

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



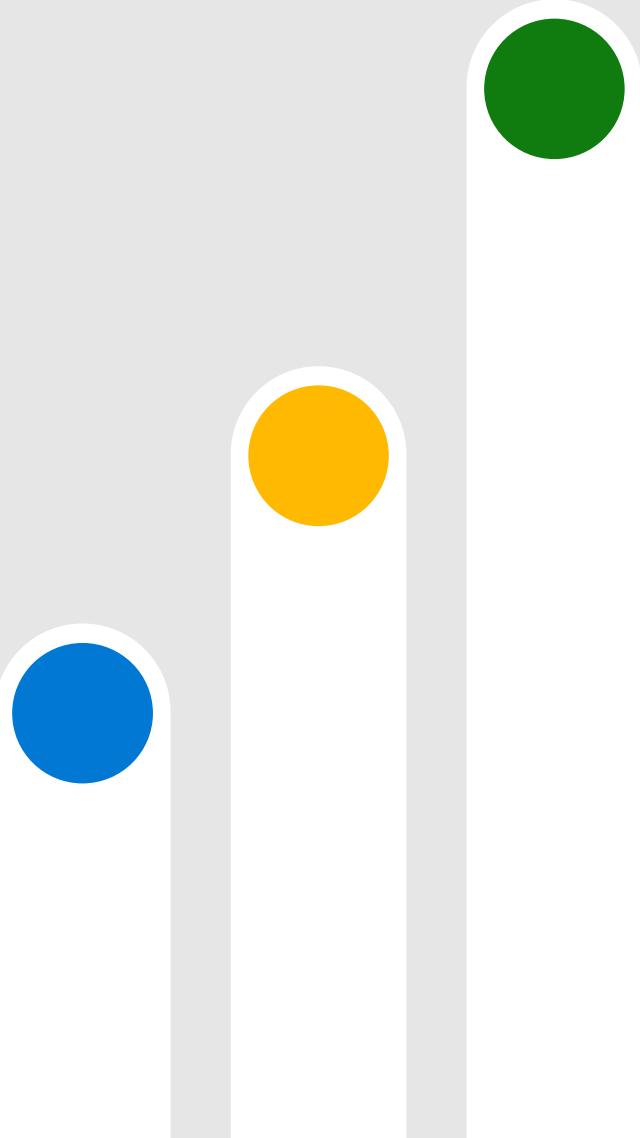
Bojan Magusic
Program Manager
Defender for Cloud



Tom Janetscheck
Senior Program Manager
Defender for Cloud
Engineering



Liana Tomescu
Program Manager
Defender for Cloud



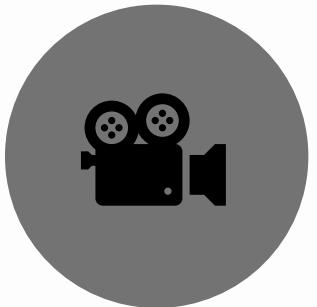
Housekeeping



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



<https://aka.ms/MDFCMasterclassP1-Feedback>



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



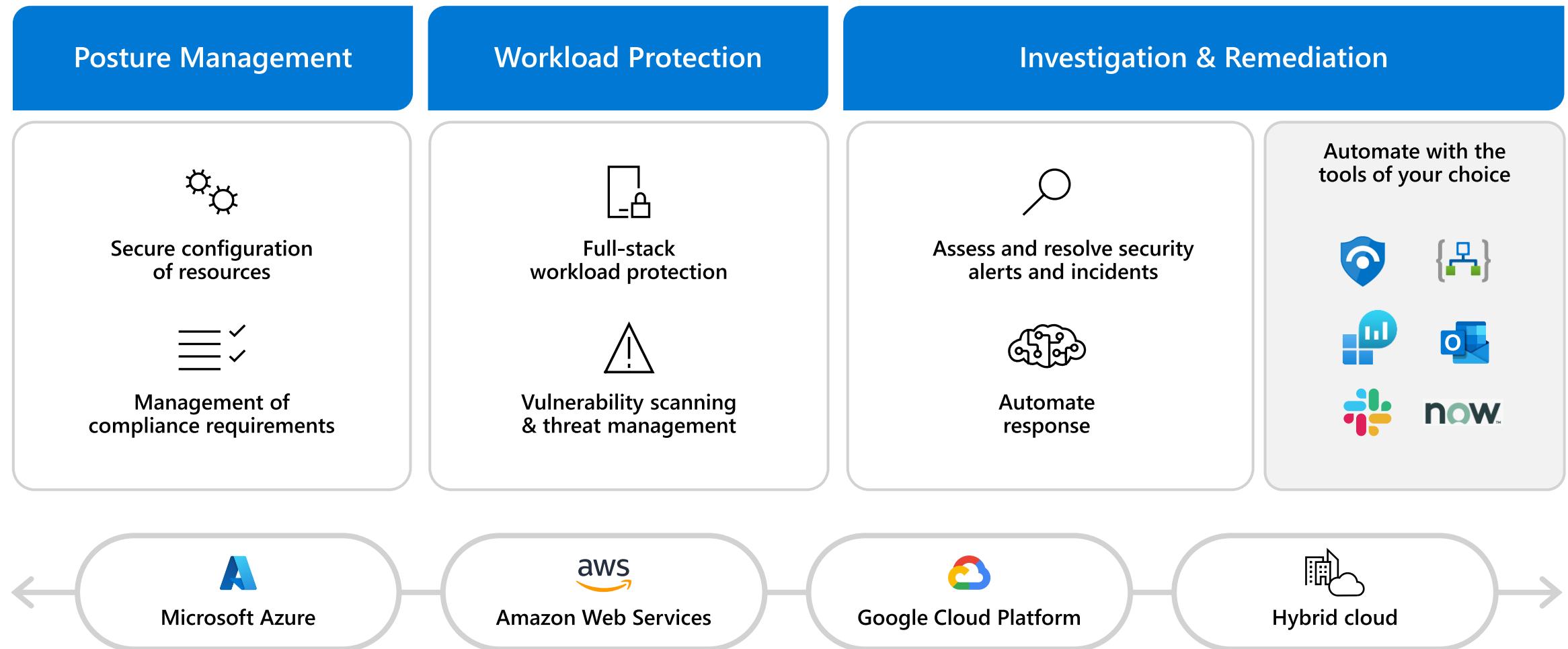
All content is under your partnership NDA



Microsoft Defender for Cloud Overview

Cassandra Browning

Microsoft Defender for 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

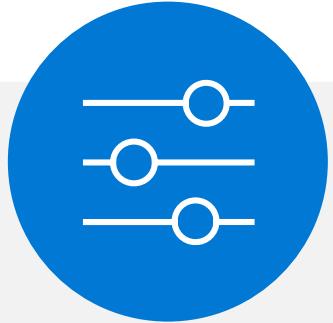
- Deterministic, AI, and anomaly-based detection mechanism
- Leverages the power of Microsoft Threat Intelligence



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](#)

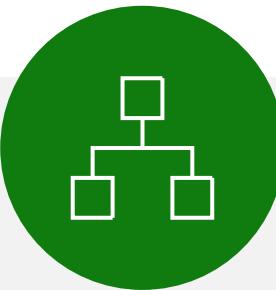
<https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report> (p.124)

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



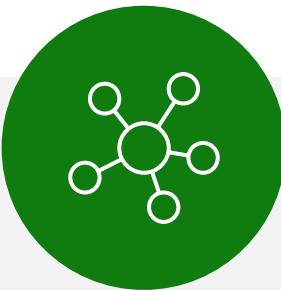
Leading threat intelligence

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

AWS workloads



Amazon EKS



Amazon EC2

GCP workloads



GKE clusters



Google Compute

Databases and Storage



Blob storage



File storage



Maria DB



Azure Cosmos DB



Azure SQL



MySQL



Postgres SQL



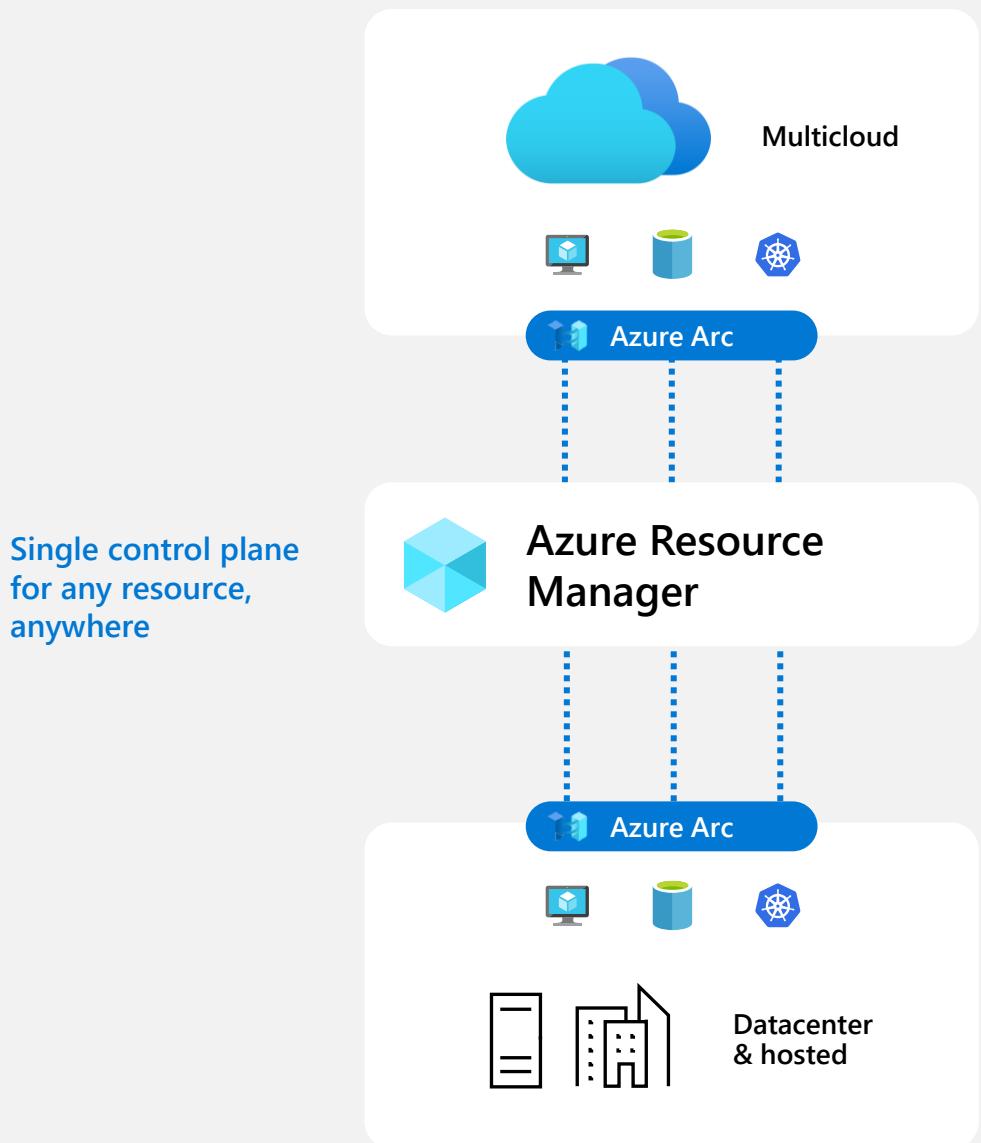
Multicloud and hybrid protection

- 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	

Azure Resource Manager (ARM)

Access and Security

RBAC | MSPs | Subscriptions

Environments and Automation

Templates | Extensions

Organization and Inventory

Search | Index | Groups | Tags

Governance and Compliance

Logs | Policy | Blueprints

Azure Resources

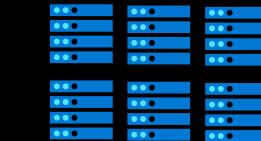


Microsoft Azure

Azure Arc

aws
ORACLE
Multi-Cloud

Google Cloud
IBM Cloud



On-Premises / Hosted Services

Customer Environments

Existing Tools

Azure Data Studio
Kubernetes Tools
Server Admin Tools

Microsoft Defender for Servers

Threat protection for servers

Protect Linux, Windows, EC2, and Google Compute

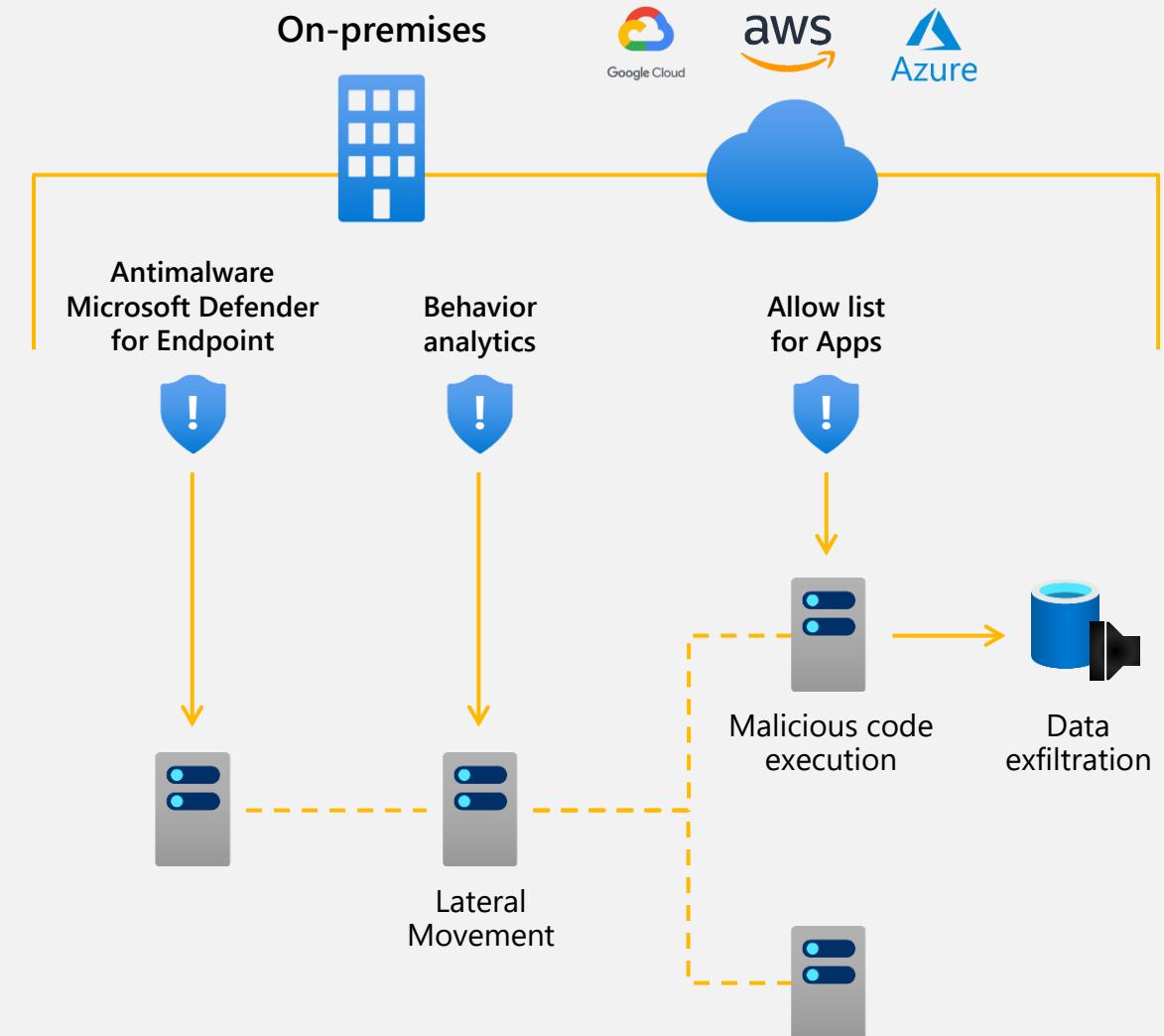
Reduce open network ports (Azure)

- 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.



The screenshot shows a Microsoft Azure Defender for Cloud interface. At the top, it says "Vulnerabilities in your virtual machines should be remediated". Below this, there are filters for "Exempt", "Disable rule", "View policy definition", and "Open query". The main area displays a table of findings:

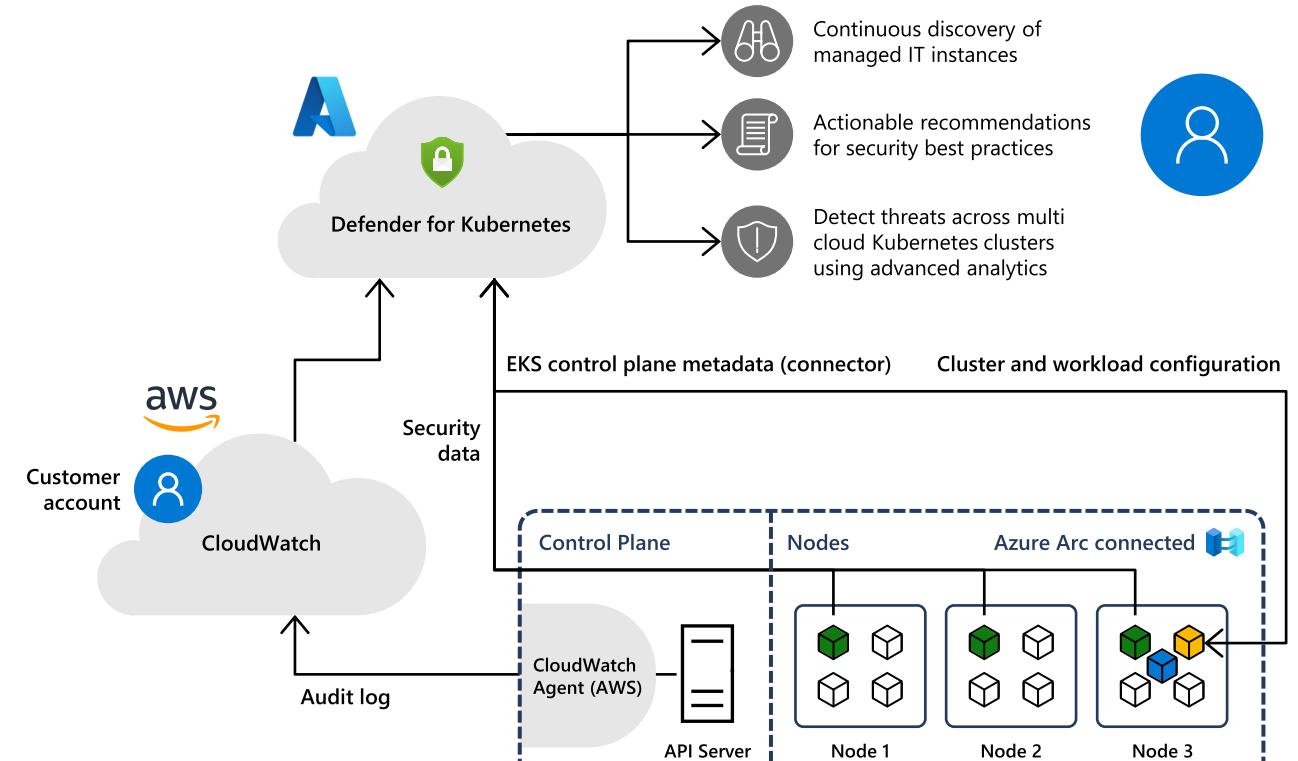
ID	Security check	Category	Applies to	Severity
105977	EOL/Obsolete Operating System: Ubuntu 16.04 Detected	Security Policy	2 of 13 resources	High
100410	Microsoft Internet Explorer Security Update for September 2020	Internet Explorer	2 of 13 resources	High
91674	Microsoft Windows Security Update for September 2020	Windows	2 of 13 resources	High
91462	Microsoft Windows Security Update Registry Key Configuration	Windows	1 of 13 resources	High
178369	Debian Security Update for tzdata (DLA 2424-1)	Debian	1 of 13 resources	High
178418	Debian Security Update for screen (DLA 2570-1)	Debian	1 of 13 resources	High
374891	Sudo Heap-based Buffer Overflow Vulnerability (Baron Samedi...)	Local	1 of 13 resources	High
177442	Debian Security Update for file (DSA 4550-1)	Debian	1 of 13 resources	High

At the bottom left are buttons for "Trigger logic app" and "Exempt".

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

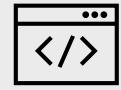


[Microsoft Defender for Containers feature availability](#)
| Microsoft Docs

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



3 Use the client experience tool of your choice



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



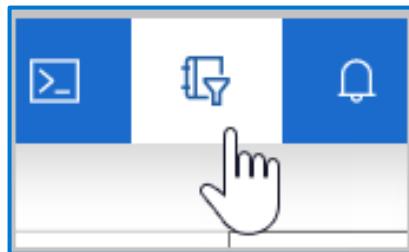
Adopt cloud practices on-premises



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



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

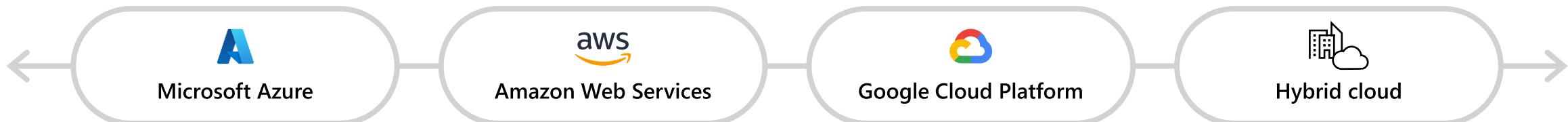


Assess and resolve security
alerts and incidents



Automate
response

Automate with the
tools of your choice



Multi-cloud – previous implementation



Multi-cloud – new solution



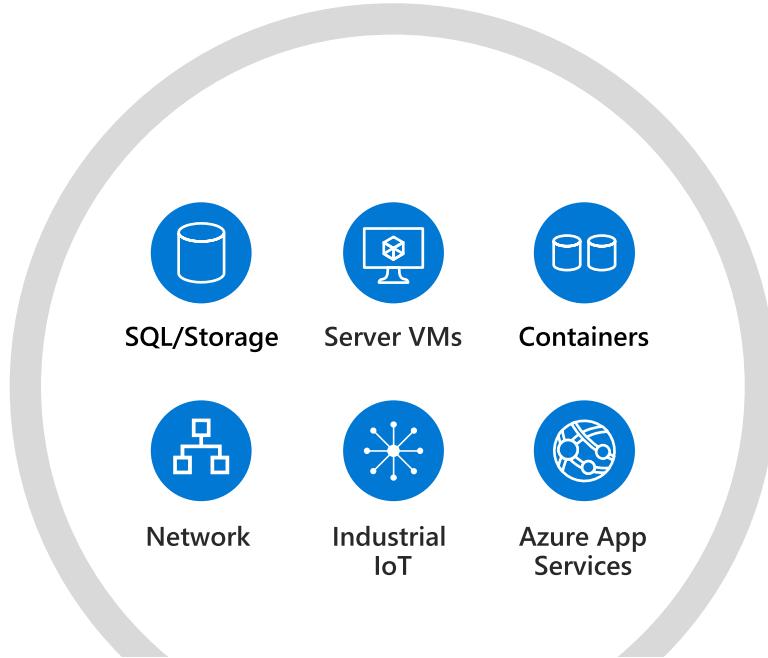
Seamless onboarding at scale

Regulatory standards breadth

Agentless design

Microsoft Defender for Cloud

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



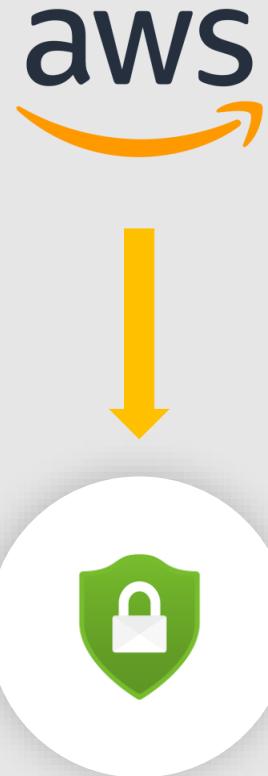
Microsoft Defender for Cloud



- 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

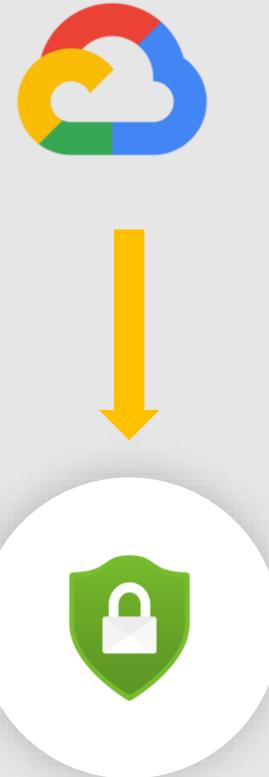
Connecting AWS accounts

- 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

The screenshot shows the Microsoft Defender for Cloud Recommendations interface. The left sidebar includes sections for General (Overview, Getting started, Recommendations), Cloud Security (Secure Score, Regulatory compliance, Workload protections, Firewall Manager), and Management (Environment settings, Security solutions, Workflow automation). The main area displays a list of security controls under the 'Controls' section, each with a title, max score, current score, potential score increase, unhealthy resources, and a progress bar. A specific control titled 'Security groups should not allow unrestricted access to ports with high risk' is highlighted with a tooltip. The interface also features filters for Control status, Recommendation status, Recommendation maturity, Severity, and Environment (set to AWS).

Control	Max score	Current Score	Potential score increase	Unhealthy resources	Resource health
Enable MFA	10	10	+ 0% (0 points)	None	<div style="width: 100%; background-color: #80B040;">█</div>
Hardware MFA should be enabled for the "root" a...				3 of 3 AWS acc...	<div style="width: 0%; background-color: #E04040;">█</div>
Restrict unauthorized network access	4	3.85	+ 0% (0.15 points)	1 of 197 resources	<div style="width: 95%; background-color: #80B040;">█</div>
VPC's default security group should restricts all tr...				51 of 51 AWS E...	<div style="width: 0%; background-color: #E04040;">█</div>
Amazon EC2 should be configured to use VPC en...				51 of 51 AWS E...	<div style="width: 0%; background-color: #E04040;">█</div>
Security groups should only allow unrestricted inc...				None	<div style="width: 100%; background-color: #80B040;">█</div>
Security groups should not allow unrestricted acc...				None	<div style="width: 100%; background-color: #80B040;">█</div>
Manage access and permissions				Security groups should not allow unrestricted access to ports with high risk	<div style="width: 0%; background-color: #E04040;">█</div>
Ensure credentials unused for 90 days or greater a...				None	<div style="width: 100%; background-color: #80B040;">█</div>
Ensure access keys are rotated every 90 days or less				None	<div style="width: 100%; background-color: #80B040;">█</div>
Root account access key shouldn't exist				None	<div style="width: 100%; background-color: #80B040;">█</div>
IAM policies should be attached only to groups or...				1 of 5 AWS acc...	<div style="width: 20%; background-color: #E04040;">█</div>
Do not setup access keys during initial user setup ...				None	<div style="width: 100%; background-color: #80B040;">█</div>
IAM policies that allow full **:** administrative pri...				None	<div style="width: 100%; background-color: #80B040;">█</div>
Lambda functions should restrict public access				None	<div style="width: 100%; background-color: #80B040;">█</div>
Amazon S3 permissions granted to other AWS acc...				None	<div style="width: 100%; background-color: #80B040;">█</div>

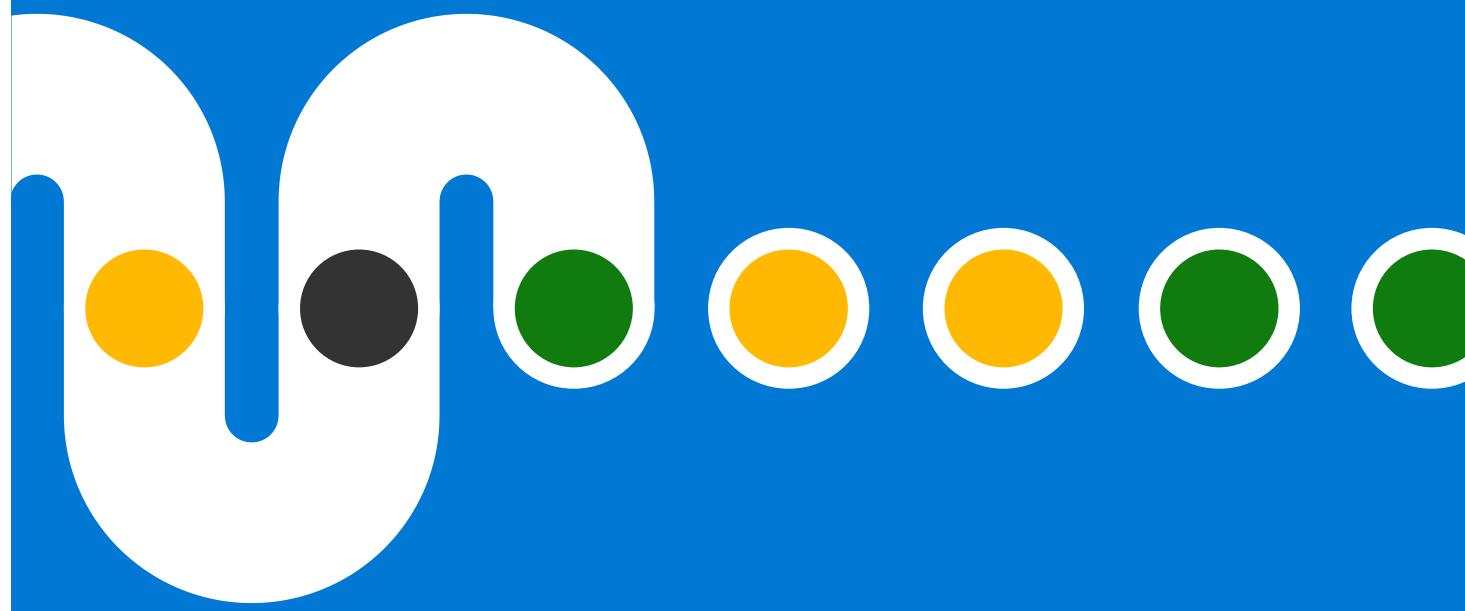
Inventory view

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

The screenshot shows the Microsoft Defender for Cloud Inventory page. At the top, it displays 'Showing 84 subscriptions'. Below this, there are four main statistics: 'Total resources' (9326), 'Unhealthy resources' (5050), 'Unmonitored resources' (0), and 'Unregistered subscriptions' (0). On the left, a navigation menu includes 'Overview', 'Getting started', 'Recommendations', 'Security alerts', 'Inventory' (which is selected), 'Workbooks', 'Community', and 'Diagnose and solve problems'. Under 'Cloud Security', there are links for 'Secure Score', 'Regulatory compliance', 'Workload protections', and 'Firewall Manager'. Under 'Management', there are links for 'Environment settings', 'Security solutions', and 'Workflow automation'. The main area contains a detailed list of resources, each with a small icon, a name, its type ('Virtual machines', 'AWS account', etc.), its subscription ('ASC DEMO', 'Ben Klijer', 'CyberSecSOC', etc.), and a status indicator ('Not installed' or 'Installed'). The list is paginated at the bottom.

AWS Demo



Microsoft Defender for Cloud – AWS



Microsoft Defender for Cloud | Recommendations ...

Showing subscription 'Microsoft Azure Sponsorship 2'

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

Completed recommendations (by severity)

High	Medium	Low
45/56	18/40	19/66

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

Home >

Microsoft Defender for Cloud | Overview

Showing 54 subscriptions

Search



54

Azure subscriptions

4

AWS accounts

18

GCP projects

8928

Assessed resources

215

Active recommendations

7768

Security alerts

General

Overview

Getting started

Recommendations

Security alerts

Inventory

Workbooks

Community

Diagnose and solve problems

Cloud security

Secure score

Regulatory compliance

Workload protection

Firewall manager

Management

Environment settings

Security solution

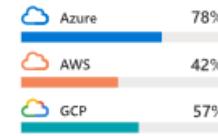
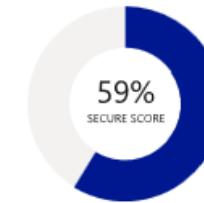
Workflow automation

Security posture

Recommendations status

95 of 455 overdue recommendations

Secure score

[Explore your security posture >](#)

Regulatory compliance

Azure security benchmark

2 of 44 passed controls

Lowest compliance regulatory standards by passed controls

CMMC Level 3	0/55
ISO 27001	1/20
AWS CIS 1.2.0	3/43

[Improve your compliance >](#)

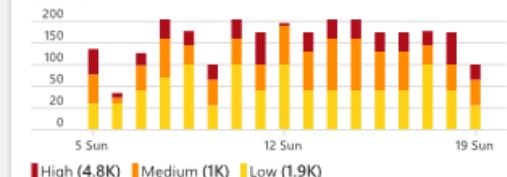
Workload protections

Resource coverage

95% For full protection, enable 8 resource plans

Alerts

by severity

[Enhance your threat protection capabilities >](#)

Firewall manager

5

Firewalls

3

Firewall policies

4

Regions with firewalls

Network protection status

by resource

Virtual hubs

Total resources

8928

Virtual networks

0/0

8/126

[Improve your network security >](#)

Inventory

Unmonitored VMs

54

To better protect your organization, we recommend [Install agents](#)

Recommendations & Alerts

by classified resources

SQL servers

Storage accounts

SQL databases

45

35

25

15

5

0

Information protection

[Preview](#)

Integrated with Purview

Resource scan coverage

2%

For full coverage [scan](#) additional resources

Recommendations & Alerts

by classified resources

Alerts

Recommendations

[View classified resources in inventory >](#)

Insights

[Upgrade to New Containers plan](#)[Click here to upgrade >](#)

Most prevalent recommendations

[Audit diagnostic setting](#)

619 Resources

[Storage account public access should...](#)

161 Resources

[A vulnerability assessment solution...](#)

107 Resources

Most attacked resources

[contoso5.cloudapp.net](#)

63 Alerts

[Virtual machine 2](#)

41 Alerts

[CentOS](#)

28 Alerts

[View full alert list >](#)

Controls with the highest potential increase

[Remediate vulnerabilities](#)

+11% (6pt)

[Enable encryption at rest](#)

+7% (4pt)

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

Amazon Web Services (preview) AWS accounts 1

Google Cloud Platform (preview) GCP projects 1

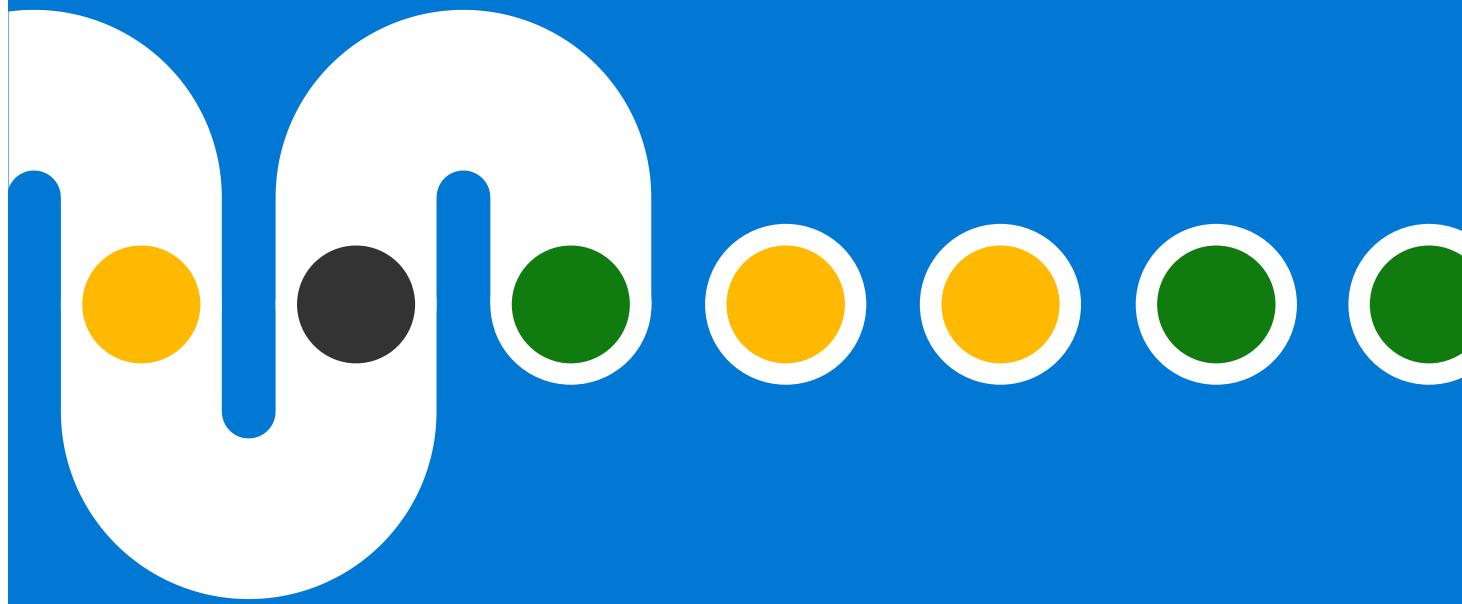
Multi-cloud account management page (preview). To switch back to the classic cloud connectors experience, click here.

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

Expand all

Name	Total resources	Defender coverage	Standards
Azure	208	3/4 plans	AWS C
AWS (preview)	139	3/4 plans	AWS C
GCP (preview)	45	3/3 plans	GCP C

GCP Demo



Microsoft Defender for Cloud – GCP



The screenshot shows the Microsoft Defender for Cloud interface under the "Recommendations" section. The top navigation bar includes "Home > Microsoft Defender for Cloud" and "Showing subscription 'ASC DEMO'". The main area displays "Secure score recommendations" and "All recommendations". It shows "Active recommendations (by severity)" with counts: High (49/132), Medium (38/178), and Low (40/215). Below this is a "Resource health" summary with counts: Unhealthy (7951), Healthy (1320), and Not applicable (43). A table lists various recommendations with columns for "Recommendation", "Unhealthy resources", "Resource health", "Initiative", and "Actions". Some recommendations include:

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 appro...	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		

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

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



Defender for Endpoint

GCP – Environment settings

Microsoft Azure (Preview) Search resources, services, and docs (G+/)

Home > Microsoft Defender for Cloud

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

Azure subscriptions: 1

AWS accounts: 7

GCP projects: 7

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

Name ↑↓	Total resources ↑↓	Defender coverage ↑↓	Standards ↑↓
72f988bf-86f1-41af-91ab-2d7cd011db47 (1 of 4 subscriptions)	9352	Limited permissions	
098881452406 (MDC_Containers_demo)	3/4 plans	AWS Foundational Security Best Practices (preview)	...
371992567628 (AwsManagementAccount)	1/4 plans	Amit test standard, CustomRecommendati...	...
102614528198 (securityConnector)	3/4 plans	AWS CIS 1.2.0 (preview), AWS Foundation...	...
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	...

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 Our Security Community

By Valon Kolica Published Feb 22 2021 01:50 PM 525K Views

Microsoft Security Community

Want to help defend the world against we can have a global impact together.

Co-Authors

- Valon_Kolica
- JasonCohen1892
- Ryan Heffernan
- AshleyMartin

Version history

Last updated: Feb 24 2022 11:07 AM

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

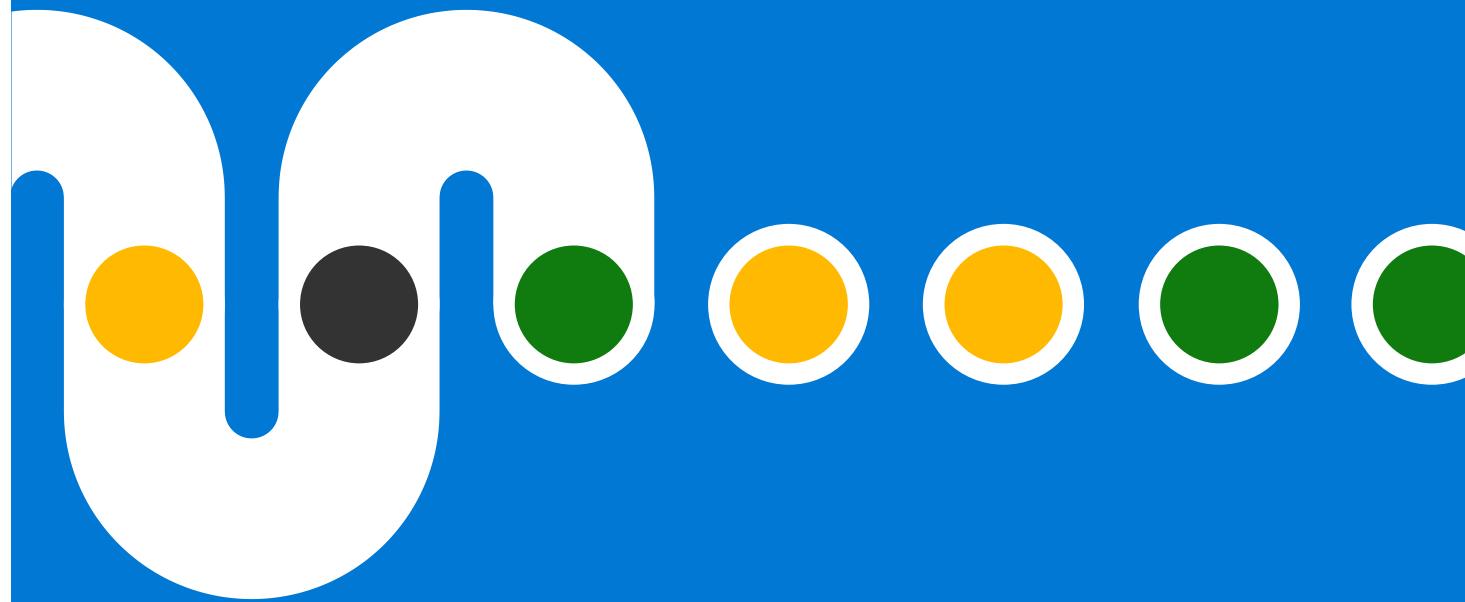
<https://aka.ms/MDfCMasterclassP1-Poll>



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

The screenshot shows the Microsoft Defender for Cloud Regulatory Compliance dashboard. At the top, there are logos for Google Cloud, AWS, and Azure. Below the logos, a message says: "You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above." A sidebar on the left lists navigation options: General (Overview, Getting started, Recommendations, Security alerts, Inventory, Workbooks, Community, Diagnose and solve problems), Cloud Security (Security posture, Regulatory compliance, Workload protections, Firewall Manager), Management (Environment settings, Security solutions, Workflow automation). The main content area displays the Azure Security Benchmark with 9 of 43 passed controls. It also shows the Lowest compliance regulatory standards: ISO 27001:2013 (0/17), CMMC Level 3 (0/55), SWIFT CSP CSCF v2020 (1/14), and SOC TSP (1/13). A survey question "Is the regulatory compliance experience clear to you?" with options "Yes" and "No" is shown. A note below states: "Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status." A section titled "Azure Security Benchmark V3" lists standards: ISO 27001, PCI DSS 3.2.1, SOC TSP, HIPAA HITRUST, NIST SP 800-53 R4, NIST SP 800-171 R2, UKO and UK NHS, Canada Federal PBMM. A "Customer responsibility" table shows failed resources and resource compliance status for various controls across different resource types like Web applications, Virtual machines extensions, and Azure resources.

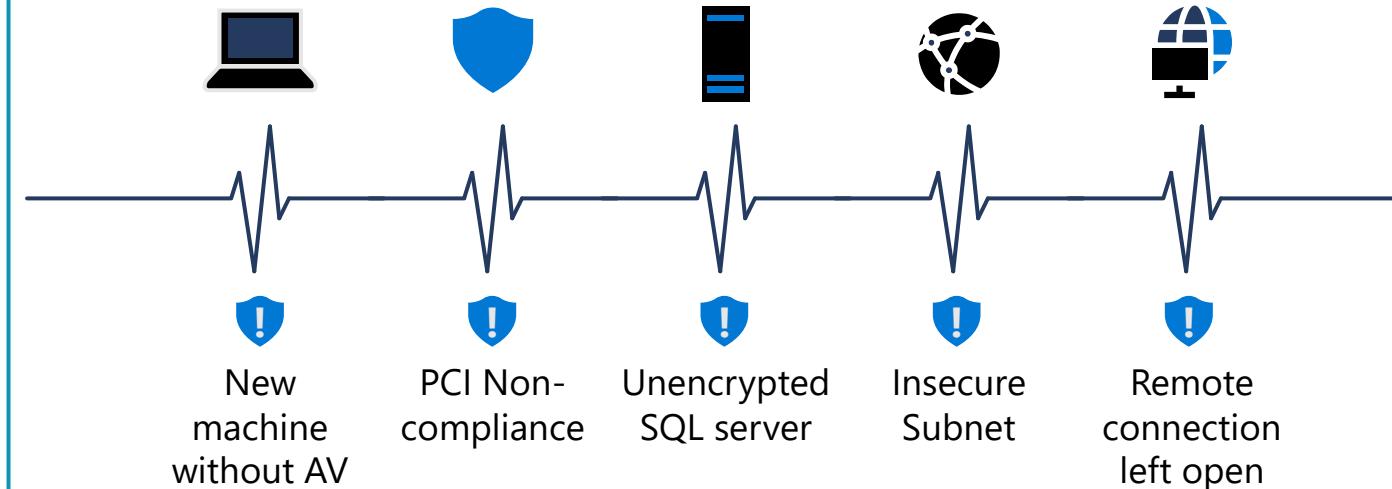


Manage organizational security policies and assess compliance in minutes

Manage security policies at an organizational level

Easily set security policies for subscriptions or management groups

Highly Dynamic Environment



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

The screenshot shows the Microsoft Defender for Cloud Settings page under the Security policy section. On the left, there is a sidebar with options like Settings, Defender plans, Auto provisioning, Email notifications, Integrations, Workflow automation, Continuous export, and Security policy (which is selected). Below the sidebar, there are three policy standards listed:

Standard	Description	Status	Action
ISO 27001	Track ISO 27001:2013 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Disable
SOC TSP	Track SOC TSP controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Enable
Azure CIS 1.1.0	Track Azure CIS 1.1.0 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Manually added	Delete

Below the standards, there is a button labeled "Add more standards".

Under "Your custom initiatives", there are three entries:

Initiative	Description	Action
Custom Benchmark	Super amazing custom benchmark for a demo lab	Delete
Contoso Security Benchmark	Baseline for security policies to appear alongside with the built-in recommendations	Delete
Cassandratriopia_test	Test initiative for recommendations	Delete

At the bottom, there are buttons for "Add a custom initiative" and "Add a recommendation".

Preventing misconfigurations

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

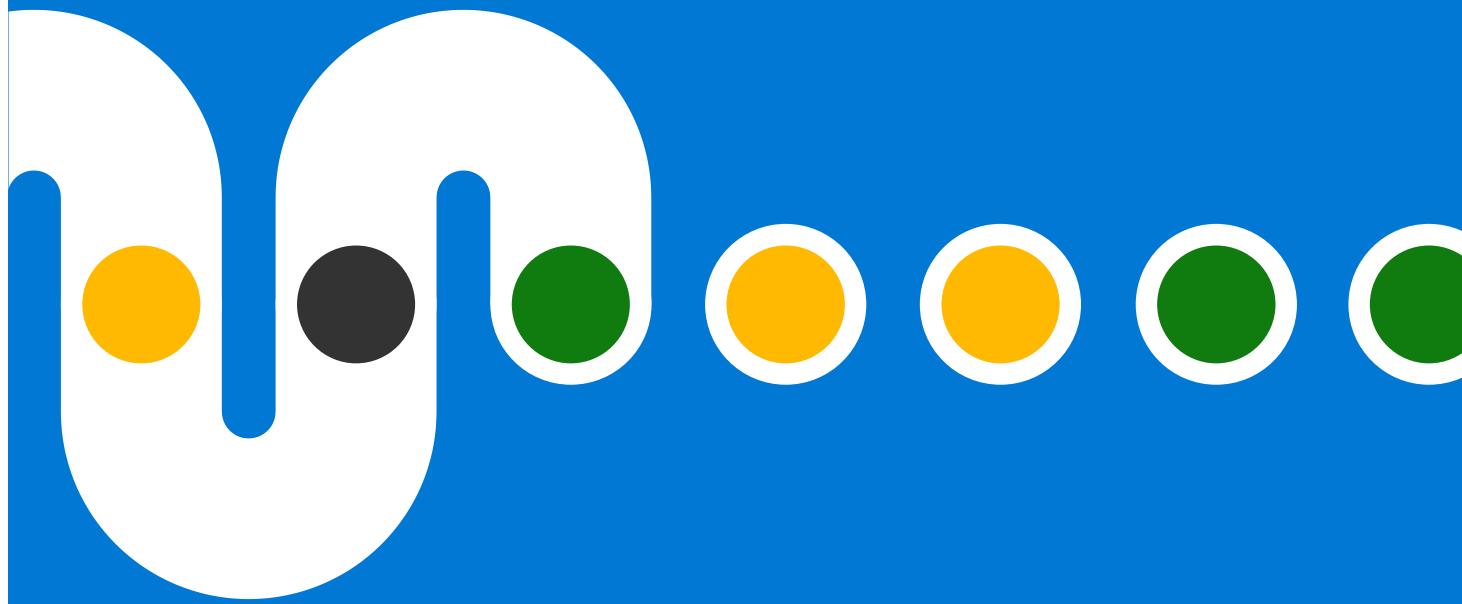
Using the **Enforce** option, you can take advantage of Azure Policy's **DeployIfNotExist** effect and automatically remediate non-compliant resources upon creation

The screenshot shows the Azure Policy blade with a policy named "Secure transfer to storage accounts should be enabled". The policy has a severity of "High" and a "Freshness interval" of "30 Min". It includes a "Tactics and techniques" section titled "Credential Access" with a "+1" link. The "Description" section explains that secure transfer is an option that forces storage accounts to accept requests only from secure connections (HTTPS). The "Remediation steps" section provides a link to "View policy definition". The "Affected resources" section shows "Unhealthy resources (0)", "Healthy resources (2)", and "Not applicable resources (0)". A search bar for "Search storage accounts" and a "Subscription" dropdown are also present. At the bottom, there are buttons for "Fix", "Trigger logic app", and "Exempt".

The screenshot shows the "Policy parameters" tab of the "Cassandratopia_test" initiative definition. The table lists policy parameters with their reference ID, parameter name, type, value type, and value(s). The "Effect" column shows values like "Audit", "AuditIfNotExists", and "Deny". The "Value Type" column shows "Default Value" and "Set value". The "Value(S)" column shows specific values such as "AuditIfNotExists" and "Audit". A dropdown menu for the last parameter shows options: "Set value" (selected), "Audit", "Deny", and "Disabled". Navigation buttons at the bottom include "Review + save", "Cancel", "Previous", and "Next".

REFERENCE ID	PARAMETER NAME	TYPE	VALUE TYPE	VALUE(S)
Azure Backup should be enabled for Virtual Machines_1	Effect	String	Default Value	AuditIfNotExists
Management ports of virtual machines should be prote...	Effect	String	Default Value	AuditIfNotExists
Managed disks should be double encrypted with both ...	Effect	String	Default Value	Audit
MFA should be enabled accounts with write permission...	Effect	String	Default Value	AuditIfNotExists
MFA should be enabled on accounts with owner permis...	Effect	String	Default Value	AuditIfNotExists
MFA should be enabled on accounts with read permissi...	Effect	String	Default Value	AuditIfNotExists
App Service Environment apps should not be reachable...	Effect	String	Set value	Audit
Internet-facing virtual machines should be protected wi...	Effect	String	Set value	AuditIfNotExists
Azure Web Application Firewall should be enabled for A...	Effect	String	Set value	Audit

Azure Demo



Regulatory Compliance Dashboard

Microsoft Defender for Cloud | Regulatory compliance

Showing 41 subscriptions

General

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

Cloud Security

- Security posture
- Regulatory compliance
- Workload protections
- Firewall Manager

Management

- Environment settings
- Security solutions
- Workflow automation

Download report Manage compliance policies Open query Audit reports Compliance over time workbook

You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above.

Azure Security Benchmark

9 of 43 passed controls

Lowest compliance regulatory standards

Regulation	Passed Controls	Total Controls
ISO 27001:2013	0/17	17
CMMC Level 3	0/55	55
SWIFT CSP CSCF v2020	1/14	14
SOC TSP	1/13	13

Show all 28

Regulatory compliance

View your compliance posture relative to the standards and regulations that are important to you. Remediate assessments to watch your compliance posture improve.

Learn more >

Azure Security Benchmark V3 ISO 27001 PCI DSS 3.2.1 SOC TSP HIPAA HITRUST NIST SP 800 53 R4 NIST SP 800 171 R2 UKO and UK NHS Canada Federal PBMM ...

Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.

Azure Security Benchmark is applied to 5 subscriptions

Expand all compliance controls

NS. Network Security

IM. Identity Management

IM-1. Use centralized identity and authentication system Control details MS C

IM-2. Protect identity and authentication system Control details MS C

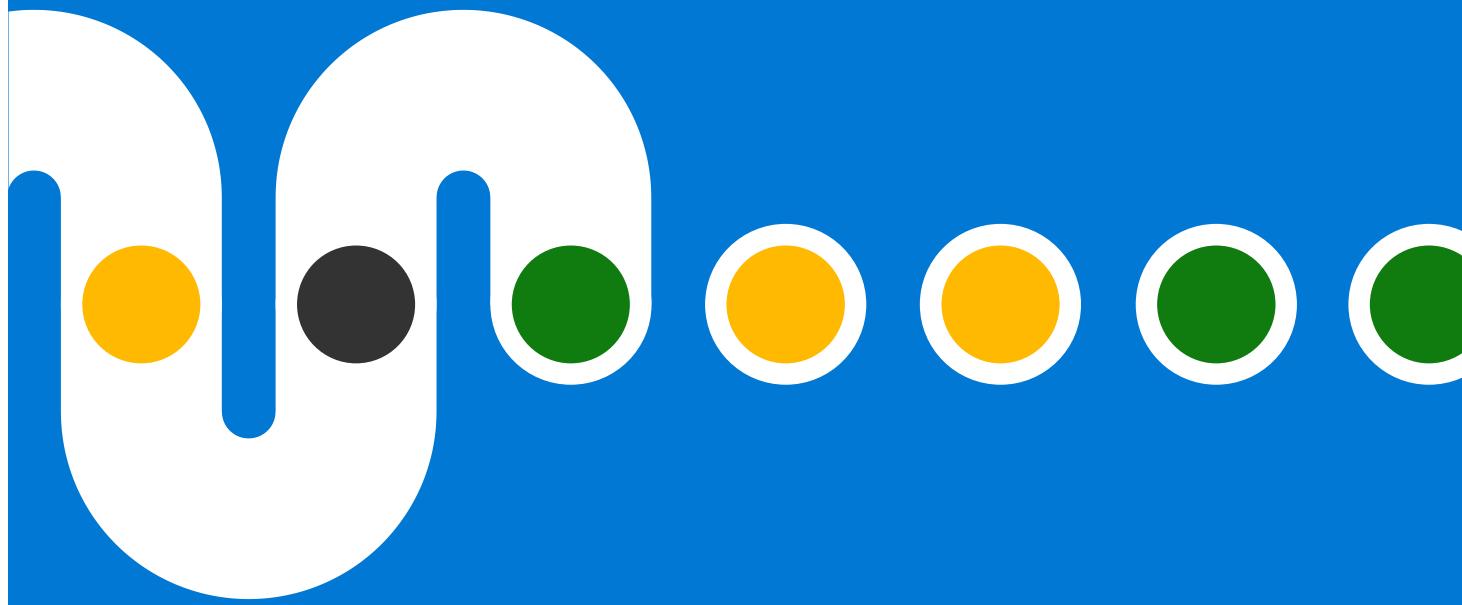
IM-3. Manage application identities securely and automatically Control details MS C

IM-4. Authenticate server and services Control details MS C

IM-5. Use single sign-on (SSO) for application access Control details MS C

Customer responsibility	Resource type	Failed resources	Resource compliance status
Managed identity should be used in web apps	Web applications	9 of 10	<div style="width: 90%; background-color: #2e7131;"></div>
Managed identity should be used in function apps	Web applications	7 of 19	<div style="width: 37%; background-color: #2e7131;"></div>
Virtual machines' Guest Configuration extension should be deployed with system-assigned man	Virtual machines extensions	4 of 71	<div style="width: 5.6%; background-color: #2e7131;"></div>
Managed identity should be used in API apps	Azure resources	0 of 0	<div style="width: 0%; background-color: #2e7131;"></div>

AWS and GCP Demo



AWS – Regulatory Compliance

Microsoft Azure (Preview) Search resources, services, and docs (G+/-) Home > Microsoft Defender for Cloud Microsoft Defender for Cloud | Regulatory compliance Showing subscription 'ASC DEMO' Search (Ctrl+ /) Download report Manage compliance policies Open query Audit reports Compliance over time workbook 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

You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above.

Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.

AWS CIS 1.2.0 (preview) is applied to the subscription ASC DEMO

Expand all compliance controls

1. Identity and Access Management

2. Logging

3. Monitoring

4. Networking

4.1. Ensure no security groups allow ingress from 0.0.0.0/0 to port 22

Customer responsibility	Resource type	Failed resources	Resource compliance status
Security groups should not allow ingress from 0.0.0.0/0 to port 22	AWS EC2 security groups	175 of 401	<div style="width: 43.75%; background-color: red;"></div> <div style="width: 56.25%; background-color: green;"></div>

4.2. Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389

Customer responsibility	Resource type	Failed resources	Resource compliance status
Ensure no security groups allow ingress from 0.0.0.0/0 to port 3389	AWS EC2 security groups	74 of 401	<div style="width: 18.5%; background-color: red;"></div> <div style="width: 81.5%; background-color: green;"></div>

Azure vs. others

Settings | Standards
Showing account 'MVC-Event-AWSTest'

Search (Ctrl+ /) Add Refresh

Standards Custom assessments (preview)

Security standards contain comprehensive sets of security recommendations to help you protect your cloud workloads.

Search by name Standard type : All

Showing 1-5 of 5 items

Name	Policy settings
AWS CIS 1.2.0	45
AWS Foundational Security Best Practices	125
AWS PCI DSS 3.2.1	44
AWS-Test-Standard	8
MegaAWSteststandard	2

Home > Microsoft Defender for Cloud > Environment settings > Settings

Settings | Security policy Visual Studio Enterprise Subscription

Search (Ctrl+ /)

The default initiative enabled on your subscription generates the security recommendations in the [Recommendations](#) page.

Assignment	Assigned On	Audit policies	Deny policies	Disable
ASC Default (subscription: 6875d1e9-3884-4a25-...)	Subscription	191	0	15

Industry & regulatory standards

Compliance initiatives shown in the [Regulatory compliance dashboard](#).

Azure Security Benchmark	Track Azure Security Benchmark controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Disable
PCI DSS 3.2.1	Track PCI-DSS v3.2.1:2018 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Enable
ISO 27001	Track ISO 27001:2013 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Deprecated
SOC TSP	Track SOC TSP controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Enable

Add more standards

Your custom initiatives

Custom initiatives generate custom recommendations in the [Recommendations](#) page.

Add a custom initiative

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



Azure Log Analytics



Azure Logic Apps



Outlook



Microsoft Teams



slack



servicenow™



Microsoft Sentinel

Wrap Up

Labs and Demo Guidance

- **On-Demand Recording** - coming in the near future after this event
- **Slides & Labs** -
<http://aka.ms/MDFCMasterclassP1-repo>

- 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=lrqkHOPFktM>
- Must Learn KQL – <http://aka.ms/mustlearnkql>

**Resources to
continue your
training**

Upcoming UK partner security events and training

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



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)

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 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)

Expert Certifications

Microsoft Cyber Security Architect (SC-100)

Training includes

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

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](#).

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

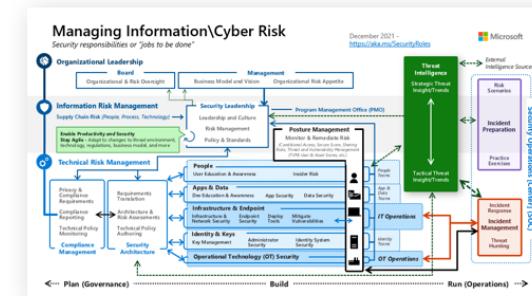
How does this map to insider and external attacks?



Build Slide

People

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



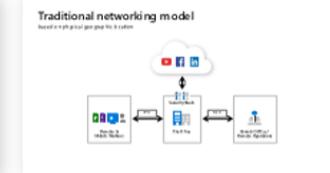
Multi-Cloud & Cross-Platform

What clouds & platforms does Microsoft protect?



Secure Access Service Edge (SASE)

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



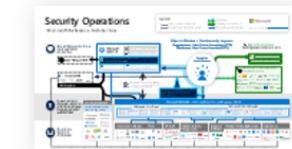
Zero Trust User Access

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



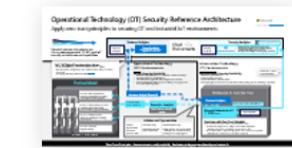
Security Operations

How to enable rapid incident response?



Operational Technology

How to enable Zero Trust Security for OT?





Share your thoughts, **feedback** via our survey. Help decide the deep dive content for Part 2 and beyond!

<https://aka.ms/MDFCMasterclassP1-Feedback>

- 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

|||

Thank you!

Feedback:

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

