arc agent to onboard workloads outside of Azure and protect them against threats



Use Azure Arc to connect workloads anywhere to Microsoft Defender for Cloud

- Azure Arc unlocks hybrid and multicloud scenarios so you can manage security for all your resources in a consistent way
  - Follow CAF hybrid and multicloud guidance
- Extension installation, e.g. Azure Monitor agent
- Enforce compliance and simplify audit reporting
- Asset organization and inventory with a unified view in the Azure Portal—Azure Tags
- Server owners can view and remediate to meet their compliance—RBAC in Azure




Azure Customer
Tools and Experiences
Portal
PowerShell
CLI
API
SDK
Ecosystem
Marketplace
Existing Tools
Azure Data Studio
Kubernetes Tools
Server Admin Tools
Management Services
Monitoring | Microsoft Sentinel | Defender for Cloud | More...
Azure Resource Manager (ARM)
Access and Security
RBAC | MSPs | Subscriptions
Organization and Inventory
Search | Index | Groups | Tags
Environments and Automation
Templates | Extensions
Governance and Compliance
Logs | Policy | Blueprints
Azure Resources
Microsoft Azure
Azure Arc
aws
Google Cloud
ORACLE
IBM Cloud
Multi-Cloud
On–Premises / Hosted Services
Customer Environments

Microsoft Defender for Servers

Threat protection for servers

Protect Linux, Windows, EC2, and Google Compute

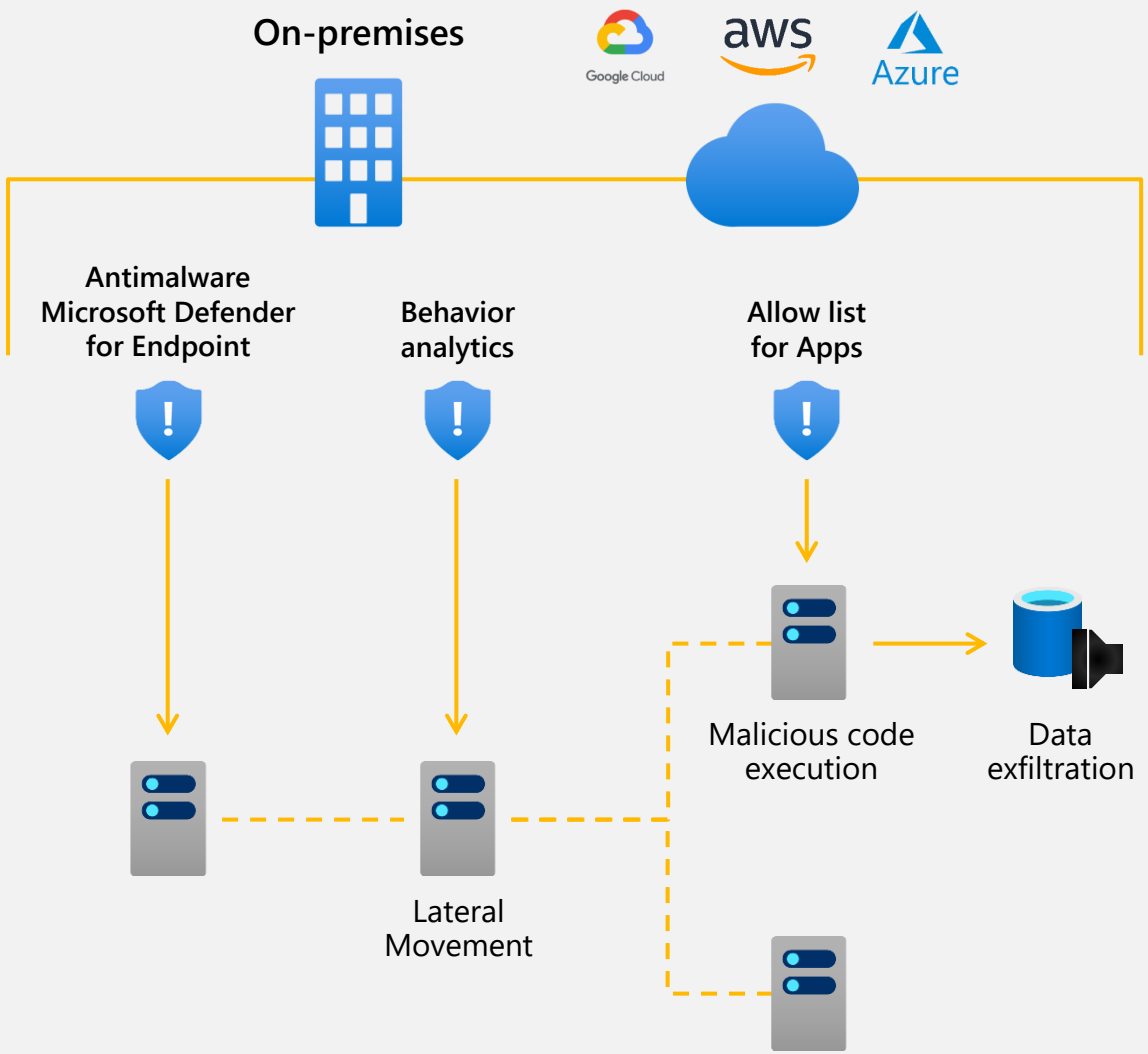
Reduce open network ports (Azure)

- 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 Defender for Servers - P1 and P2 plan comparison



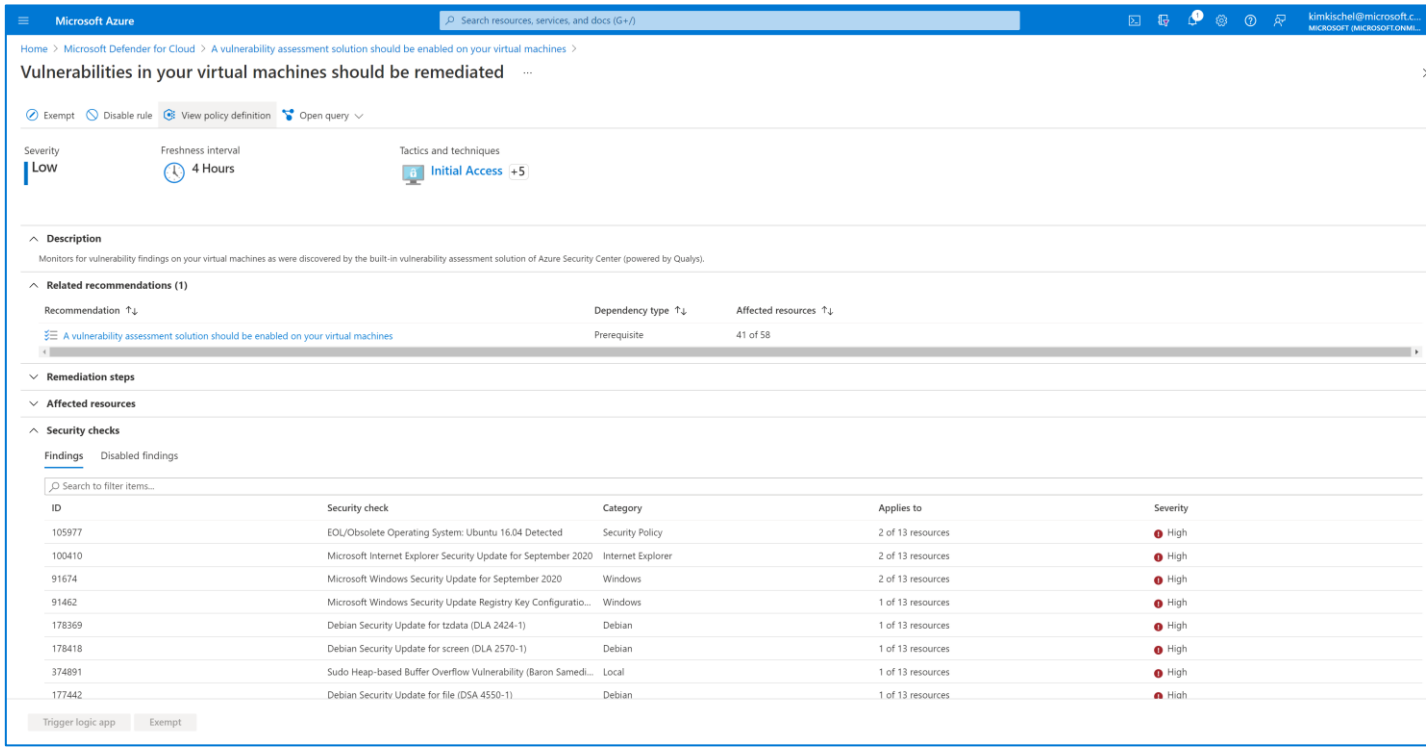
Assess your VMs for vulnerabilities

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

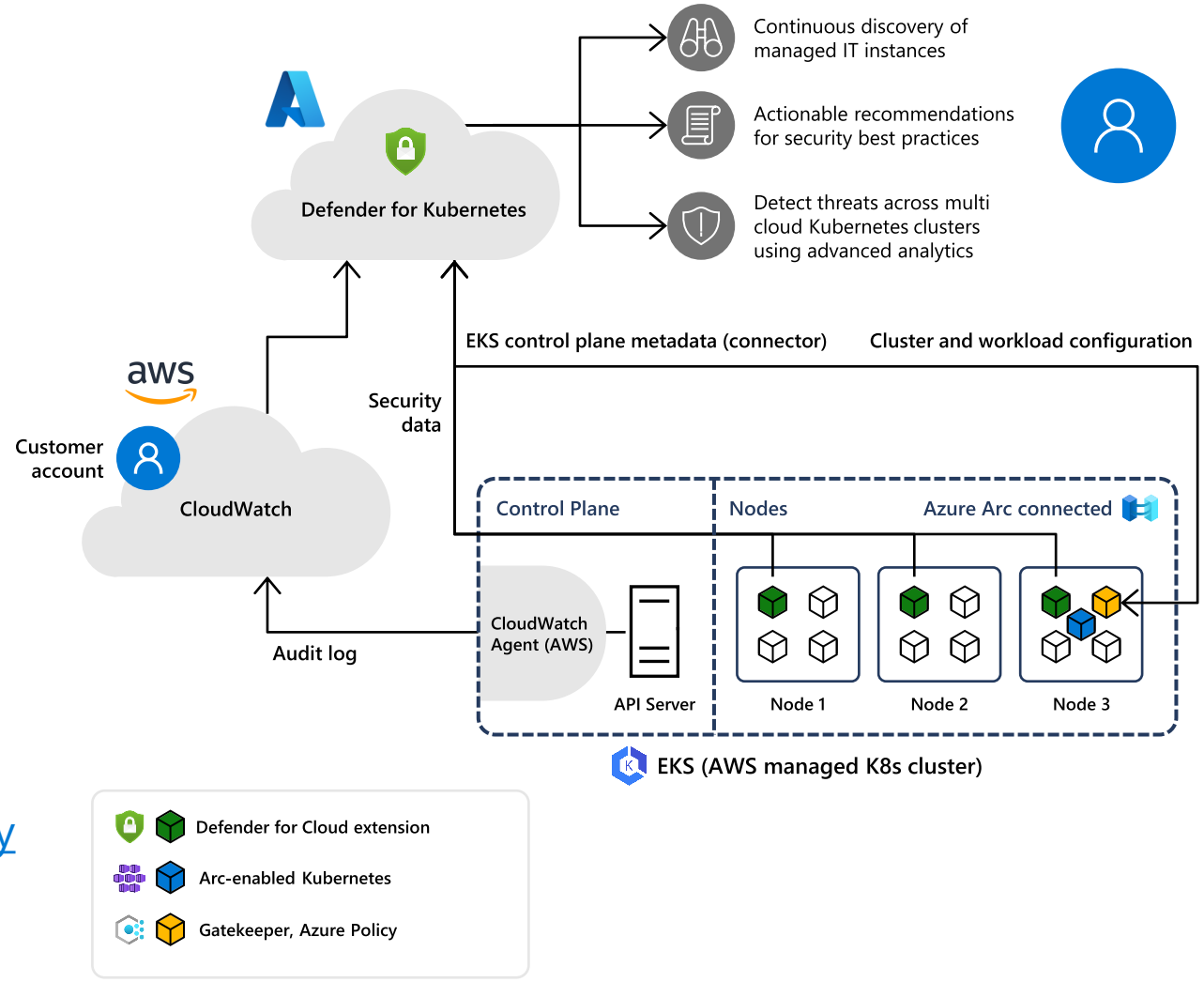
Choose between Qualys and Microsoft's threat and vulnerability management capabilities.



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]

Azure Lighthouse architecture: Bringing greater versatility and at-scale management capabilities into several scenarios

3 Use the client experience tool of your choice

Marketplace offers

ARM Template

APIs

PowerShell

Azure Portal

SDKs

CLIs

2 Cross-tenant experience integrated into Azure and third-party services

Azure Policy ⊕ Azure Monitor ⊕ Microsoft Defender for Cloud ⊕ Microsoft Sentinel ⊕ Azure Portal ⊕ Azure Kubernetes Service (AKS) ⊕ Azure Arc ⊕ Azure Virtual Network ⊕ And more...

1 Security acts as foundational fabric

Azure Resource Manager with Azure Role-Based Access Control (RBAC)

Privileged Identity Management + Azure Multi-Factor Authentication

Azure Lighthouse Deployment Samples on Github

Head to Microsoft Docs for more details

Azure Lighthouse + Azure Arc: Bring Azure services and management to any infrastructure

Azure Arc extends Azure management & enables Azure services to run across on-premises, multi-cloud, & edge

Grow revenue by expanding Servers & Kubernetes management in hybrid environments

Consolidate tool sets and governance for complex environments

Extend Azure Lighthouse security and visibility to hybrid and multi-cloud

Extend Azure management across environments

Adopt cloud practices on-premises

Run Azure data services anywhere

Azure Lighthouse + Microsoft Defender for Cloud: Bring secure posture management and workload protection to any infrastructure

Views and actions in cross tenant management

Manage security policies	From one view, manage the security posture of many resources with policies, take actions with security recommendations, and collect and manage security-related data.
Improve Secure Score and compliance posture	Cross-tenant visibility enables you to view the overall security posture of all your tenants and where and how to best improve the secure score and compliance posture for each of them.
Remediate recommendations	Monitor and remediate a recommendation for many resources from various tenants at one time. You can then immediately tackle the vulnerabilities that present the highest risk across all tenants.
Manage Alerts	Detect alerts throughout the different tenants. Take action on resources that are out of compliance with actionable remediation steps.
Manage advanced cloud defense features and more	Manage the various threat protection services, such as just-in-time (JIT) VM access, Adaptive Network Hardening, adaptive application controls, and more.

Cross-tenant management in Microsoft Defender for Cloud

Extending Microsoft Defender for Cloud beyond Azure

Bojan Magusic

Microsoft Security

THANK YOU!

Microsoft Defender For Cloud

Cloud native protection across clouds and hybrid environments

Harden and manage your Security Posture

Secure configuration of resources

Management of compliance requirements

Detect threats and protect your workloads

Full-stack threat protection

Vulnerability assessment & management

Respond & Automate

Assess and resolve security alerts and incidents

Automate response

Automate with the tools of your choice

Microsoft Azure

Amazon Web Services

Google Cloud Platform

Hybrid cloud

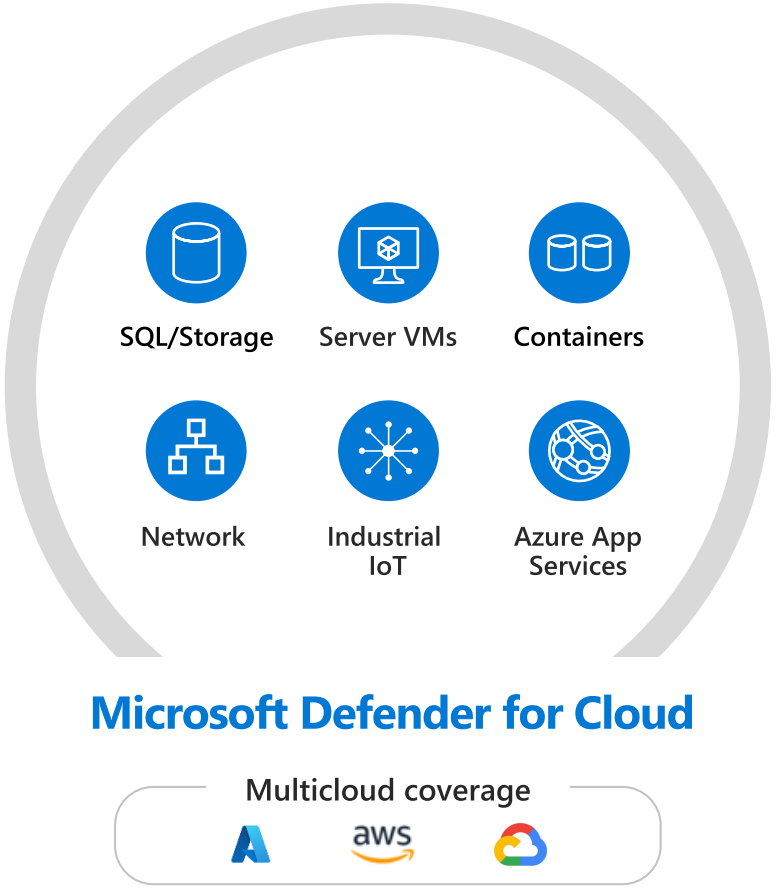
Multi-cloud – previous implementation

Multi-cloud – new solution

Seamless onboarding at scale | Regulatory standards breadth | Agentless design

Microsoft Defender for Cloud

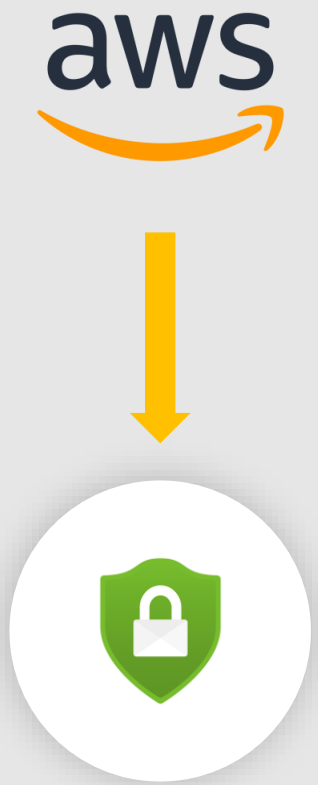
Secure your critical cloud workloads running in AWS, Azure, and Google Cloud



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

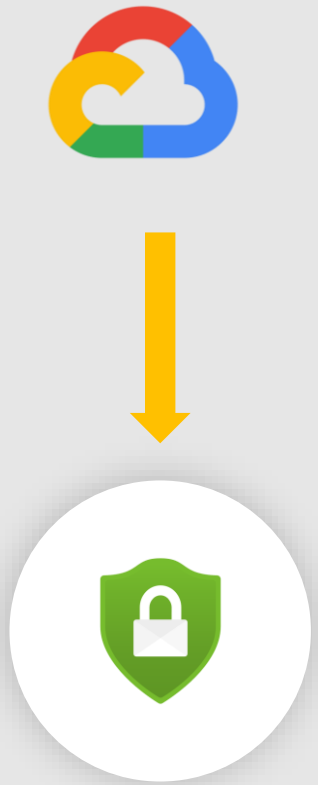
Connecting AWS accounts

- Easy, fast and granular onboarding
- Onboard single accounts or auto-provision the management account
- Defender plans are not dependent (e.g. enable CSPM only)



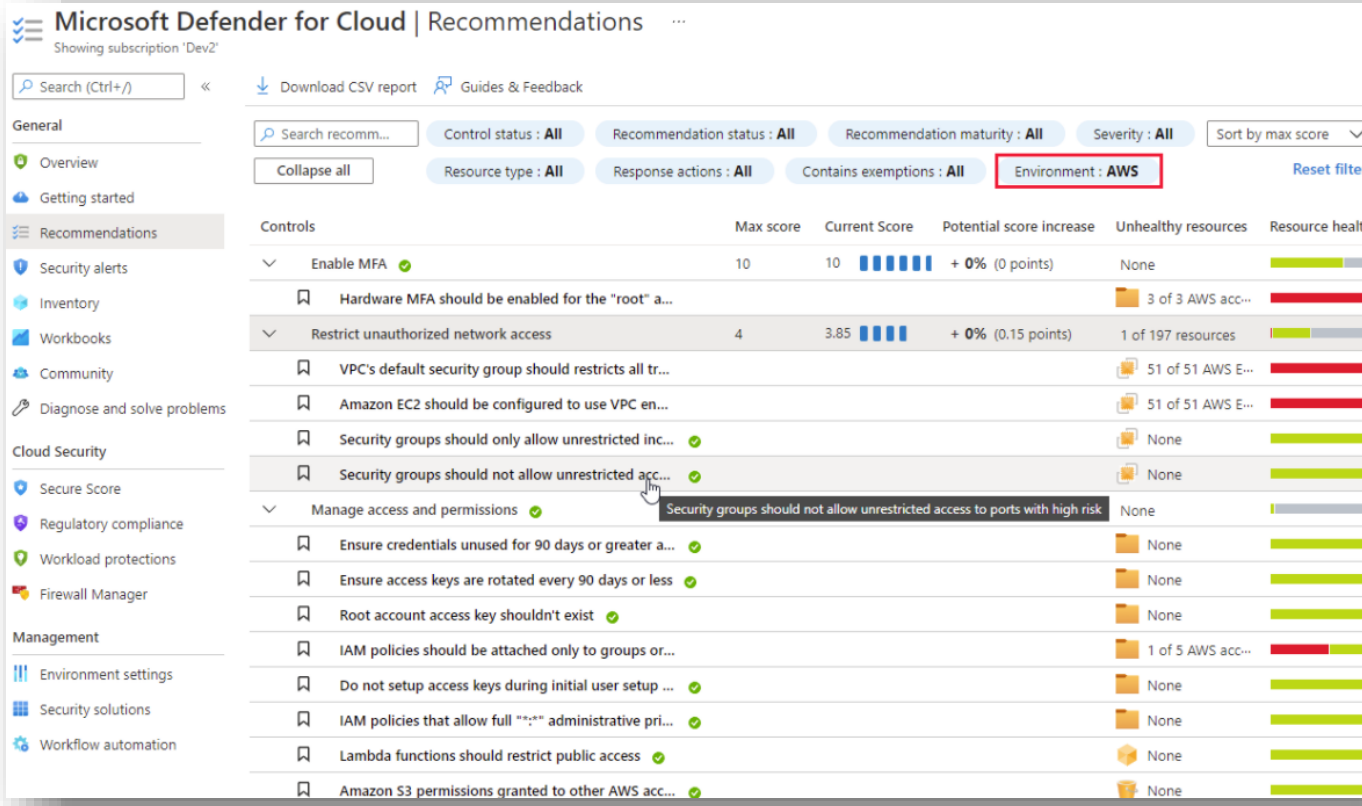
Connecting GCP projects

- Connect GCP projects on the project level granular onboarding
- Run the provided script to GCP Cloud Shell
- Defender plans are not dependent (e.g. enable CSPM only)



Security Recommendations

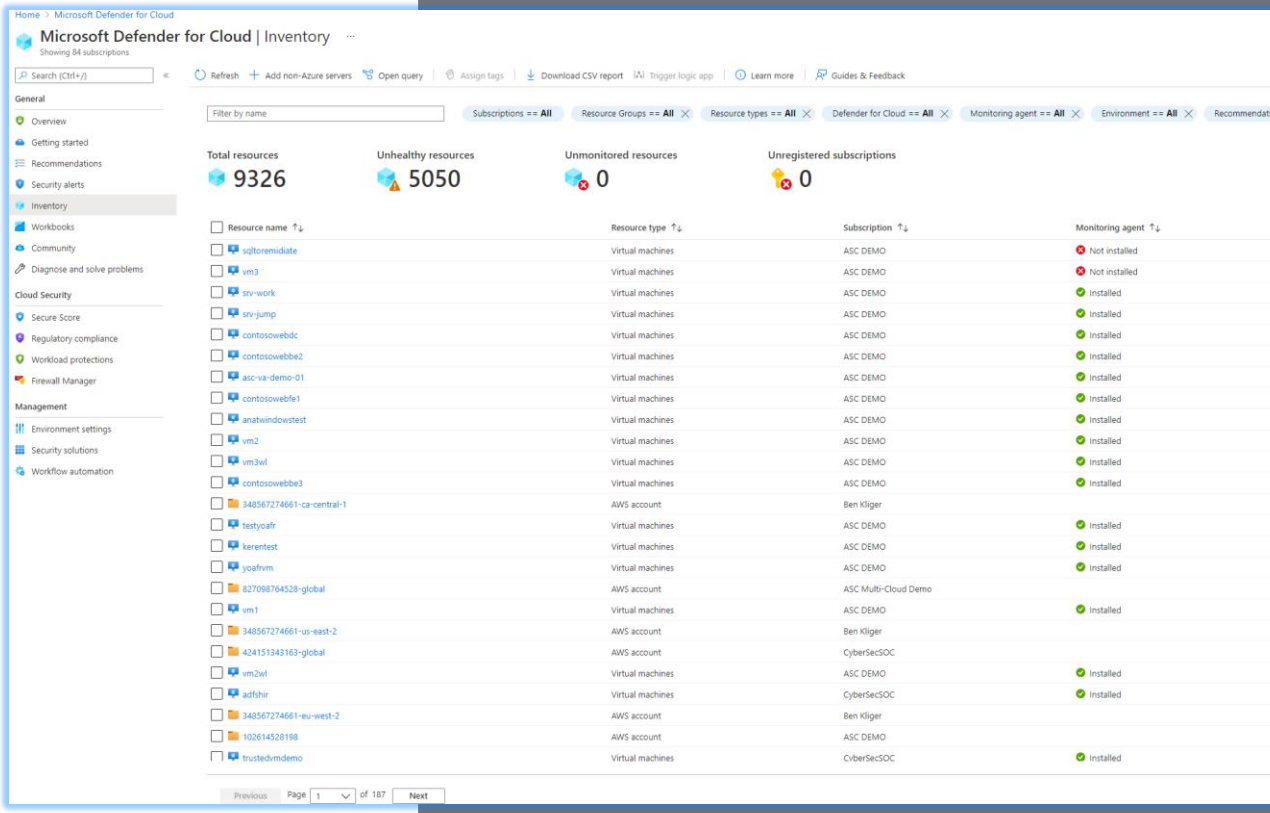
- API based
- Assessments' logic is built with KQL
- +160 out of the box security recommendations for AWS
- +130 out of the box security recommendations for GCP
- Covering +30 resource types
- 3 out of the box regulatory compliance standards (AWS CIS, AWS PCI DSS, AWS Foundational Security Best Practices)
- Built-in GCP CIS standard



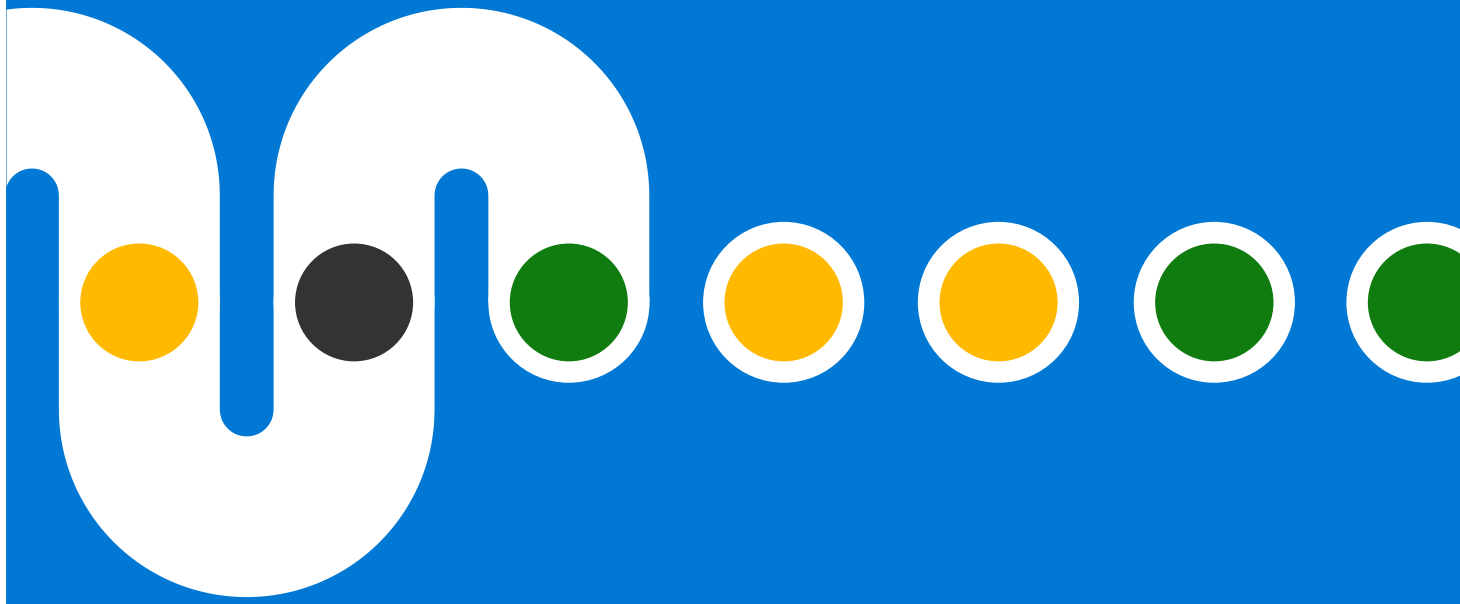
Inventory view

Improved visibility across the entire estate

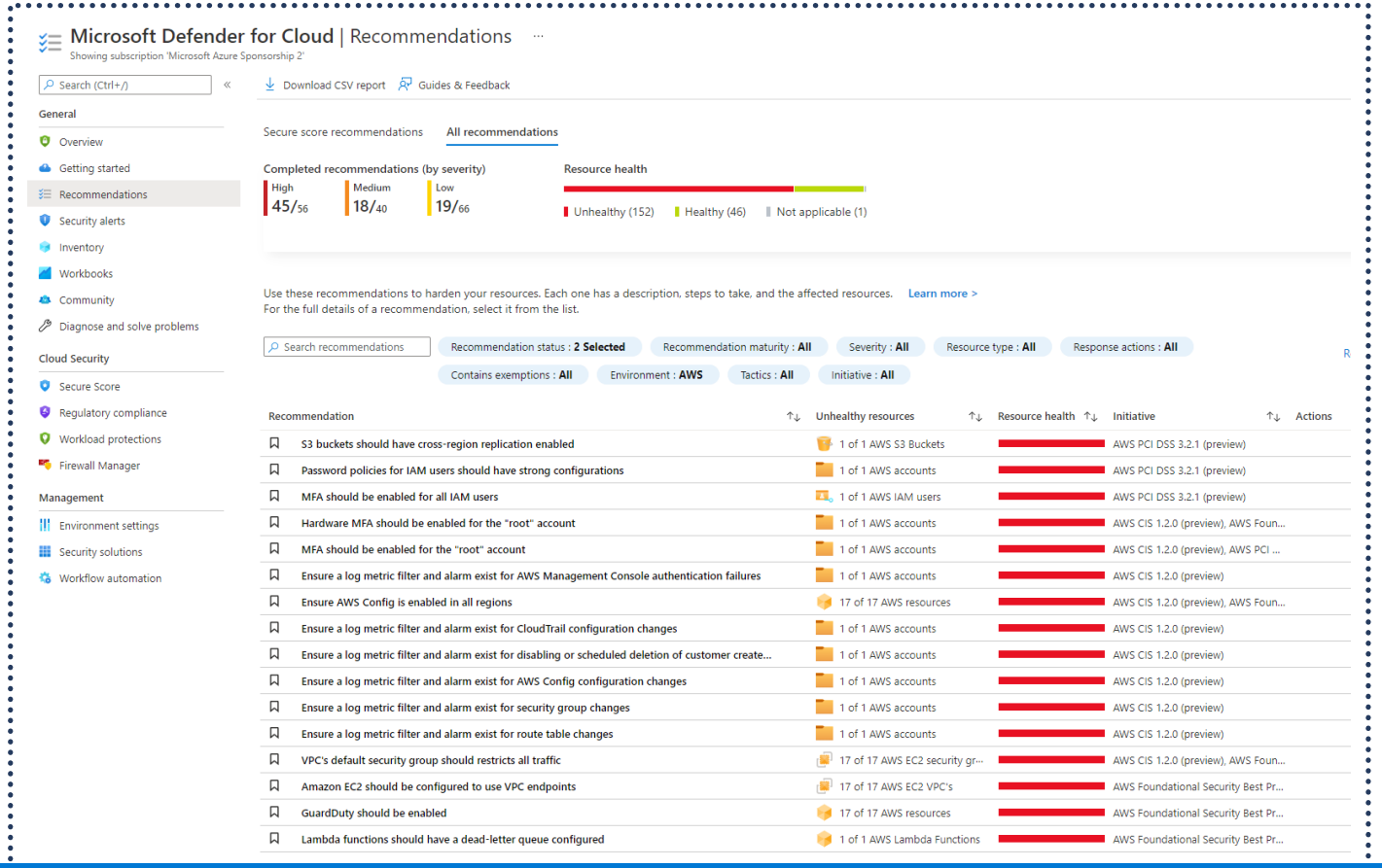
- Single view of all monitored resources
- Easy filtering, sorting and cross-referencing experience
- Continue exploration in Azure Resource Graph & export to CSV
- Management of resources



AWS Demo



Microsoft Defender for Cloud – AWS



Native AWS support using the AWS API

Policy management

Vulnerability management

Embedded Endpoint Detection and Response (EDR)

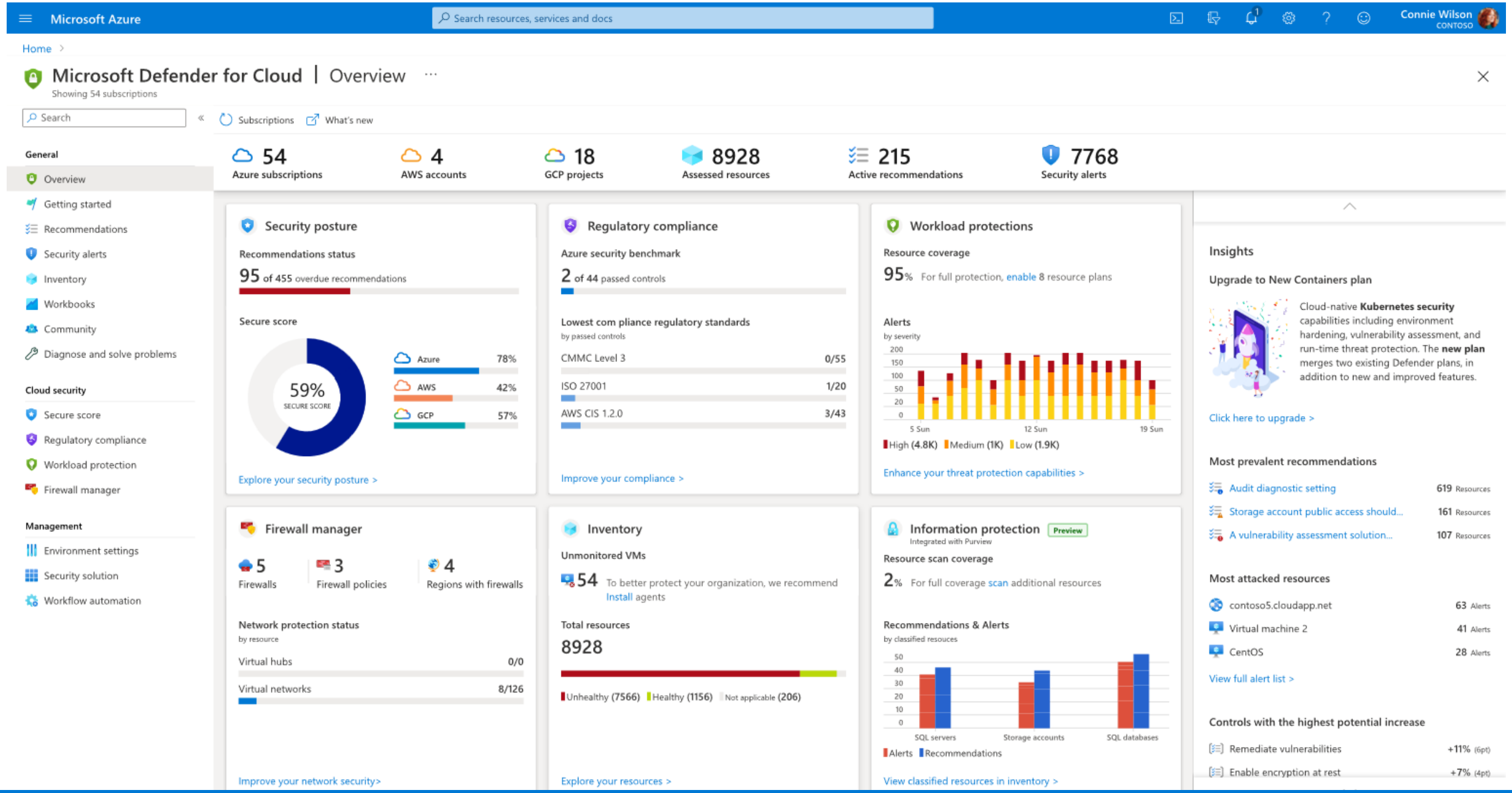
Detection of security misconfigurations

Protect Amazon EKS clusters and AWS EC2 workloads

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

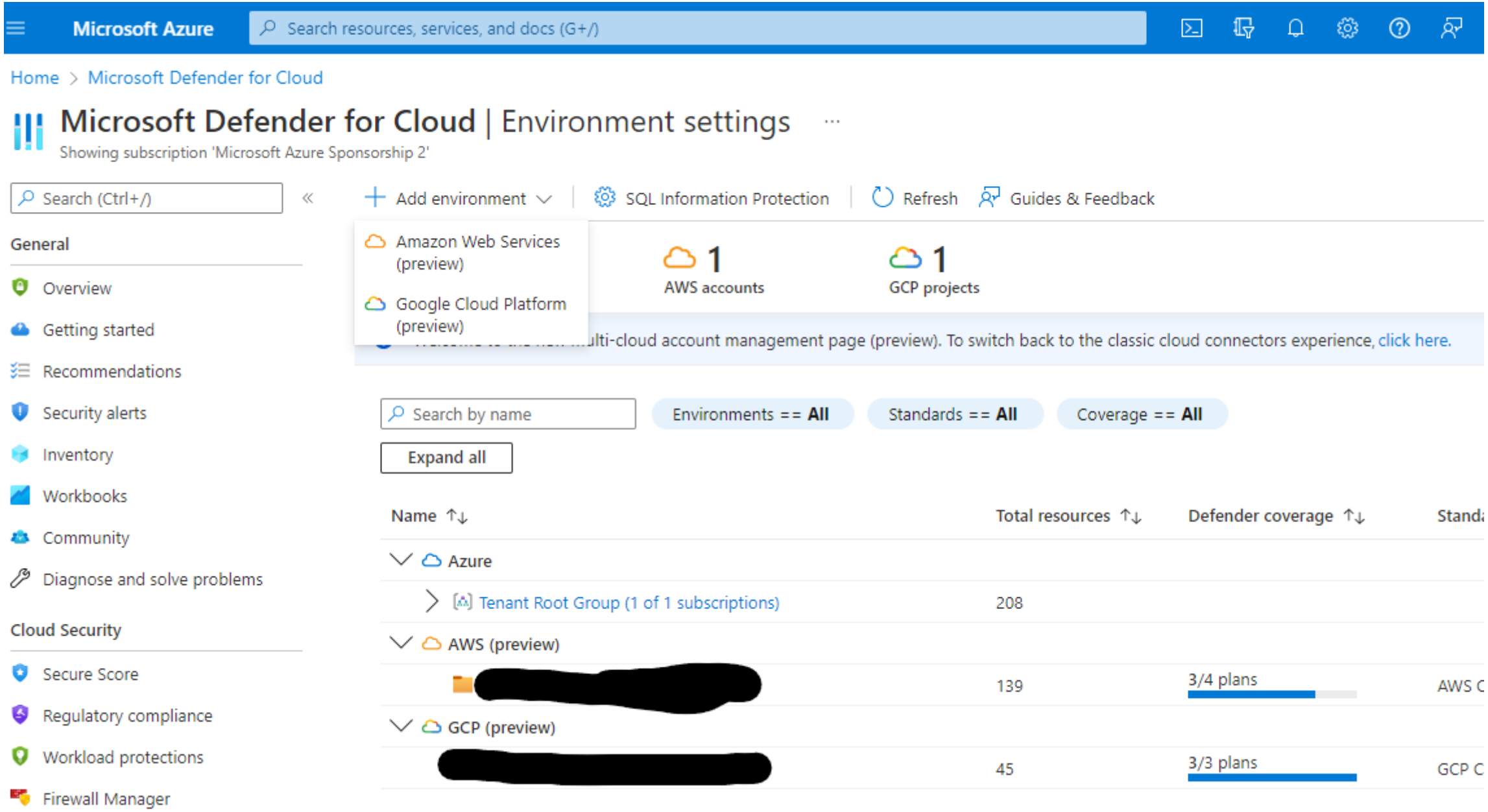
160+ out of the box recommendations, CIS, PCI & AWS Foundational Security Best Practices support

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

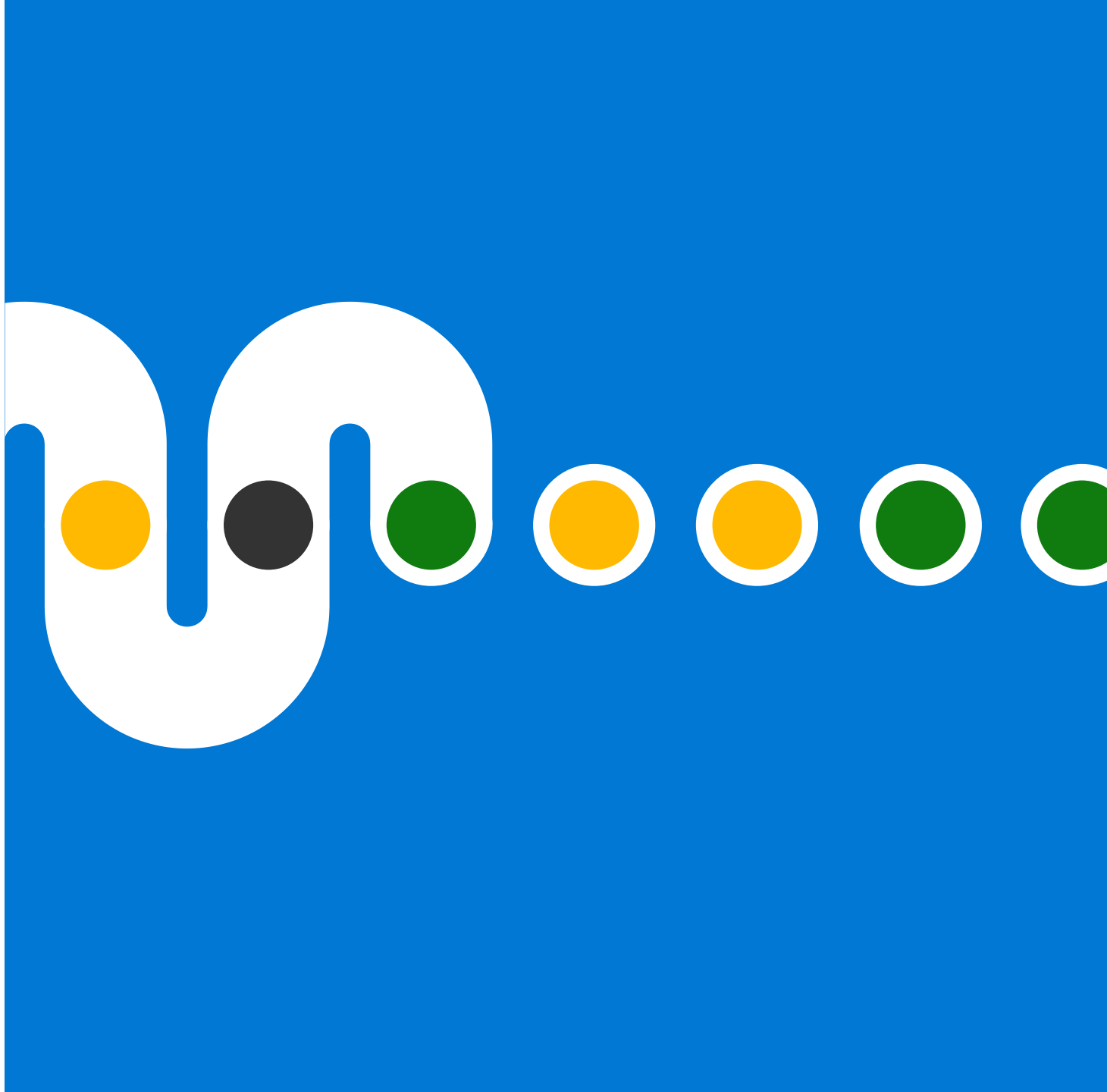


Microsoft Defender for Cloud dashboard

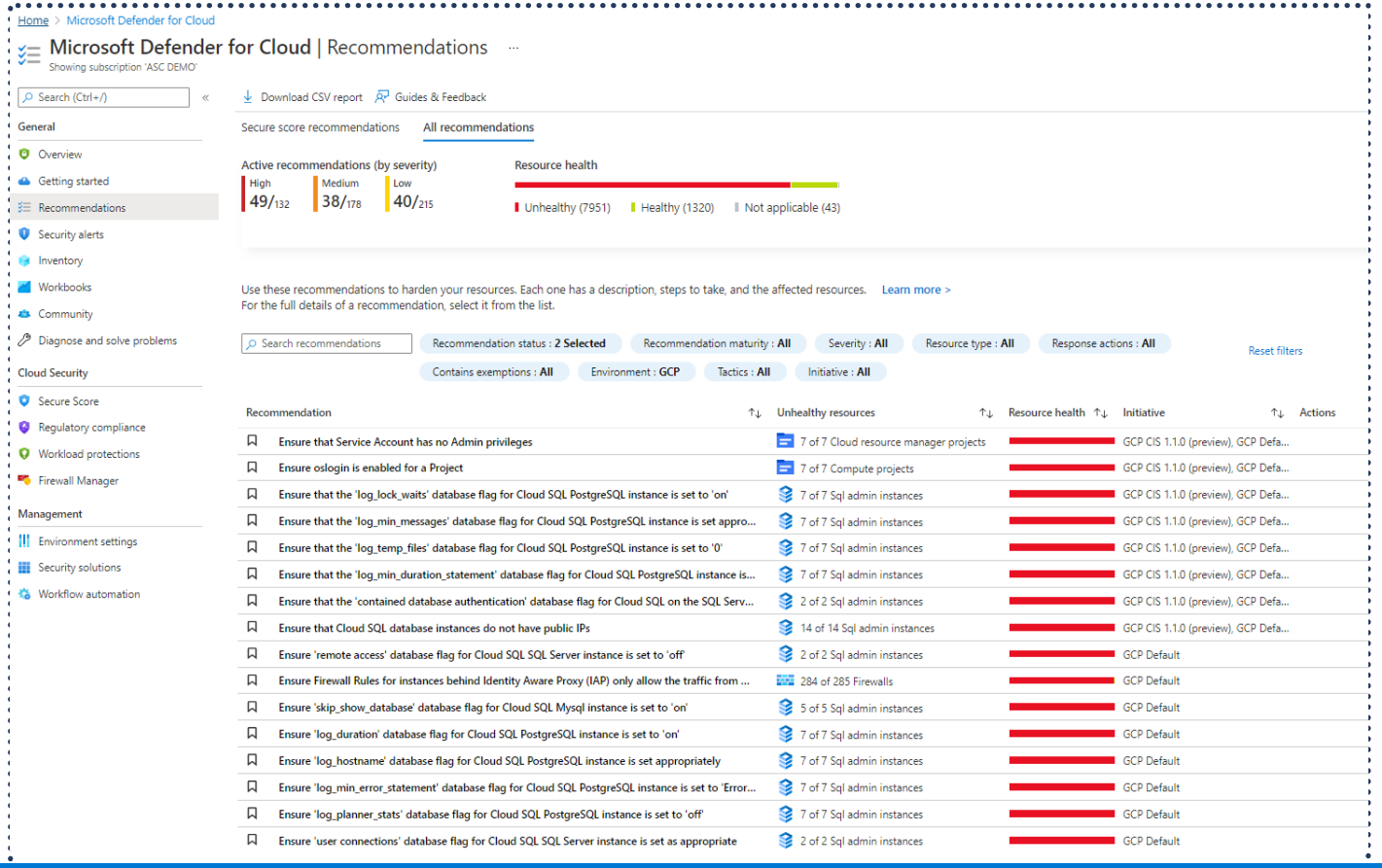
AWS – MDfC Environment Settings



GCP Demo



Microsoft Defender for Cloud – GCP



Native GCP support using the Google APIs

Policy management

Vulnerability management

Embedded Endpoint Detection and Response (EDR)

Detection of security misconfigurations

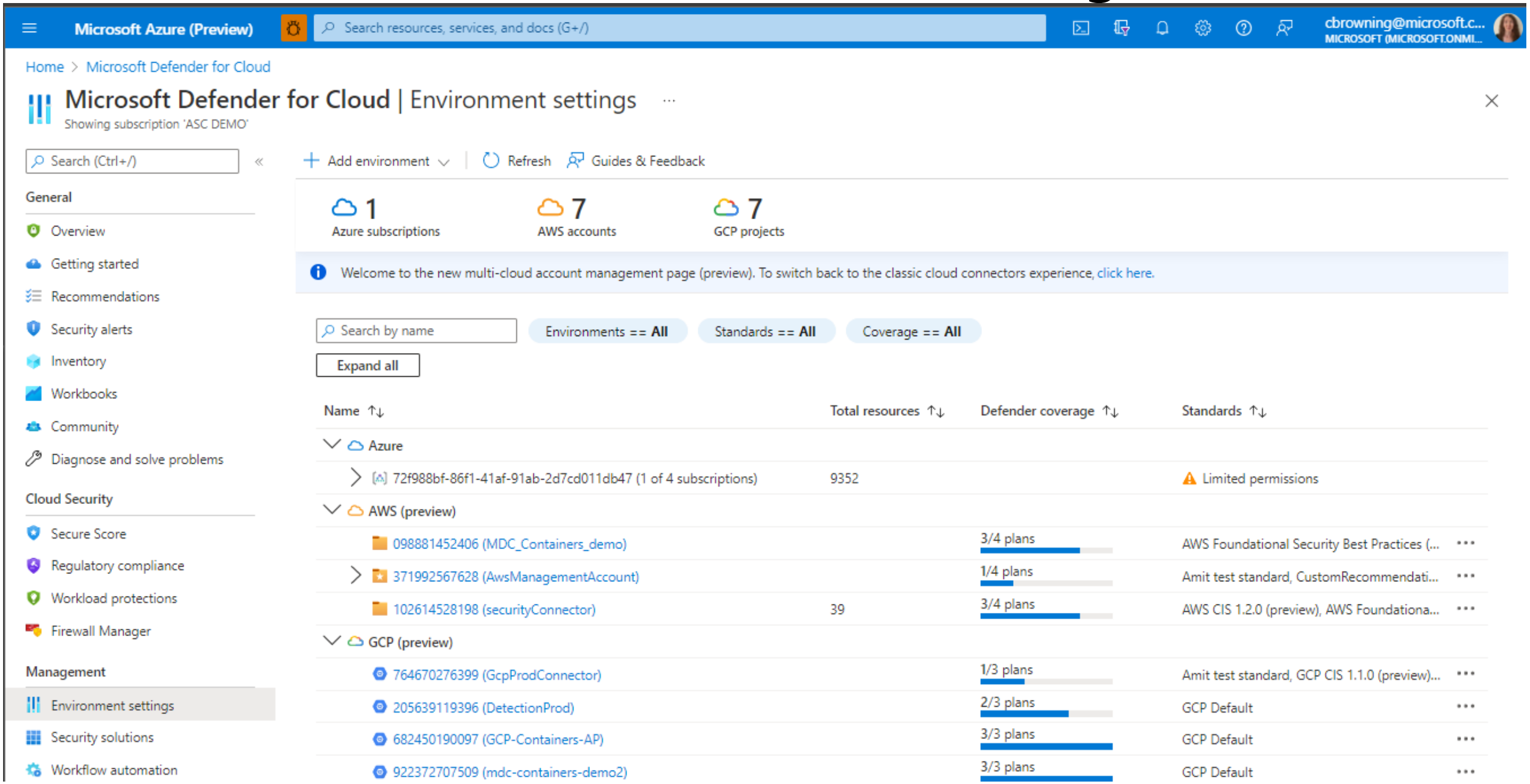
Protect Google GKE clusters and GCE workloads

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 – Environment settings



Learn more about new native AWS and GCP support

Check out the *Technical Community Articles*!

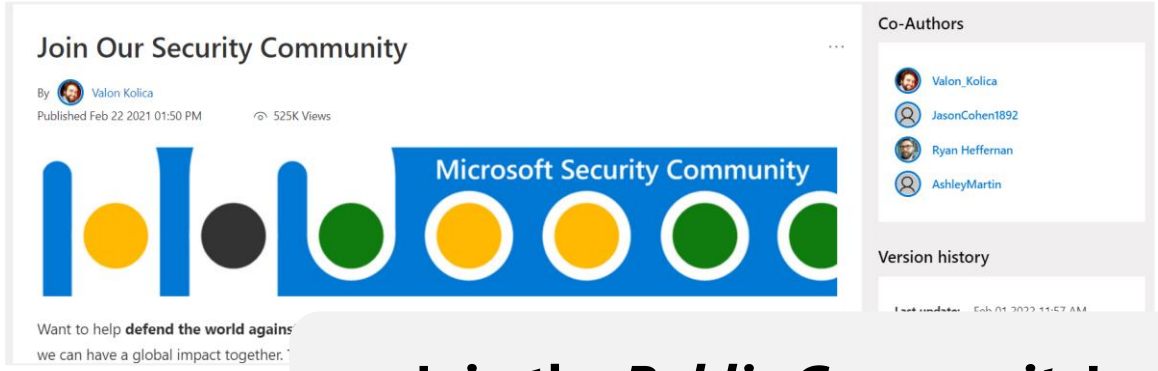
[Custom assessments and standards in Microsoft Defender for Cloud for GCP workloads (Preview) - Microsoft Tech Community]

[Custom assessments and standards in Microsoft Defender for Cloud for AWS workloads (Preview) - Microsoft Tech Community]

Need technical guidance?

[Connect your AWS account to Microsoft Defender for Cloud | Microsoft Docs]

[Connect your GCP project to Microsoft Defender for Cloud | Microsoft Docs]



Join the *Public Community*!

[https://aka.ms/SecurityCommunity]

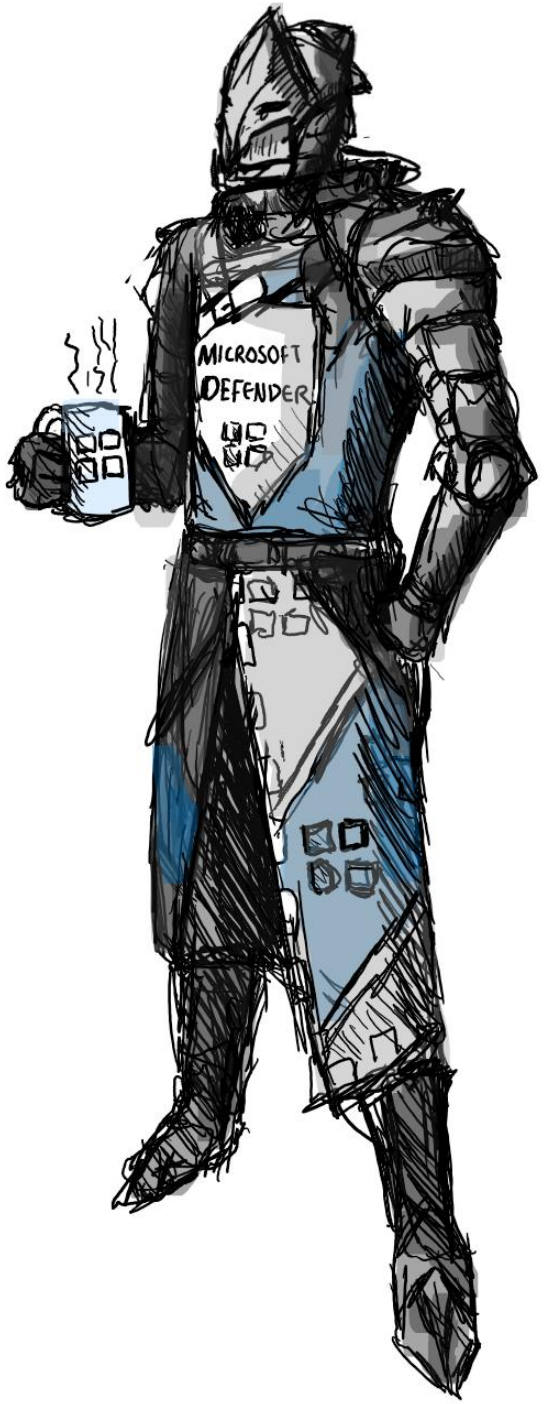
Check out short videos on how to set up the new connector!

[Connect AWS accounts to Defender Microsoft for Cloud – YouTube]

[Connect GCP accounts to Defender Microsoft for Cloud – YouTube]

Break

Please return at 14:25pm BST



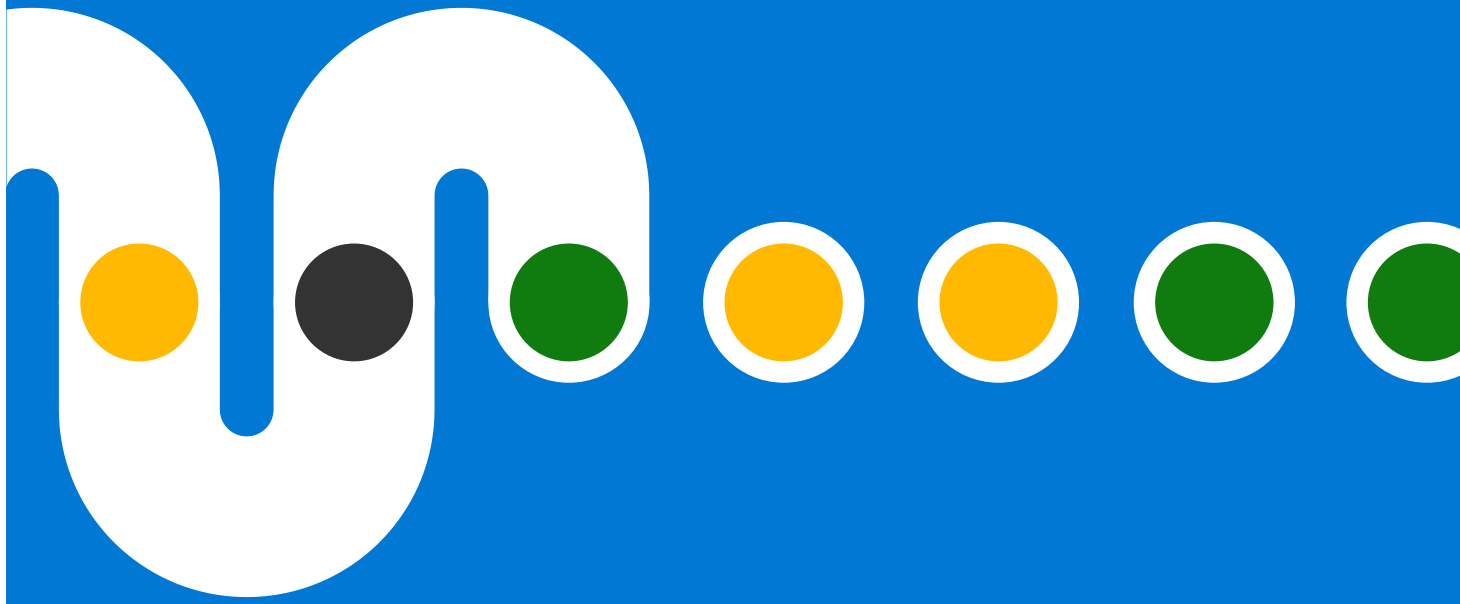
Please complete the poll if you haven't already

https://aka.ms/MDfCMasterclassP1-Poll

Microsoft Defender for Cloud

Regulatory Compliance across Azure, GCP, and AWS

Cassandra Browning and Liana Tomescu



Compliance management and assessment

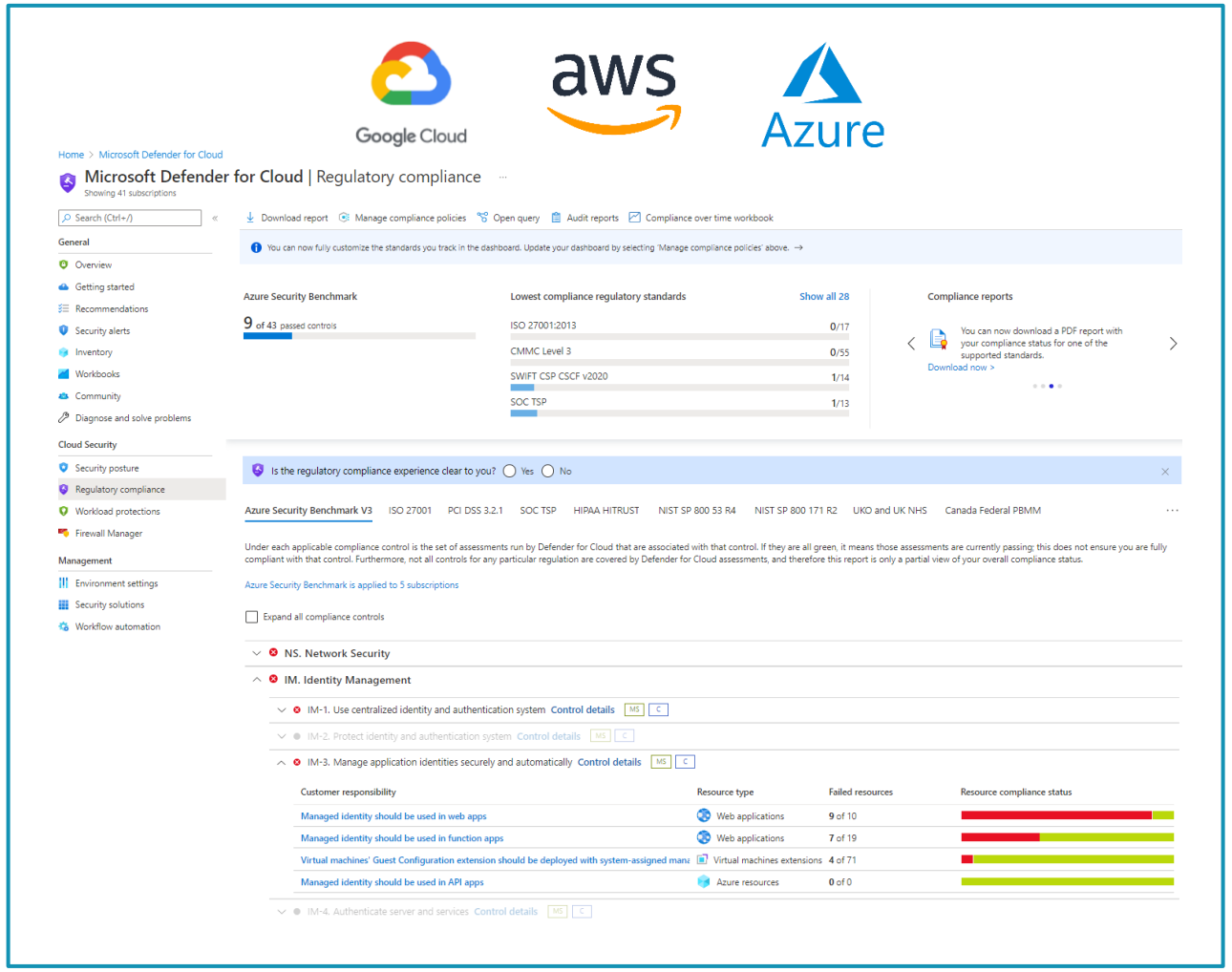
Demonstrate compliance status, based on continuous assessments of Azure resources

Monitor AWS and GCP resources with multi-cloud support

Azure Security Benchmark monitoring enabled by default, fully aligned with Secure Score

Support common industry standards, as well as custom initiatives based on Azure Policy

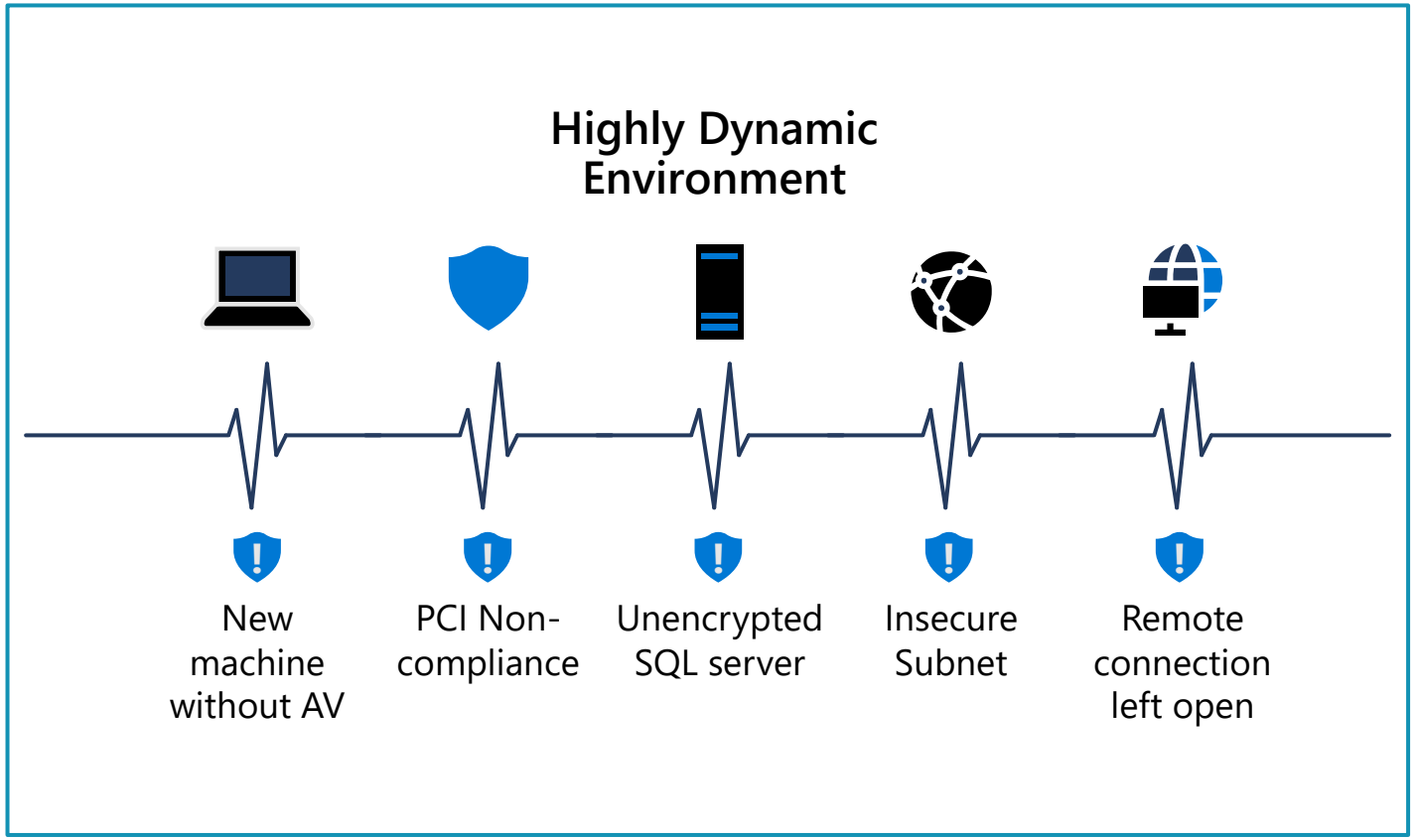
Overview of compliance status, compliance over time, and report download



Manage organizational security policies and assess compliance in minutes

Manage security policies at an organizational level

Easily set security policies for subscriptions or management groups

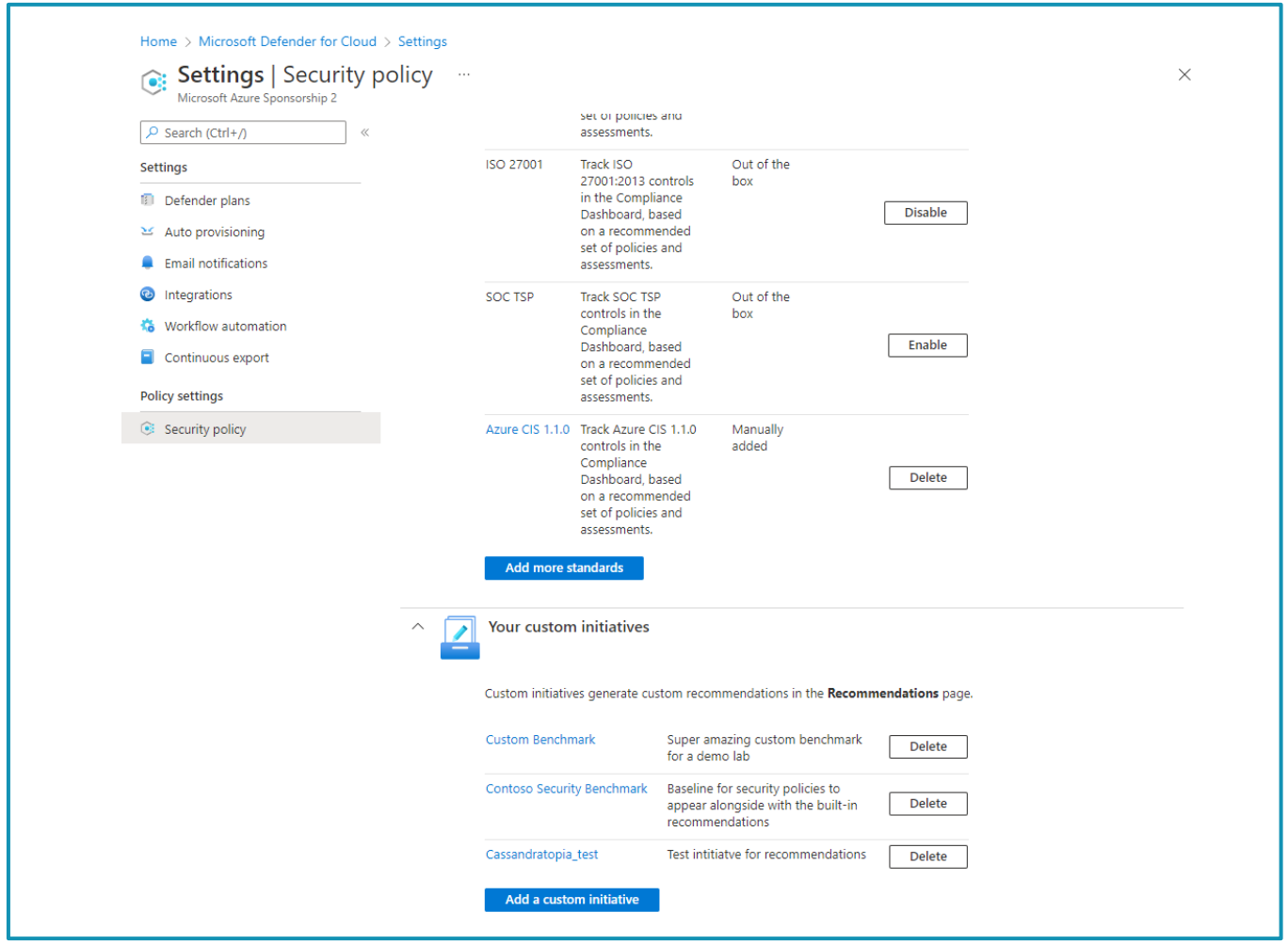


Editing security policies

You can edit security policies through the Azure Policy portal, Microsoft Defender for Cloud's Policy settings blade, via REST API or using Windows PowerShell

There are two specific Microsoft Defender for Cloud roles

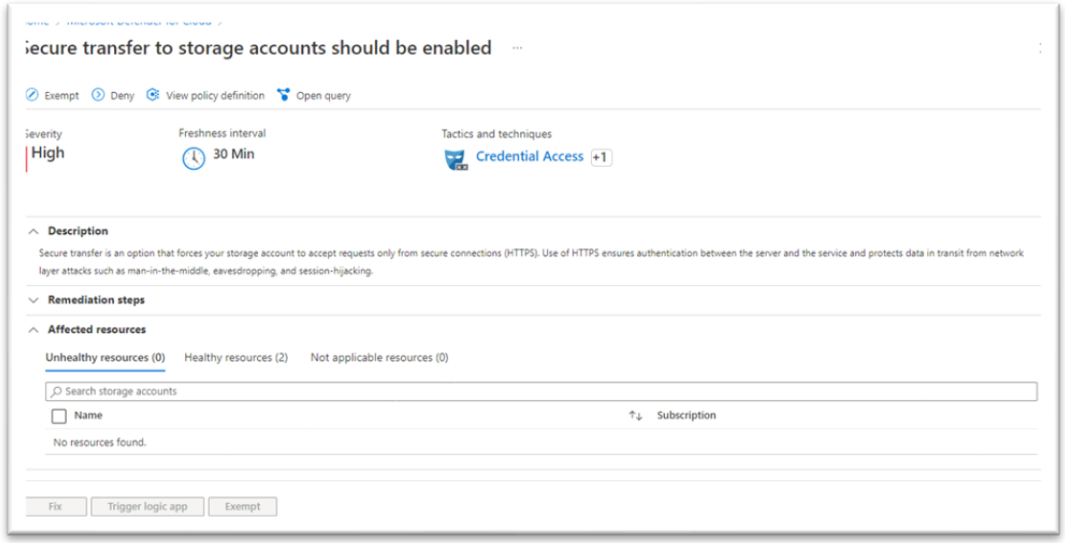
- Security reader
- Security admin

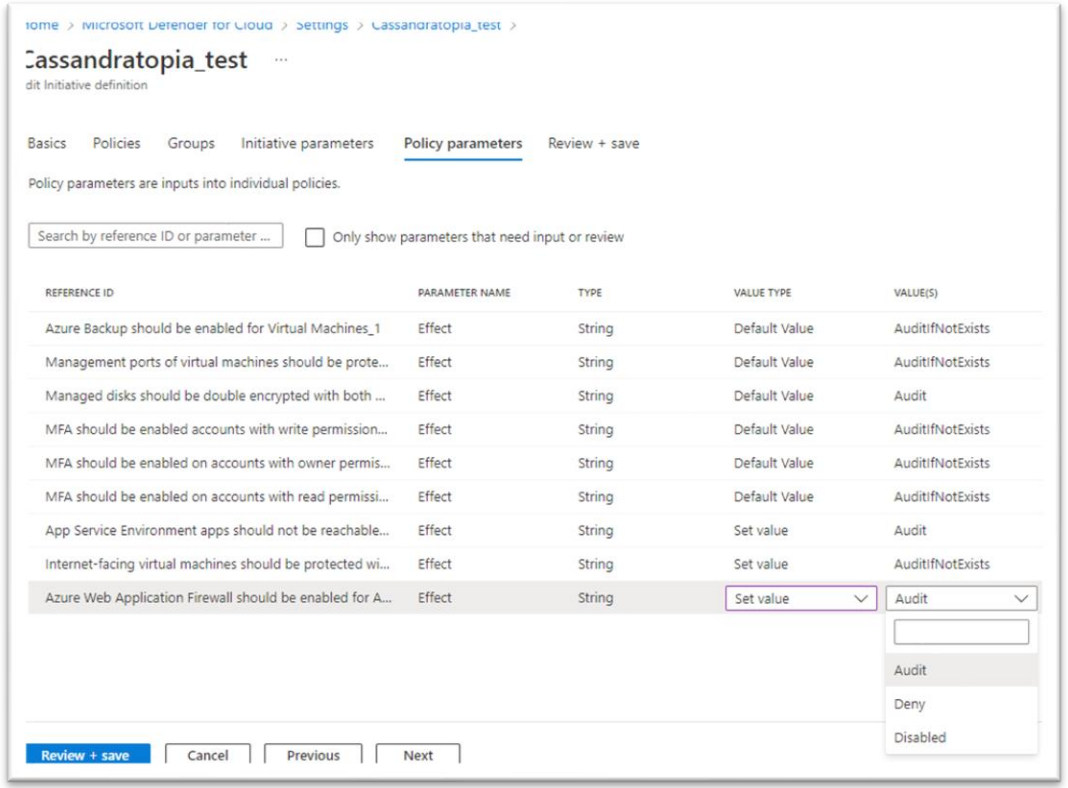


Preventing misconfigurations

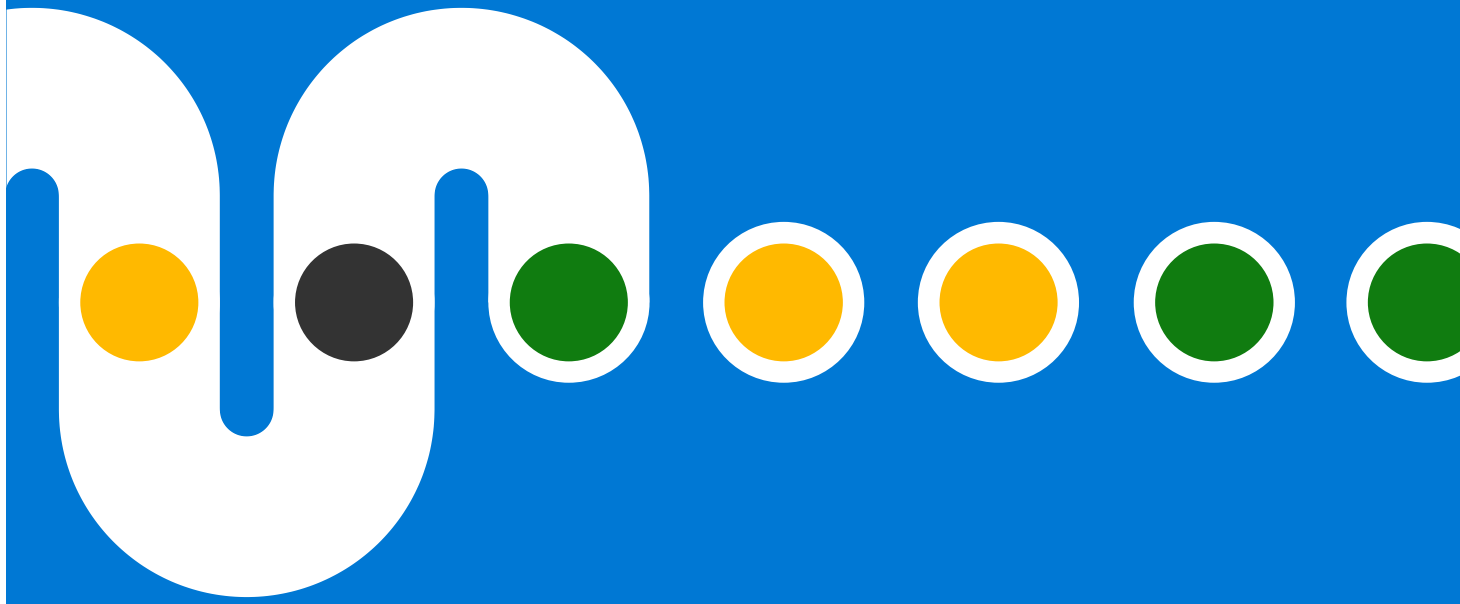
Using the **Deny** effect of Azure Policy, you can stop unhealthy resources from being created

Using the **Enforce** option, you can take advantage of Azure Policy's **DeployIfNotExist** effect and automatically remediate non-compliant resources upon creation

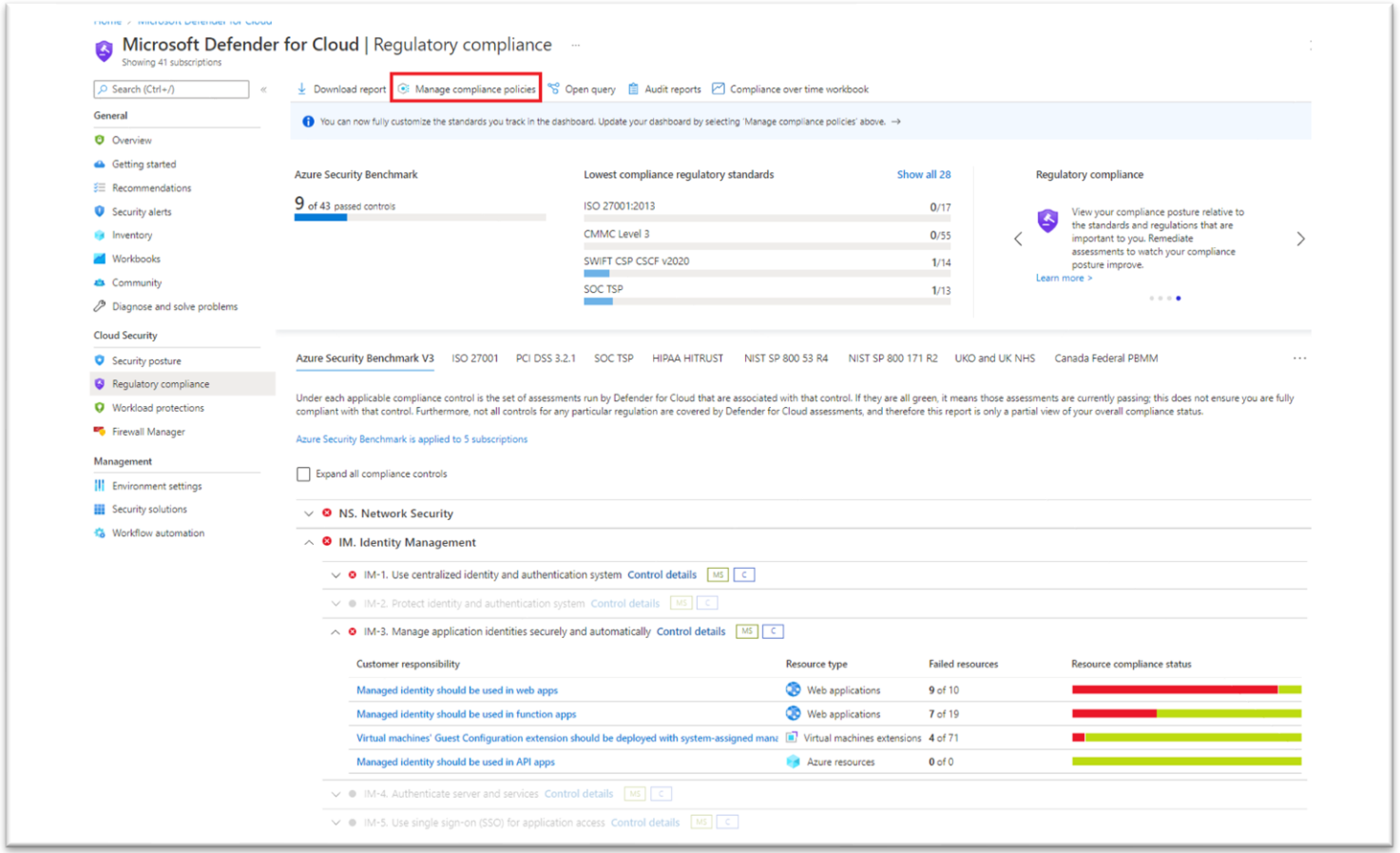




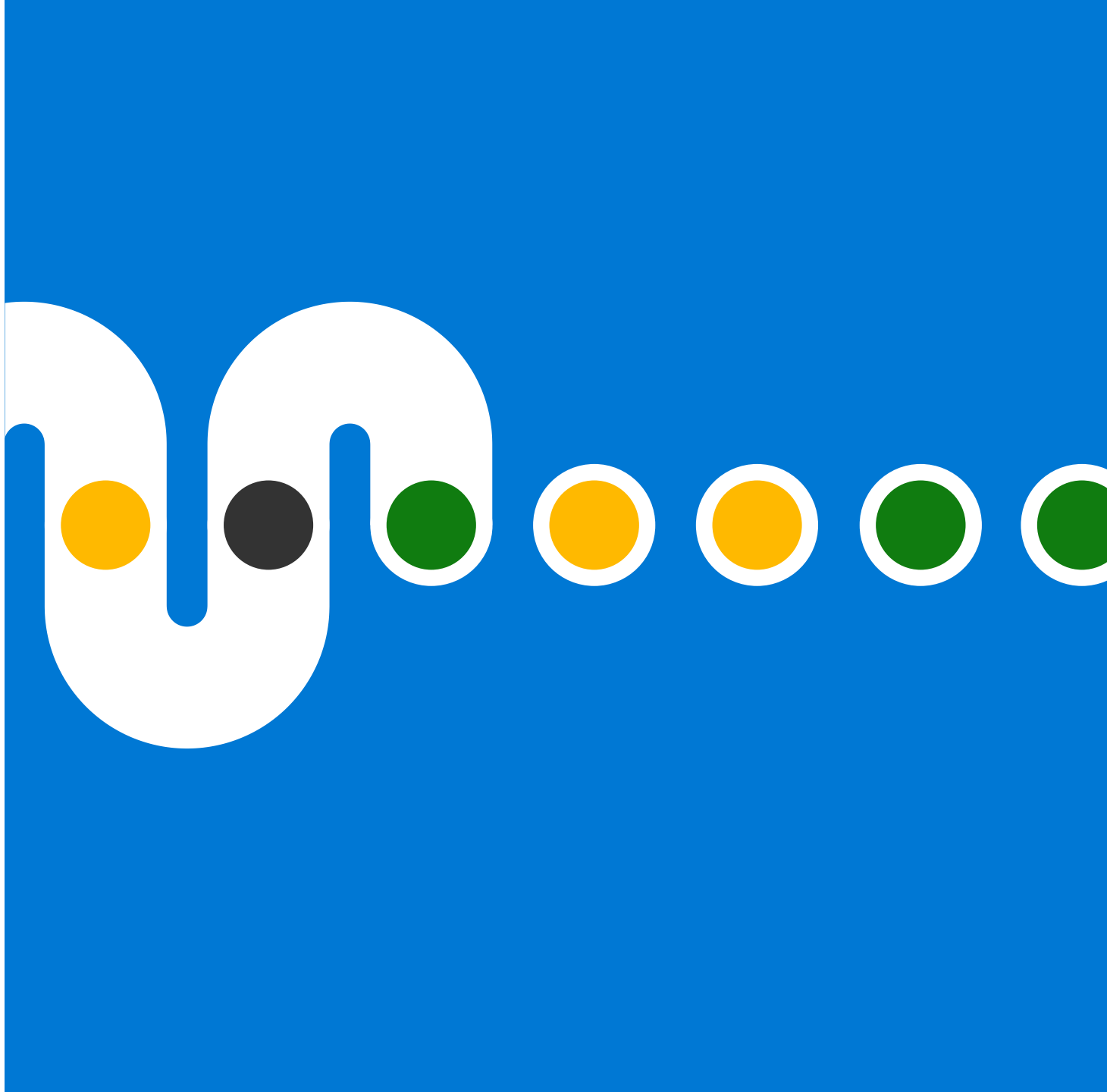
Azure Demo



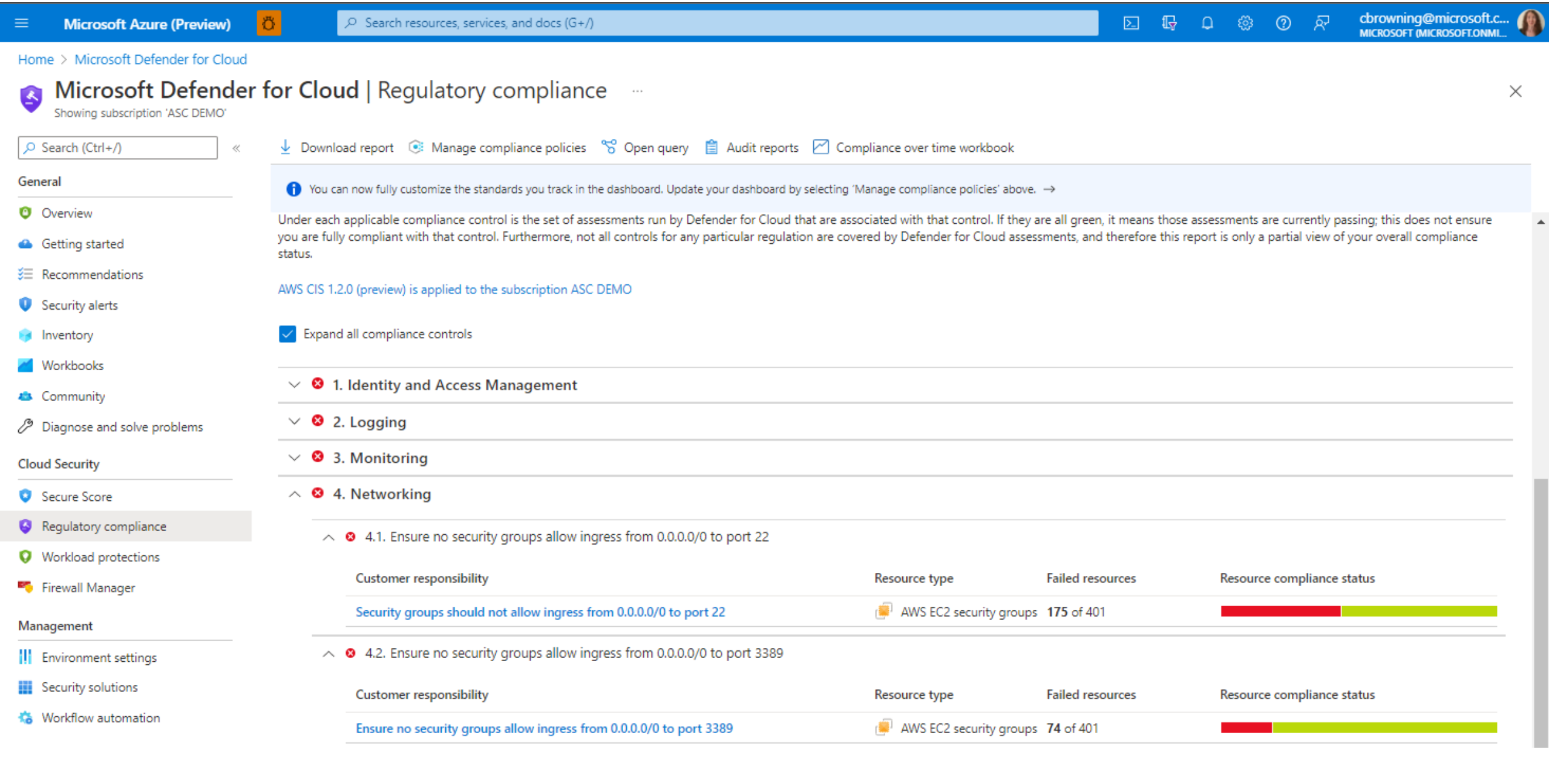
Regulatory Compliance Dashboard



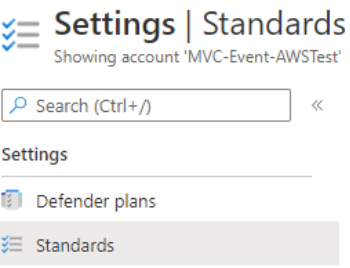
AWS and GCP Demo

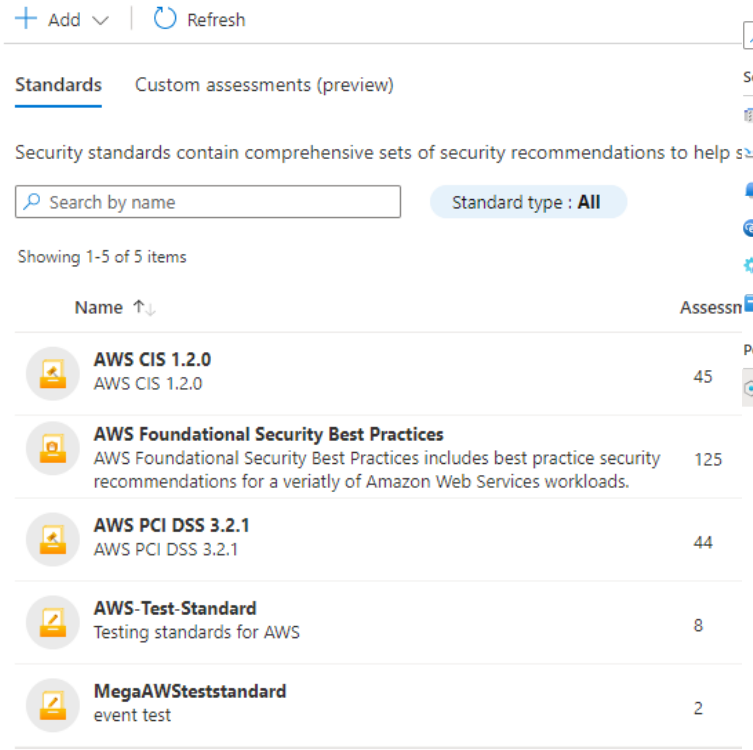


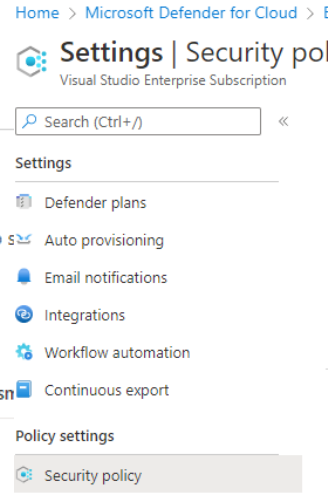
AWS – Regulatory Compliance

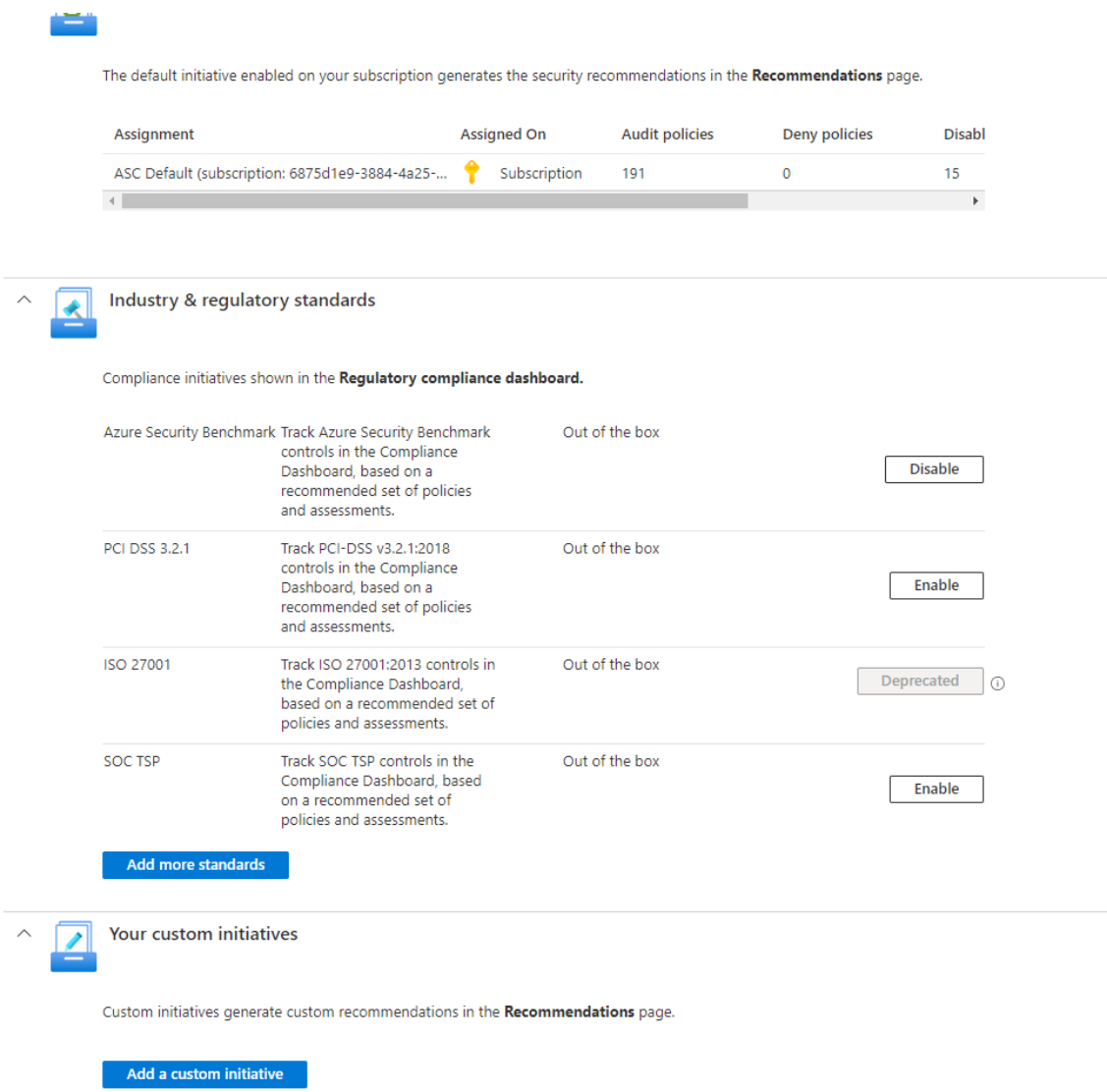


Azure vs. others



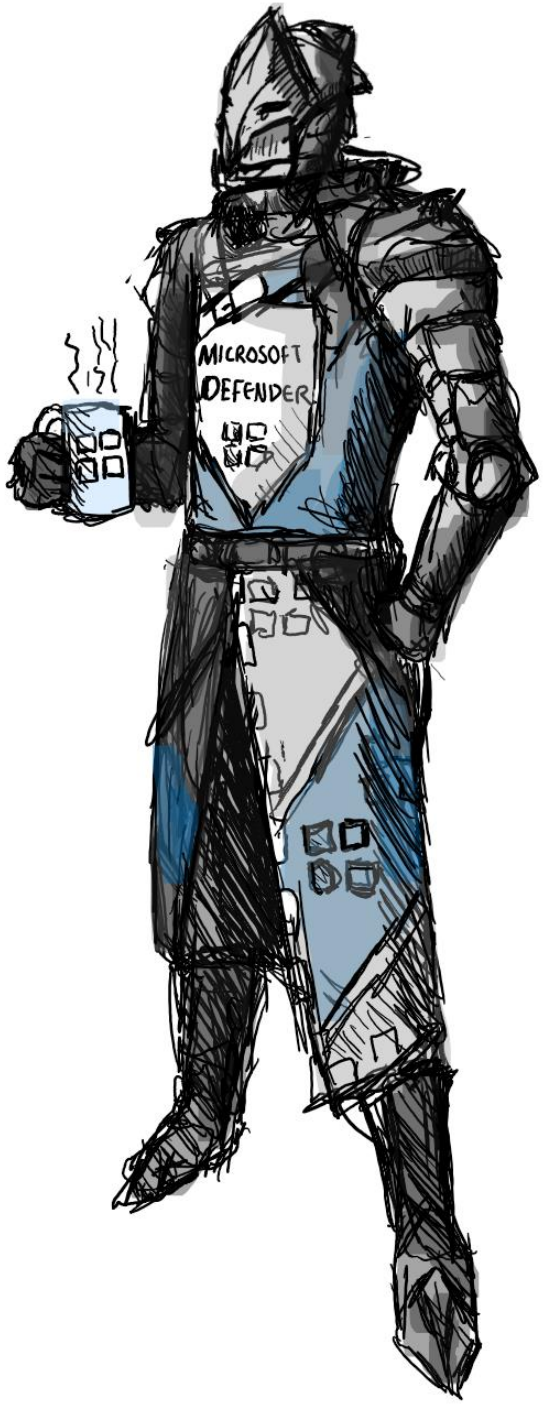






Break

Please return at 15:20pm BST



Please complete the poll if you haven't already

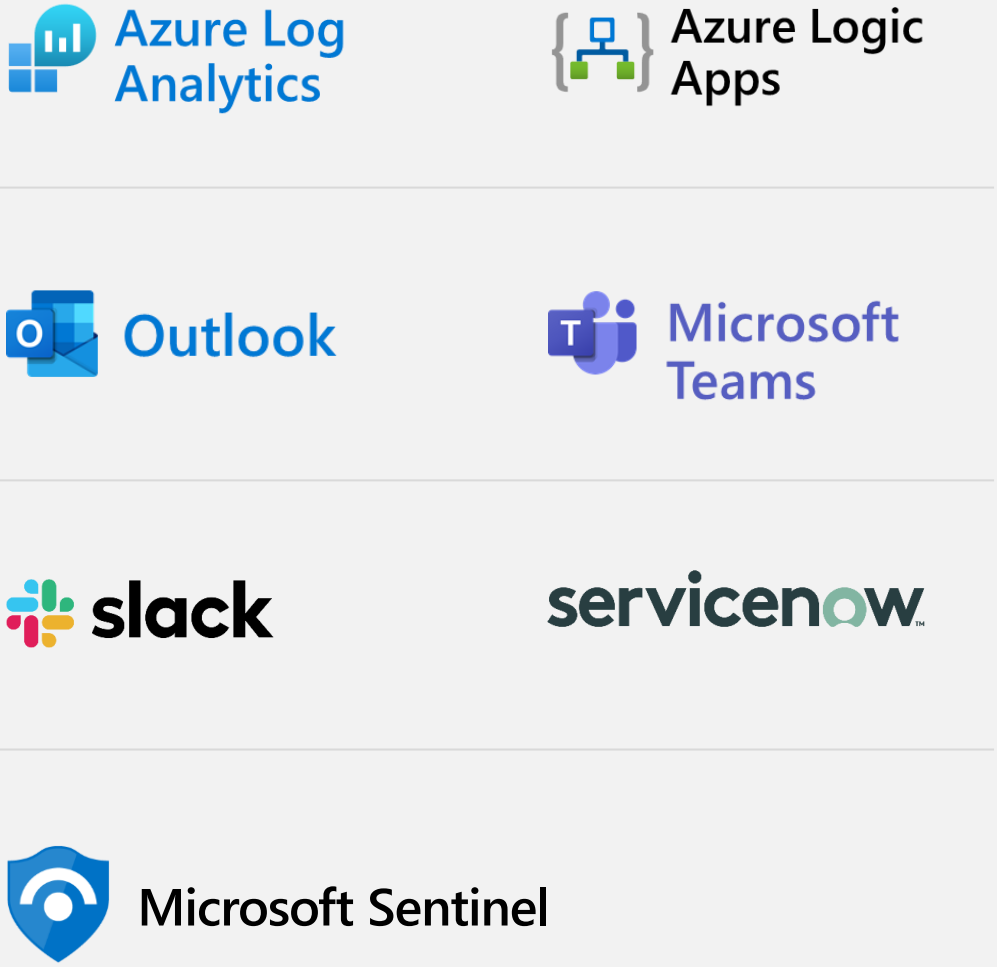
https://aka.ms/MDfCMasterclassP1-Poll

Automation in Microsoft Defender for Cloud

Tom Janetscheck

Respond and automate

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



Microsoft Security

Wrap Up

Labs and Demo Guidance

- **On-Demand Recording** - coming in the near future after this event
- **Slides & Labs** - http://aka.ms/MDfCMasterclassP1-repo

Resources to continue your training

- 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/mdfcinthefield
- Microsoft Security Community – http://aka.ms/SecurityCommunity
- Azure Arc Jumpstart – https://azurearcjumpstart.io/overview/
- Azure Lighthouse Deep Dive – https://www.youtube.com/watch?v=IrqkHOPFktM
- Must Learn KQL – http://aka.ms/mustlearnkql

Upcoming UK partner security events and training

	Event Title	Duration (Hours)	Date	Registration Link
Partner Webinars	Securing Multivendor Clouds – Part 3 – CIEM (CloudKnox)	2	23 June 2022, 1300-1600 BST	Register now, 1300 BST
	Days of the Defenders	2 days	September 2022	**IN–PERSON - TBC**

	Training Title	Duration (Hours)	Date	Registration Link
Training	Security Associate Certifications – 2022 Partner Challenge	6+	Now	Join the challenge now

Microsoft Security

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

Fundamental Certifications

Microsoft Security, Compliance, and Identity Fundamentals (SC-900)

Training includes
- 7 hours of Microsoft Learn content
- 8 hours of exam prep instructor training
- 1-day virtual training day

Associate Certifications

Microsoft Security Operations Analyst (SC-200)

Training includes
- 30 hours of Microsoft Learn content
- 10 hours of exam prep instructor training
- 4-day instructor-led training (English, Japanese, Chinese (Simplified), Korean)

Azure Security Engineer (AZ-500)

Training includes
- 32 hours of Microsoft Learn content
- 4-day instructor-led training (English, Japanese, Chinese (Simplified), Korean)

Microsoft Identity and Access Administrator (SC-300)

Training includes
- 12 hours of Microsoft Learn content
- 8 hours of exam prep instructor training
- 4-day instructor-led training (English, Japanese, Chinese (Simplified), Korean)

Microsoft 365 Security Administrator Associate (MS-500)

Training includes
- 14 hours of Microsoft Learn content
- 10 hours of exam prep instructor training
- 4-day instructor-led training (English)

Microsoft Information Protection Administrator (SC-400)

Training includes
- 10 hours of Microsoft Learn content
- 8 hours of exam prep instructor training
- 2-days of instructor-led training (English, Japanese, Chinese (Simplified), Korean)

*Azure Network Engineer Associate (AZ-700)

Training includes
- 10 hours of Microsoft Learn content
- *Exam prep instructor training not available*

Expert Certifications

Microsoft Cyber Security Architect (SC-100)

Training includes
- 30 hours of Microsoft Learn content
- *Exam prep instructor training not available*

- Go here for the latest certification roadmap **Microsoft training and certifications**.

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.

Microsoft

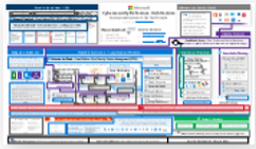
Microsoft Cybersecurity Reference Architectures

The Microsoft Cybersecurity Reference Architectures (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 and download the file here

Capabilities

What cybersecurity capabilities does Microsoft have?



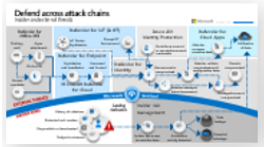
Build Slide

Azure Native Controls

What native security is available?

Attack Chain Coverage

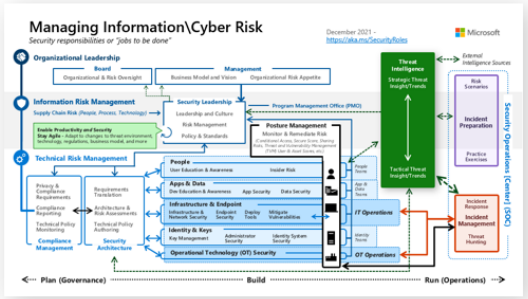
How does this map to insider and external attacks?



Build Slide

People

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



Multi-Cloud & Cross-Platform

What clouds & platforms does Microsoft protect?

Secure Access Service Edge (SASE)

What is it? How does it compare to Zero Trust?

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. Help decide the deep dive content for Part 2 and beyond!

https://aka.ms/MDfCMasterclassP1-Feedback

Thank you!

Feedback:
https://aka.ms/MDfCMasterclassP1-Feedback