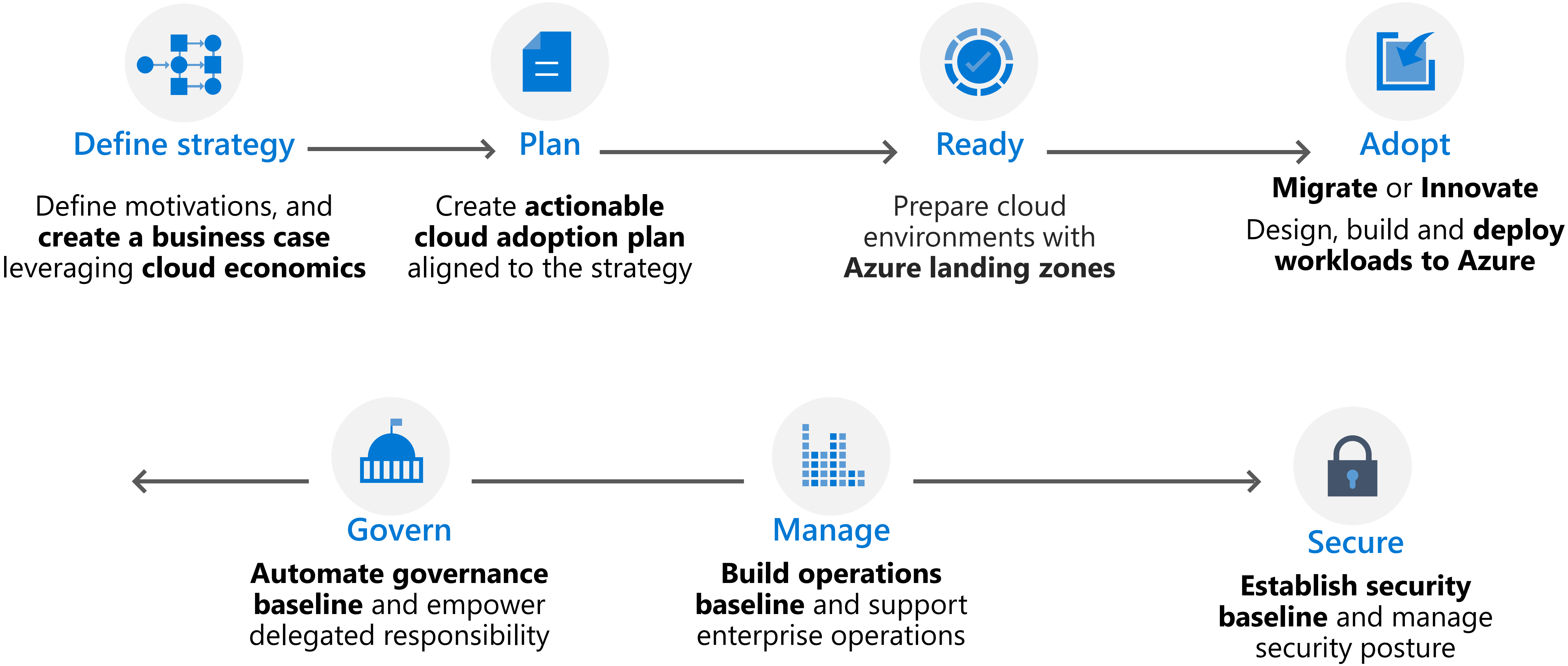
Microsoft Security

CLOUD CHAMPION

Microsoft Defender Cloud Security Posture Management

Michael Green
Sr Cloud Solution Architect
Microsoft | Global Partner Solutions

Microsoft Cloud Adoption Framework for Azure



Define strategy

Define motivations, and **create a business case** leveraging **cloud economics**

Plan

Create **actionable cloud adoption plan** aligned to the strategy

Ready

Prepare cloud environments with **Azure landing zones**

Adopt

Migrate or **Innovate**

Design, build and **deploy workloads to Azure**

Govern

Automate governance baseline and empower delegated responsibility

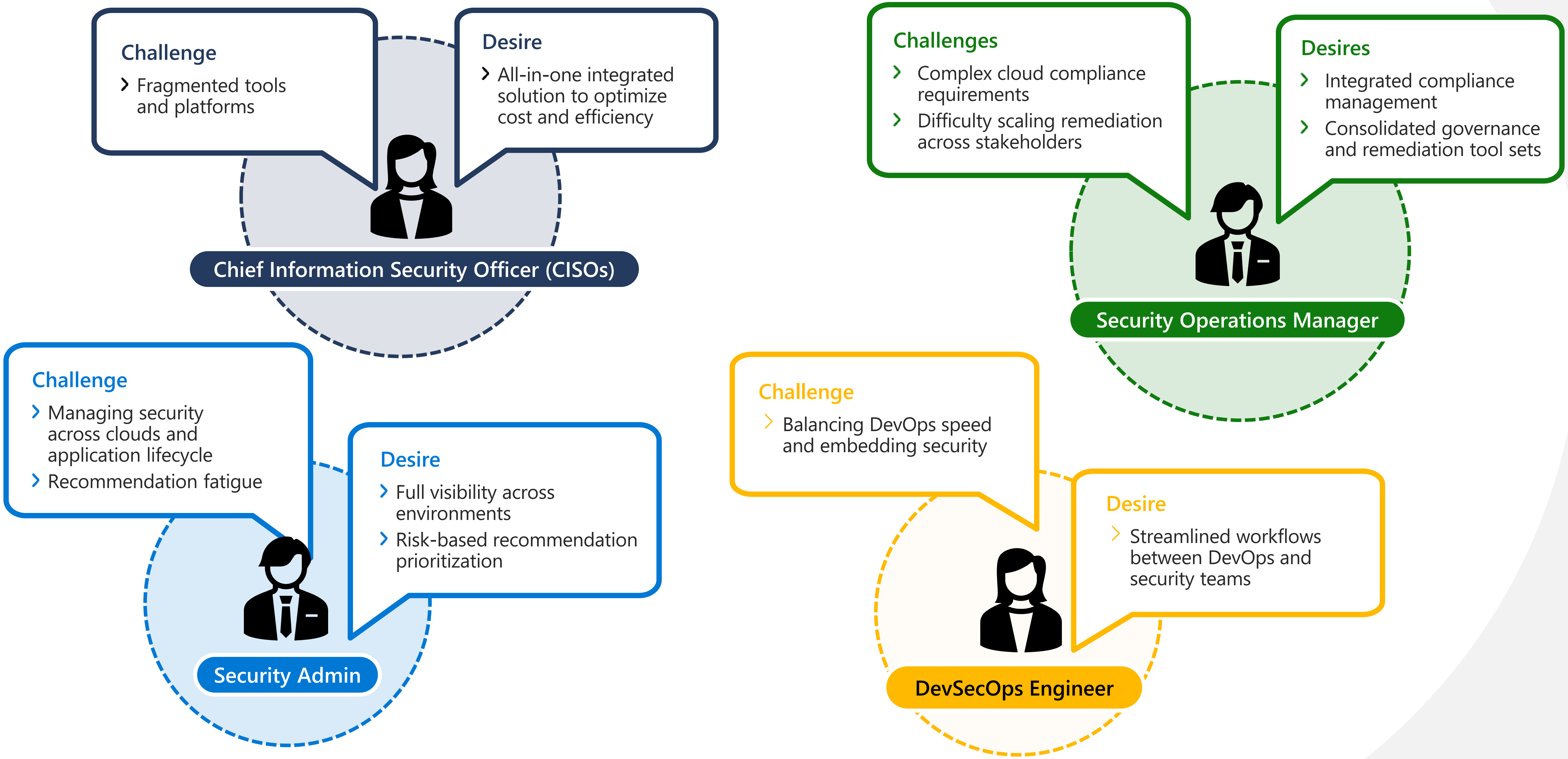
Manage

Build operations baseline and support enterprise operations

Secure

Establish security baseline and manage security posture

Siloed challenges to manage cloud security posture



Chief Information Security Officer (CISOs)

Challenge

- Fragmented tools and platforms

Desire

- All-in-one integrated solution to optimize cost and efficiency

Security Operations Manager

Challenges

- Complex cloud compliance requirements
- Difficulty scaling remediation across stakeholders

Desires

- Integrated compliance management
- Consolidated governance and remediation tool sets

Security Admin

Challenge

- Managing security across clouds and application lifecycle
- Recommendation fatigue

Desire

- Full visibility across environments
- Risk-based recommendation prioritization

DevSecOps Engineer

Challenge

- Balancing DevOps speed and embedding security

Desire

- Streamlined workflows between DevOps and security teams

CSPM + CIEM

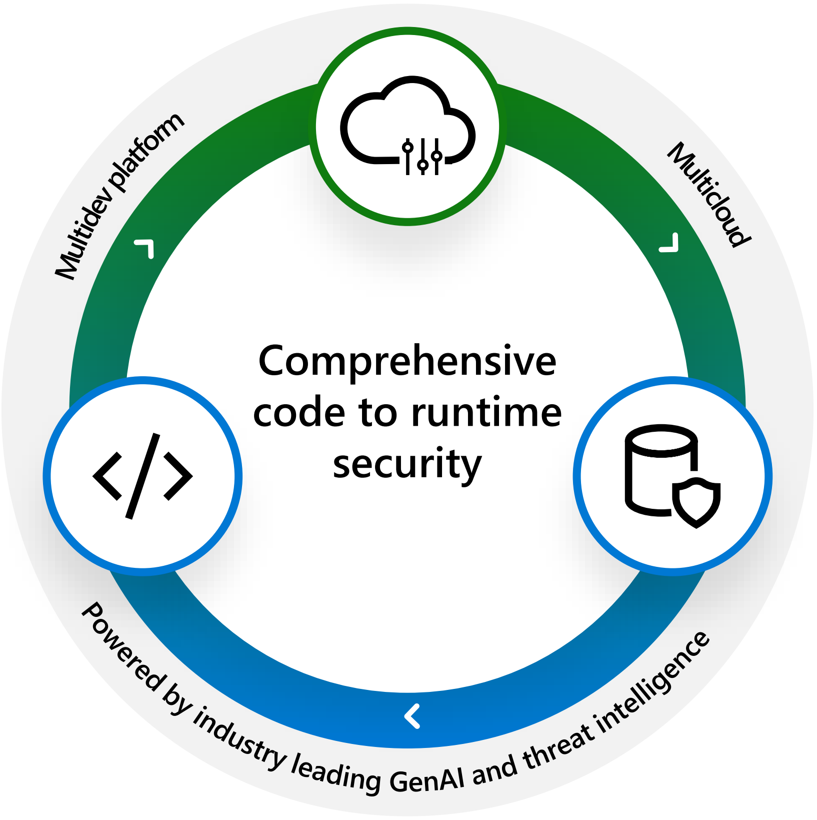
Continuously reduce risk

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

AppSec + CI/CD security

Enable secure development

Prevent vulnerabilities, misconfiguration, secrets in code, and secure your software supply chain


Multidev platform
Multicloud
Comprehensive code to runtime security
Powered by industry leading GenAI and threat intelligence

CWP + CDR

Remediate threats faster

Near real-time detection and response for cloud workloads, data and APIs in a unified XDR experience

Microsoft Defender CSPM

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

Pinpoint and remediate risks

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

Unify security standards and cloud policies

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

Fortify sensitive data across clouds

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

Prevent future risks by fixing in code

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

FREE

Gain visibility into your multicloud risks

Foundational Cloud Security Posture Management (CSPM)

Unify visibility across your multicloud resources and DevOps pipelines

Inventory all cloud assets and get unified visibility across multicloud resources, cloud applications and CI/CD environments

Continuously assess and improve your cloud security posture

Get a birds-eye view of the security and compliance posture of your entire cloud estate with 450+ built-in assessments

aws

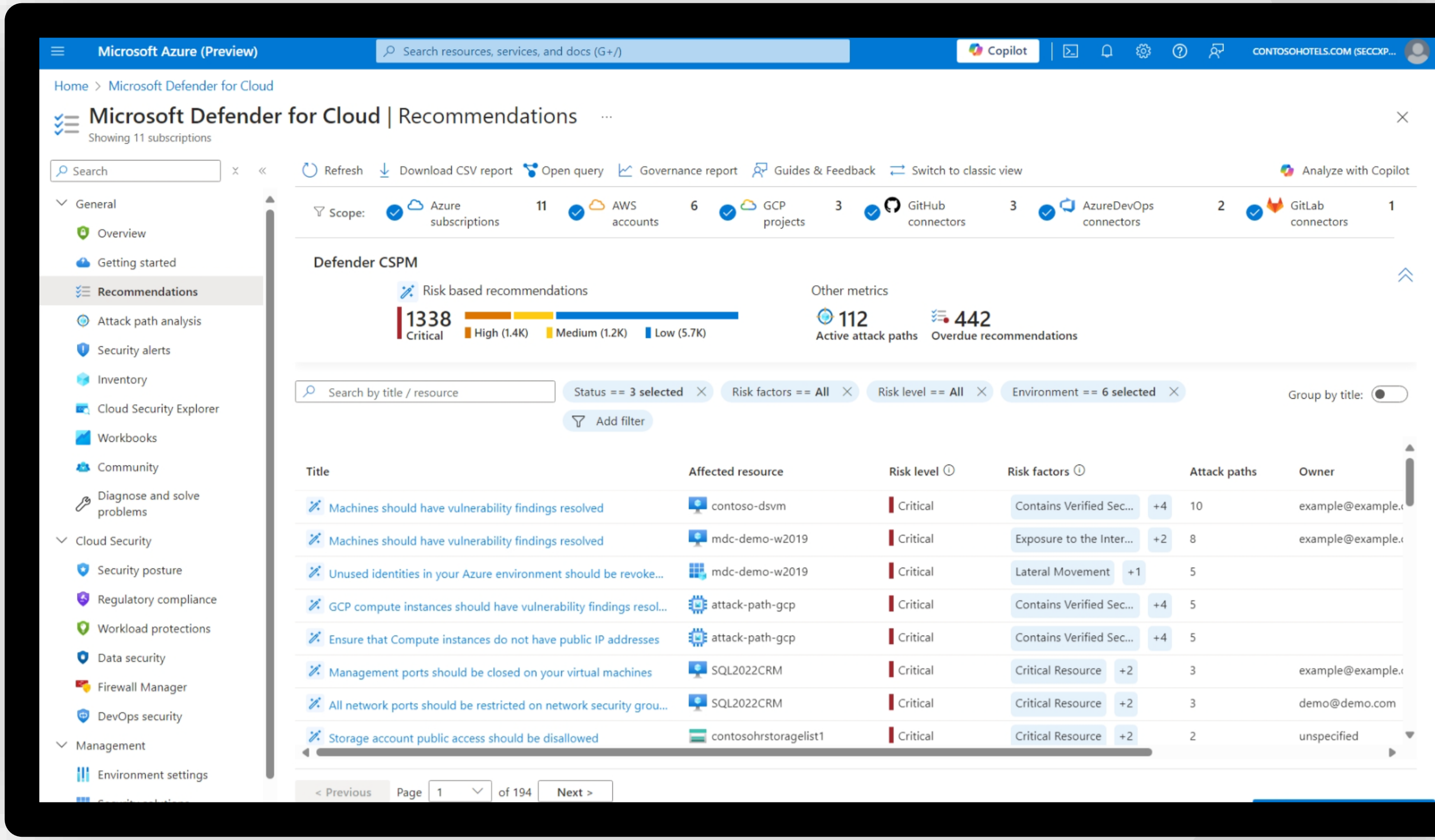
Foundational CSPM vs Defender CSPM

Feature	Foundational CSPM (free)	Defender CSPM (billing applies)	Cloud coverage		
			Azure	AWS	GCP
Security recommendations (across infrastructure, data, DevOps, network, permissions, etc.)	●	●	●	●	●
Asset inventory	●	●	●	●	●
Secure Score	●	●	●	●	●
Data visualization and reporting with Azure Workbooks	●	●	●	●	●
Data exporting	●	●	●	●	●
Workflow automation	●	●	●	●	●
Remediation tracking	●	●	●	●	●
Microsoft Cloud Security Benchmark	●	●	●	●	●
‘Azure Policy’ based recommendation customization (Azure only)	●	●	●		
Infrastructure as code (IaC) security		●			
KQL based recommendation customization (multicloud)		●		●	●
Regulatory compliance assessments		●	●	●	●
Governance (including ServiceNow integration)		●	●	●	●
Attack path analysis		●	●	●	●
Cloud security explorer		●	●	●	●
EASM insights in network exposure		●	●	●	●
Agentless vulnerability assessments for compute (using Microsoft Defender Vulnerability Management)		●	●	●	●
Agentless discovery for Kubernetes		●	●	●	●
Agentless vulnerability assessments for container images, including registry scanning		●	●	●	●
Data security posture for storage and databases		●	●	●	●
Integration with Entra Permissions Management (Preview)		●	●	●	●

Pinpoint and remediate risks

Take a risk-based approach to prioritize remediation

- **Context-aware risk prioritization** engine calculates the risk level of each security recommendation
- **Aggregate exploitability and business impact** of risk factors of each resource, potential impact of security issue, and attack paths determine risk levels
- **Granular visibility at the resource level** with the ability to exempt resources to filter out unnecessary security recommendations



Microsoft Defender for Cloud | Recommendations

Showing 11 subscriptions

Scope: Azure subscriptions 11 · AWS accounts 6 · GCP projects 3 · GitHub connectors 3 · AzureDevOps connectors 2 · GitLab connectors 1

Defender CSPM

Risk based recommendations: 1338 Critical · High (1.4K) · Medium (1.2K) · Low (5.7K)

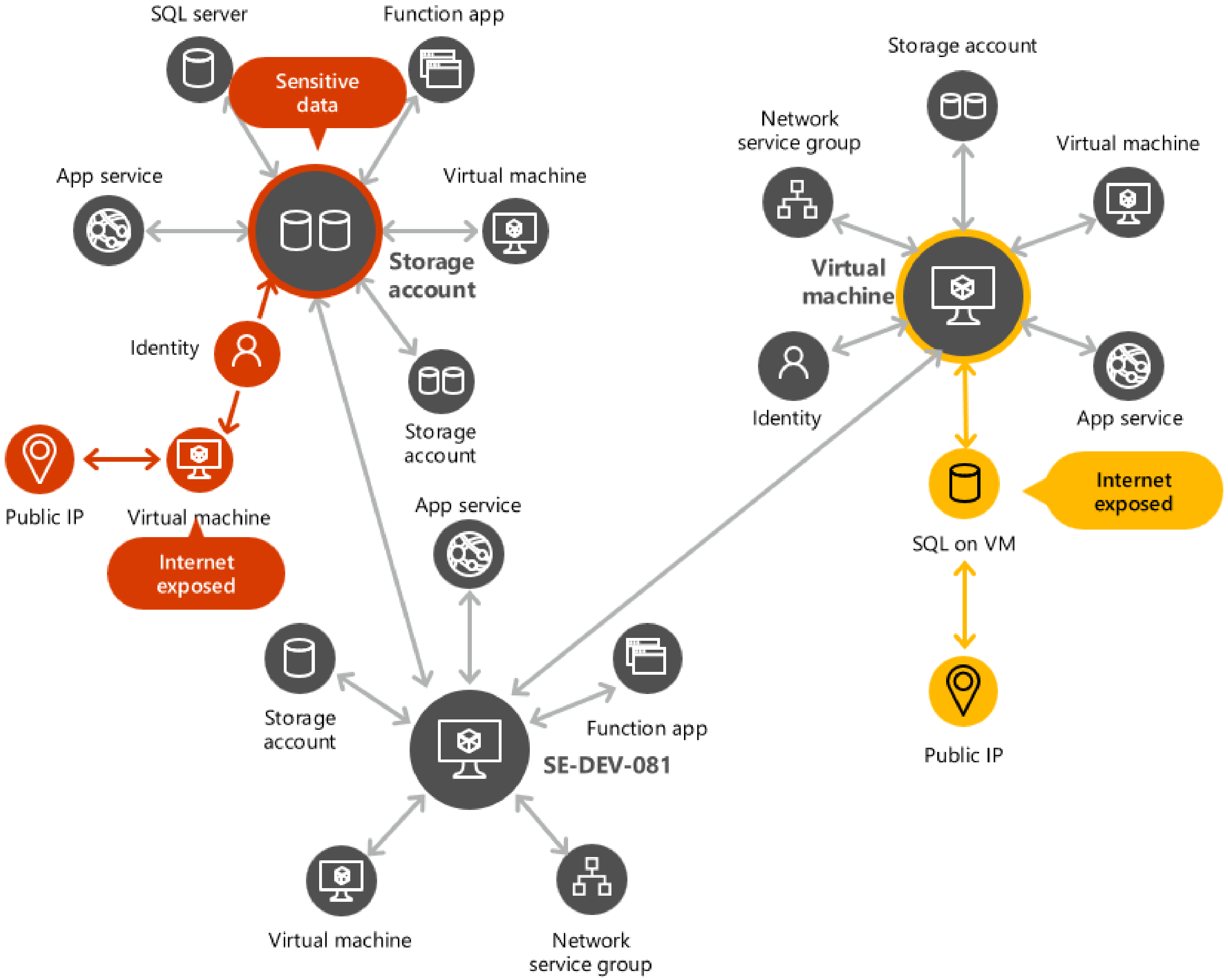
Other metrics: 112 Active attack paths · 442 Overdue recommendations

Status == 3 selected · Risk factors == All · Risk level == All · Environment == 6 selected

Title	Affected resource	Risk level	Risk factors	Attack paths	Owner
Machines should have vulnerability findings resolved	contoso-dsvm	Critical	Contains Verified Sec... +4	10	example@example.c
Machines should have vulnerability findings resolved	mdc-demo-w2019	Critical	Exposure to the Inter... +2	8	example@example.c
Unused identities in your Azure environment should be revoke...	mdc-demo-w2019	Critical	Lateral Movement +1	5	
GCP compute instances should have vulnerability findings resol...	attack-path-gcp	Critical	Contains Verified Sec... +4	5	
Ensure that Compute instances do not have public IP addresses	attack-path-gcp	Critical	Contains Verified Sec... +4	5	
Management ports should be closed on your virtual machines	SQL2022CRM	Critical	Critical Resource +2	3	example@example.c
All network ports should be restricted on network security grou...	SQL2022CRM	Critical	Critical Resource +2	3	demo@demo.com
Storage account public access should be disallowed	contosohrstoragelist1	Critical	Critical Resource +2	2	unspecified

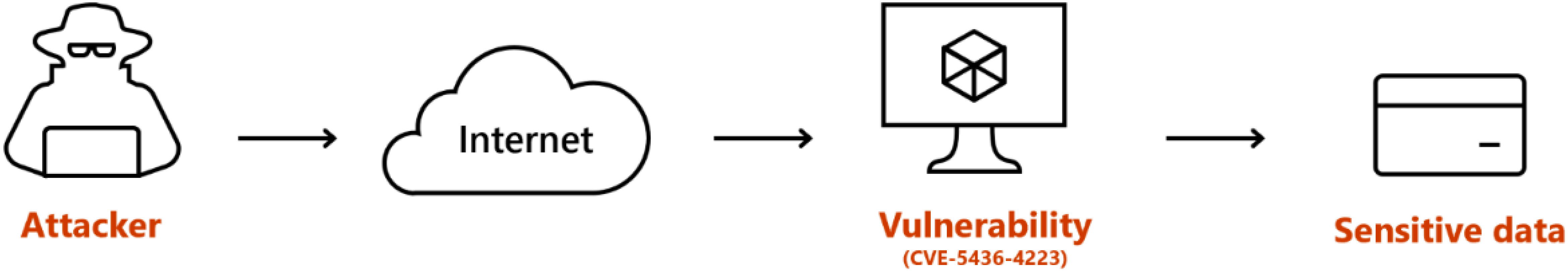
Page 1 of 194

Cloud Security Graph



Investigate risks with security explorer/attack paths in Microsoft Defender for Cloud - Microsoft Defender for Cloud | Microsoft Learn

Attack Path Analysis

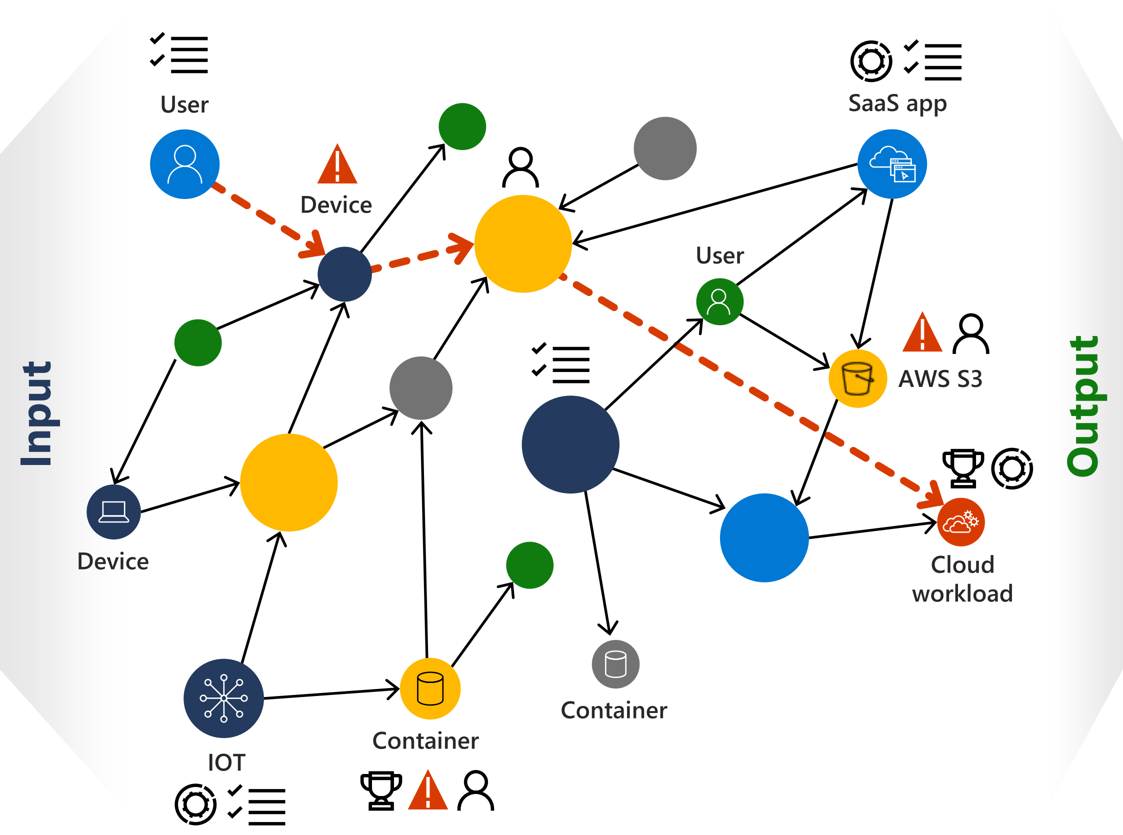


Attacker → Internet → Vulnerability (CVE-5436-4223) → Sensitive data

Investigate risks with security explorer/attack paths in Microsoft Defender for Cloud - Microsoft Defender for Cloud | Microsoft Learn

Extend posture management to the entire digital estate

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



Attack surface management

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

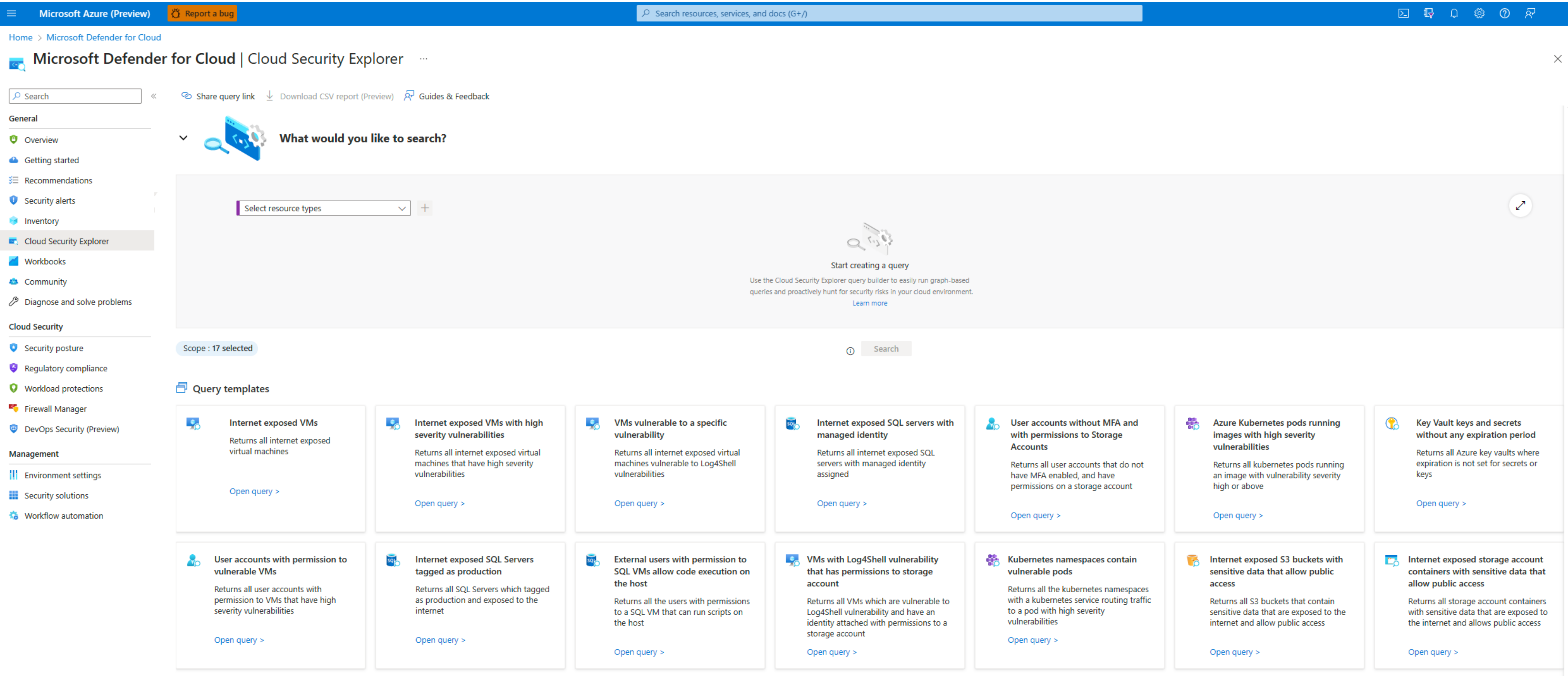
Attack path analysis

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

Unified exposure insights

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

☑ Risk Posture ◎ Optimization ⚠ Security risk 🏆 Asset value 👤 Business owner → Relationship ⇢ Attack path



Microsoft Defender for Cloud | Cloud Security Explorer

What would you like to search?

Start creating a query

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

Learn more

Query templates

Internet exposed VMs
Returns all internet exposed virtual machines
Open query >

Internet exposed VMs with high severity vulnerabilities
Returns all internet exposed virtual machines that have high severity vulnerabilities
Open query >

VMs vulnerable to a specific vulnerability
Returns all internet exposed virtual machines vulnerable to Log4Shell vulnerabilities
Open query >

Internet exposed SQL servers with managed identity
Returns all internet exposed SQL servers with managed identity assigned
Open query >

User accounts without MFA and with permissions to Storage Accounts
Returns all user accounts that do not have MFA enabled, and have permissions on a storage account
Open query >

Azure Kubernetes pods running images with high severity vulnerabilities
Returns all kubernetes pods running an image with vulnerability severity high or above
Open query >

Key Vault keys and secrets without any expiration period
Returns all Azure key vaults where expiration is not set for secrets or keys
Open query >

User accounts with permission to vulnerable VMs
Returns all user accounts with permission to VMs that have high severity vulnerabilities
Open query >

Internet exposed SQL Servers tagged as production
Returns all SQL Servers which tagged as production and exposed to the internet
Open query >

External users with permission to SQL VMs allow code execution on the host
Returns all the users with permissions to a SQL VM that can run scripts on the host
Open query >

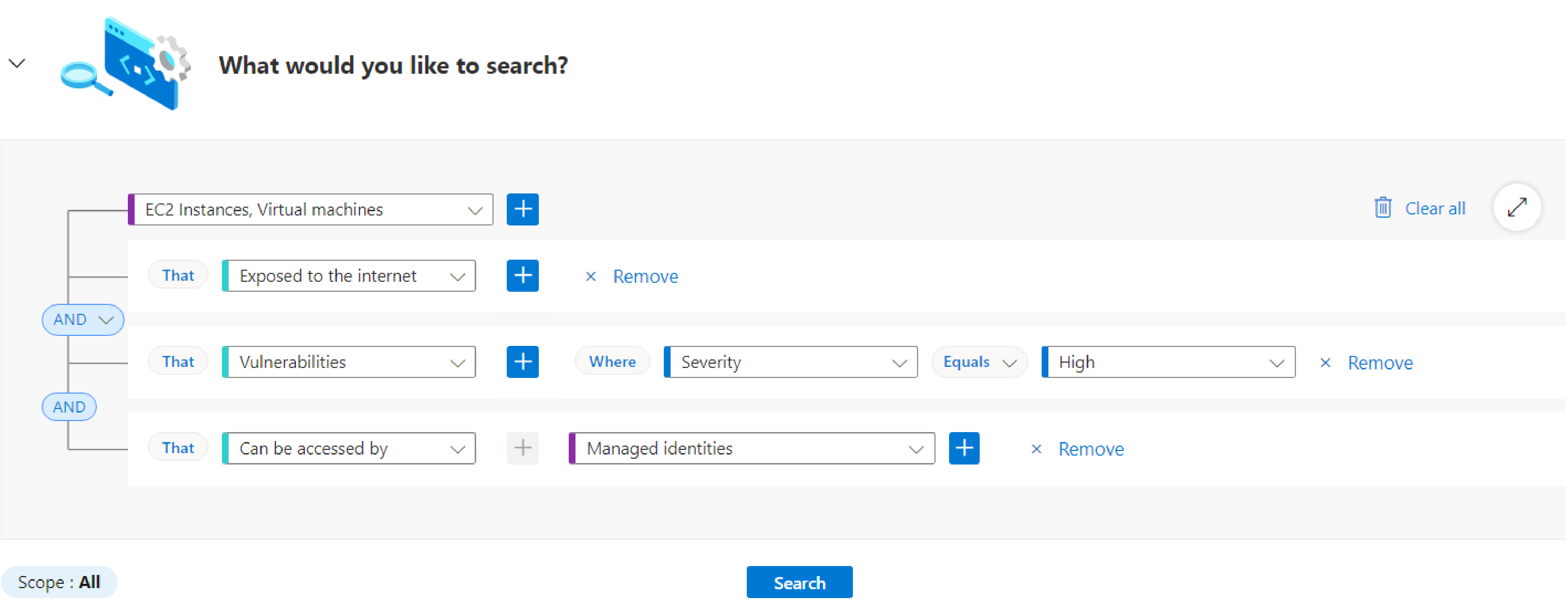
VMs with Log4Shell vulnerability that has permissions to storage account
Returns all VMs which are vulnerable to Log4Shell vulnerability and have an identity attached with permissions to a storage account
Open query >

Kubernetes namespaces contain vulnerable pods
Returns all the kubernetes namespaces with a kubernetes service routing traffic to a pod with high severity vulnerabilities
Open query >

Internet exposed S3 buckets with sensitive data that allow public access
Returns all S3 buckets that contain sensitive data that are exposed to the internet and allow public access
Open query >

Internet exposed storage account containers with sensitive data that allow public access
Returns all storage account containers with sensitive data that are exposed to the internet and allows public access
Open query >

[Build queries with cloud security explorer - Microsoft Defender for Cloud | Microsoft Learn]



What would you like to search?

EC2 Instances, Virtual machines

That Exposed to the internet

AND

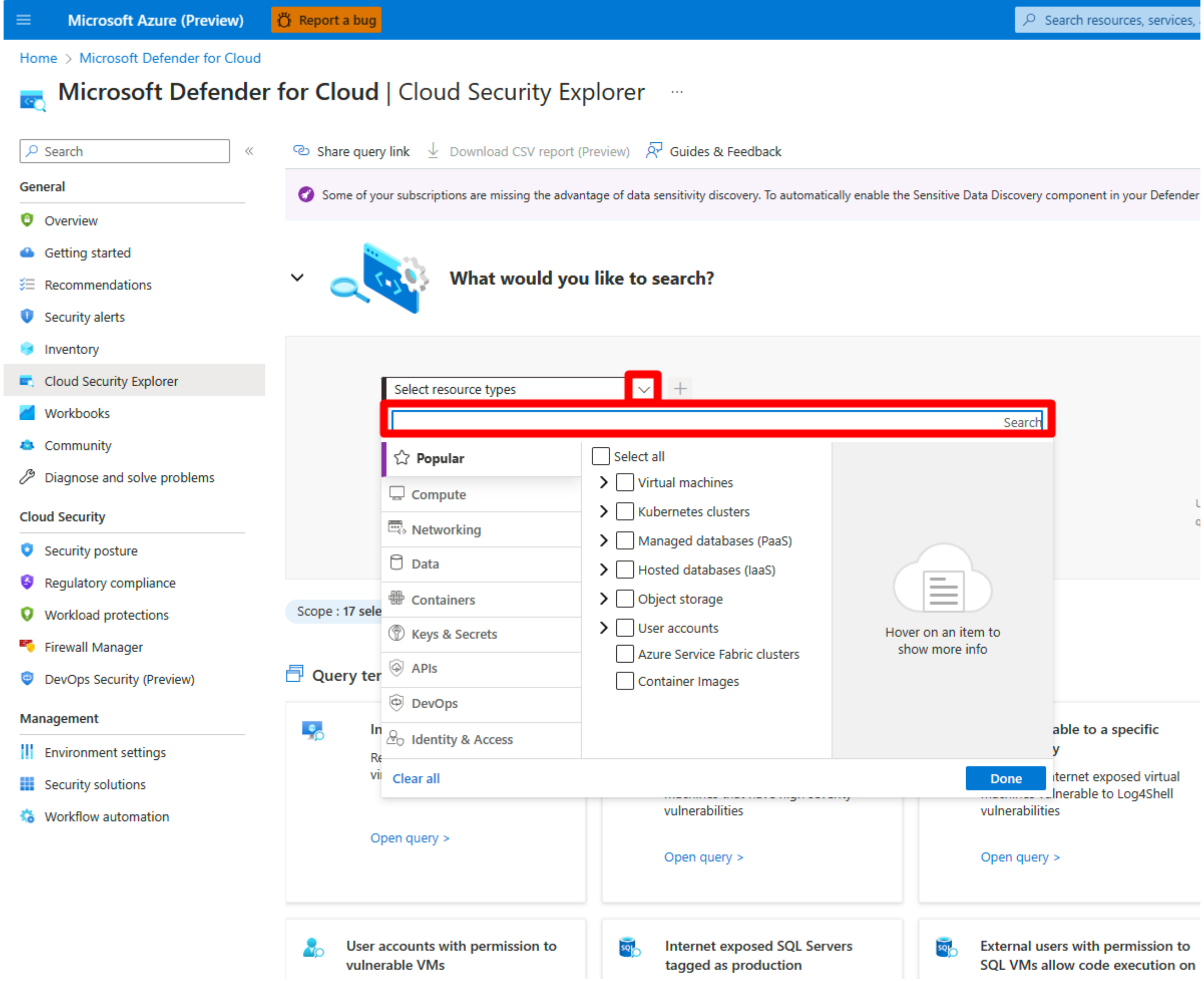
That Vulnerabilities Where Severity Equals High

AND

That Can be accessed by Managed identities

Scope : **All**

Build queries with cloud security explorer - Microsoft Defender for Cloud | Microsoft Learn



Some of your subscriptions are missing the advantage of data sensitivity discovery. To automatically enable the Sensitive Data Discovery component in your Defender

In
Re
vi

vulnerabilities

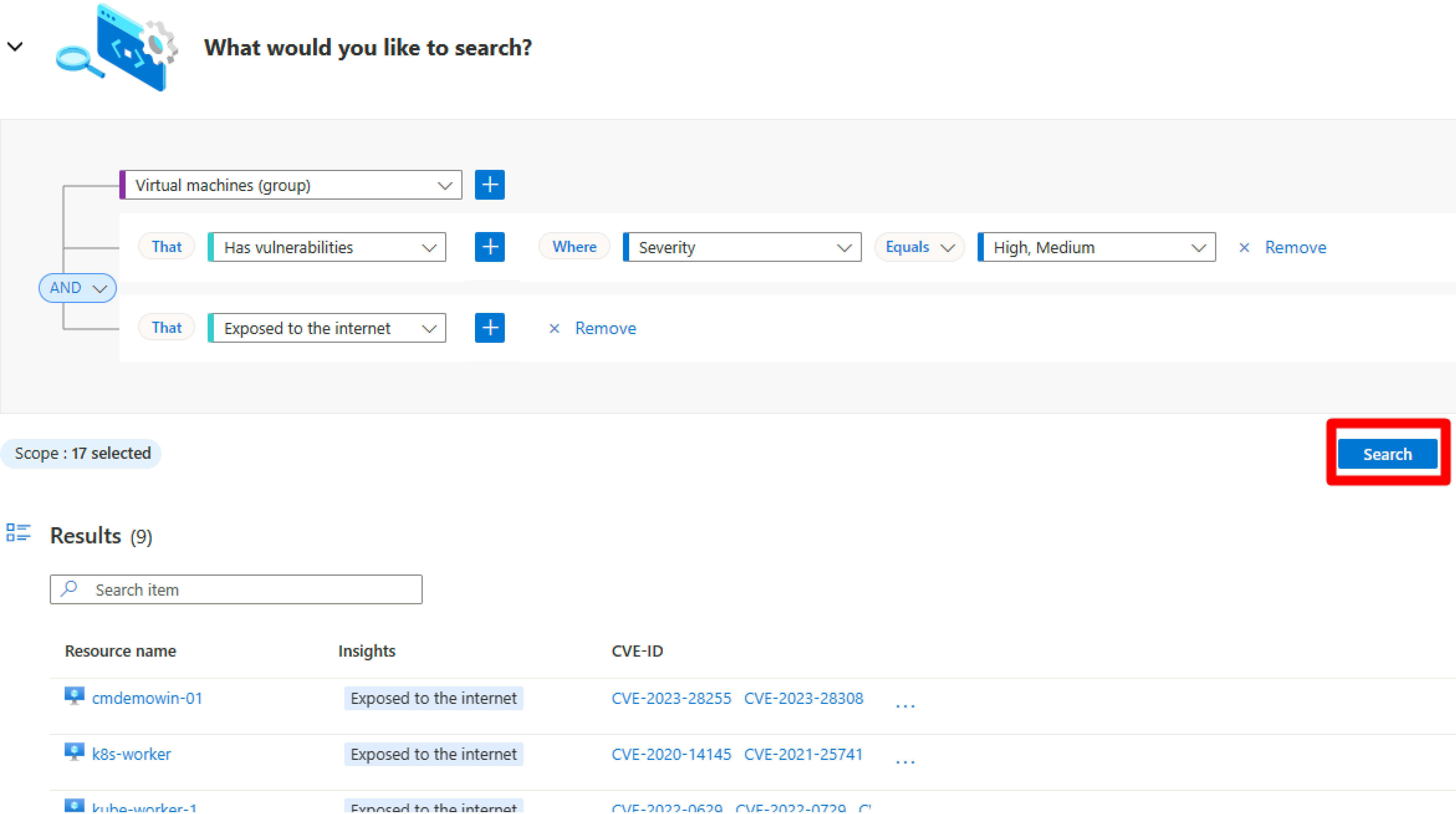
able to a specific
y
ternet exposed virtual
lnerable to Log4Shell
vulnerabilities

User accounts with permission to vulnerable VMs

Internet exposed SQL Servers tagged as production

External users with permission to SQL VMs allow code execution on

[Build queries with cloud security explorer - Microsoft Defender for Cloud | Microsoft Learn]



Resource name	Insights	CVE-ID
cmdemowin-01	Exposed to the internet	CVE-2023-28255 CVE-2023-28308 ...
k8s-worker	Exposed to the internet	CVE-2020-14145 CVE-2021-25741 ...
kube-worker-1	Exposed to the internet	CVE-2022-0629 CVE-2022-0729 C'

[Build queries with cloud security explorer - Microsoft Defender for Cloud | Microsoft Learn]

Unify security standards and policies across clouds

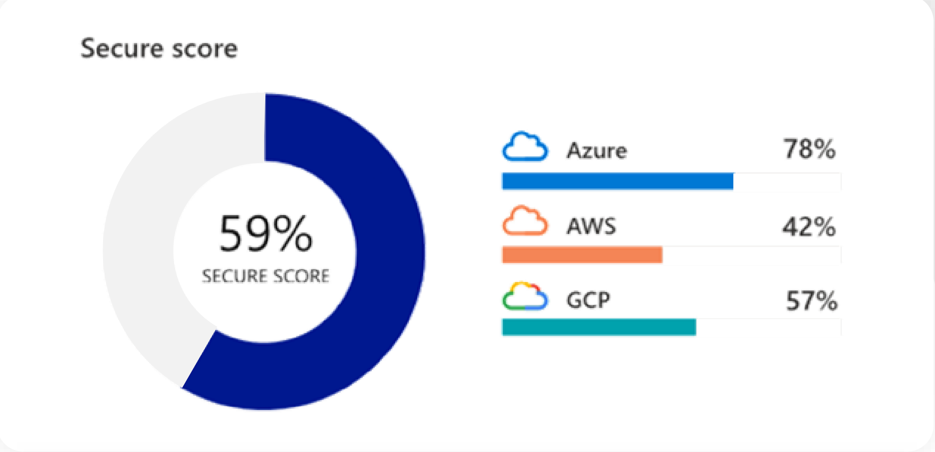
Strengthen security from the start

Evaluate posture at-a-glance with Secure Score

- Assess security posture across all critical cloud resources including network, access, compute, databases, your service layer, and more
- 450+ out-of-the-box recommendations
- Create custom recommendations to meet unique organizational needs

Multicloud security benchmark for security compliance

- Manage cloud security compliance and continuously assess cloud resources across AWS, Azure, and GCP
- Use industry standards, compliance frameworks, and cloud-specific benchmarks to implement best practices (CIS, PCI, NIST, ISO HIPAA, etc.)



Evaluated categories

Access

Compute

SQL server

IoT

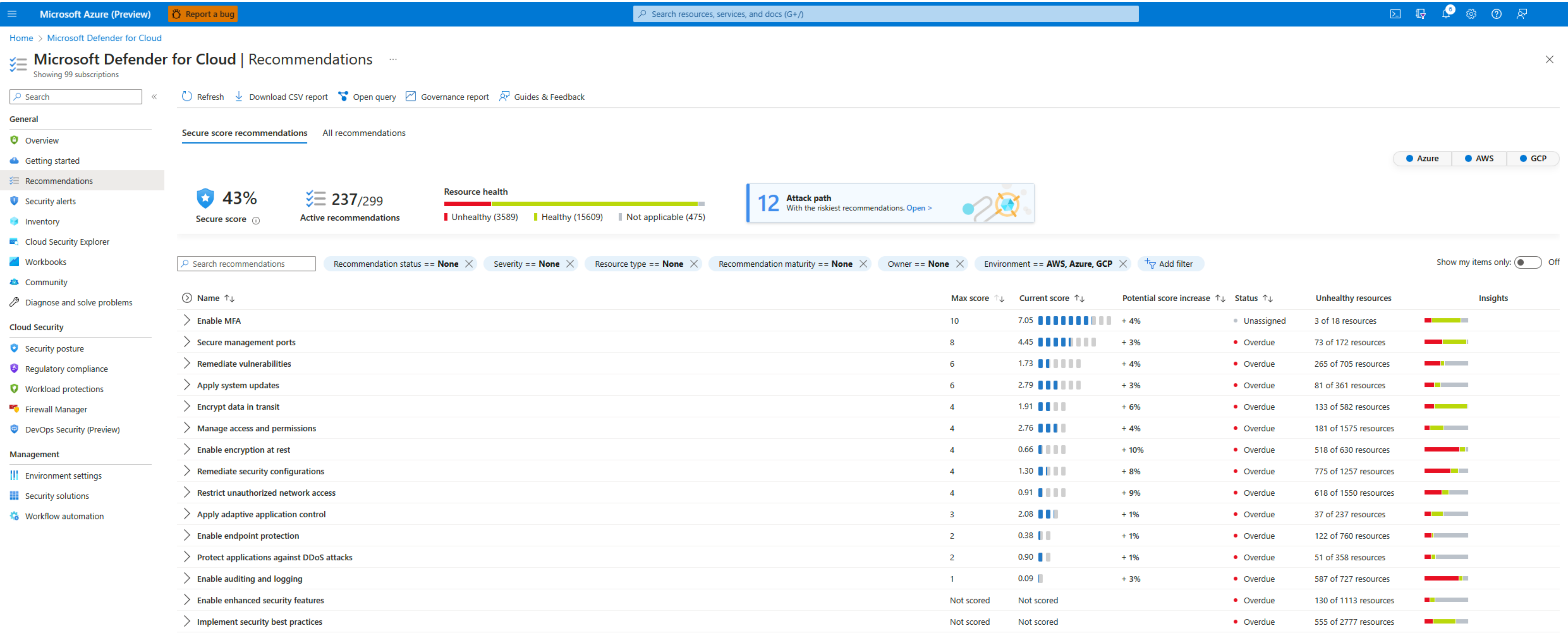
Network

App services

Containers

Azure API Management

Recommendations



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

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Recommendations

Showing 99 subscriptions

43% Secure score

237/299 Active recommendations

Resource health: Unhealthy (3589) | Healthy (15609) | Not applicable (475)

12 Attack path — With the riskiest recommendations. Open >

Recommendation status == **None** | Severity == **None** | Resource type == **None** | Recommendation maturity == **None** | Owner == **None** | Environment == **AWS, Azure, GCP** | Add filter

Show my items only: Off

Name	Max score	Current score	Potential score increase	Status	Unhealthy resources	Insights
Enable MFA	10	7.05	+ 4%	Unassigned	3 of 18 resources	
Secure management ports	8	4.45	+ 3%	Overdue	73 of 172 resources	
Remediate vulnerabilities	6	1.73	+ 4%	Overdue	265 of 705 resources	
Apply system updates	6	2.79	+ 3%	Overdue	81 of 361 resources	
Encrypt data in transit	4	1.91	+ 6%	Overdue	133 of 582 resources	
Manage access and permissions	4	2.76	+ 4%	Overdue	181 of 1575 resources	
Enable encryption at rest	4	0.66	+ 10%	Overdue	518 of 630 resources	
Remediate security configurations	4	1.30	+ 8%	Overdue	775 of 1257 resources	
Restrict unauthorized network access	4	0.91	+ 9%	Overdue	618 of 1550 resources	
Apply adaptive application control	3	2.08	+ 1%	Overdue	37 of 237 resources	
Enable endpoint protection	2	0.38	+ 1%	Overdue	122 of 760 resources	
Protect applications against DDoS attacks	2	0.90	+ 1%	Overdue	51 of 358 resources	
Enable auditing and logging	1	0.09	+ 3%	Overdue	587 of 727 resources	
Enable enhanced security features	Not scored	Not scored		Overdue	130 of 1113 resources	
Implement security best practices	Not scored	Not scored		Overdue	555 of 2777 resources	

Understand gaps in your cloud compliance posture

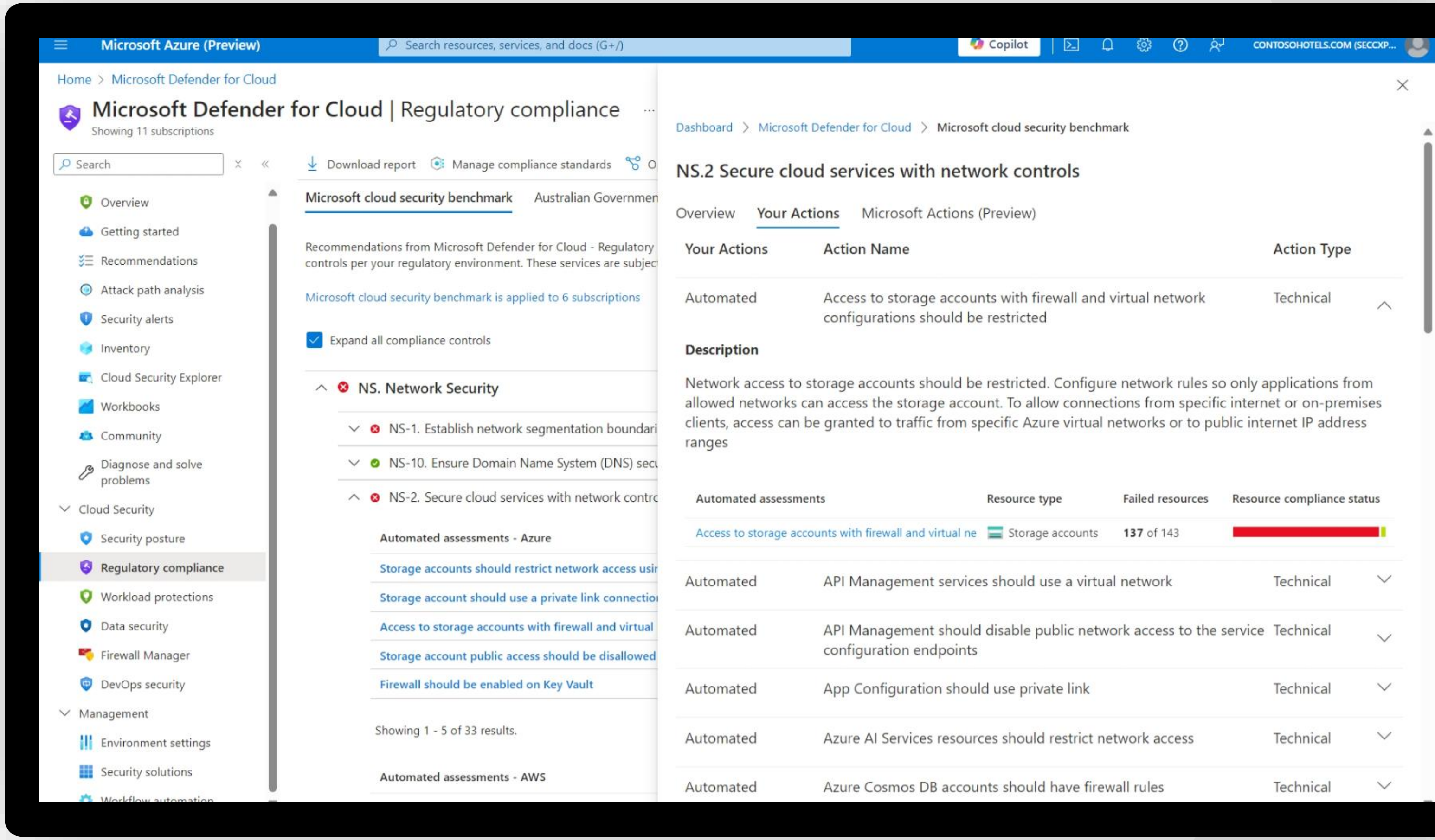
Assess and manage your cloud security compliance

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

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

Supported (among others):

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



Microsoft Defender for Cloud | Regulatory compliance

Showing 11 subscriptions

Recommendations from Microsoft Defender for Cloud - Regulatory controls per your regulatory environment. These services are subjec

Microsoft cloud security benchmark is applied to 6 subscriptions

☑ Expand all compliance controls

NS. Network Security

- NS-1. Establish network segmentation boundari
- NS-10. Ensure Domain Name System (DNS) secu
- NS-2. Secure cloud services with network contro

Automated assessments - Azure

- Storage accounts should restrict network access usi
- Storage account should use a private link connectio
- Access to storage accounts with firewall and virtual
- Storage account public access should be disallowed
- Firewall should be enabled on Key Vault

Showing 1 - 5 of 33 results.

Automated assessments - AWS

NS.2 Secure cloud services with network controls

Your Actions	Action Name	Action Type
Automated	Access to storage accounts with firewall and virtual network configurations should be restricted	Technical

Description

Network access to storage accounts should be restricted. Configure network rules so only applications from allowed networks can access the storage account. To allow connections from specific internet or on-premises clients, access can be granted to traffic from specific Azure virtual networks or to public internet IP address ranges

Automated assessments	Resource type	Failed resources	Resource compliance status
Access to storage accounts with firewall and virtual ne	Storage accounts	137 of 143	🟥

Your Actions	Action Name	Action Type
Automated	API Management services should use a virtual network	Technical
Automated	API Management should disable public network access to the service configuration endpoints	Technical
Automated	App Configuration should use private link	Technical
Automated	Azure AI Services resources should restrict network access	Technical
Automated	Azure Cosmos DB accounts should have firewall rules	Technical

Microsoft cloud security benchmark (v1)

The Microsoft cloud security benchmark (MCSB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure and your multi-cloud environment. This benchmark focuses on cloud-centric control areas with input from a set of holistic Microsoft and industry security guidance that includes:

•Cloud Adoption Framework: Guidance on security, including strategy, roles and responsibilities, Azure Top 10 Security Best Practices, and reference implementation.

•Azure Well-Architected Framework: Guidance on securing your workloads on Azure.

•The Chief Information Security Officer (CISO) Workshop: Program guidance and reference strategies to accelerate security modernization using Zero Trust principles.

•Other industry and cloud service providers security best practice standards and framework: Examples include the Amazon Web Services (AWS) Well-Architected Framework, Center for Internet Security (CIS) Controls, National Institute of Standards and Technology (NIST), and Payment Card Industry Data Security Standard (PCI-DSS).

disclaimer - please refer to source document

Overview of the Microsoft cloud security benchmark | Microsoft Learn

Common Use Cases

The Microsoft cloud security benchmark can often be used to address common challenges for **customers or service partners** who are:

New to Azure (and other major cloud platforms, such as AWS)

Looking to improve security posture of existing cloud deployments

Using multi-cloud environments (such as Azure and AWS)

Evaluating the security features/capabilities of Azure (and other major cloud platforms, such as AWS)

Having to meet compliance requirements in highly regulated industries, such as government, finance, and healthcare.

disclaimer - please refer to source document

Microsoft cloud security benchmark introduction | Microsoft Learn

Control Domains (MCSB v1)

Network security (NS)

Identity Management (IM)

Privileged Access (PA)

Data Protection (DP)

Asset Management (AM)

Logging and Threat Detection (LT)

Incident Response (IR)

Posture and Vulnerability Management (PV)

Endpoint Security (ES)

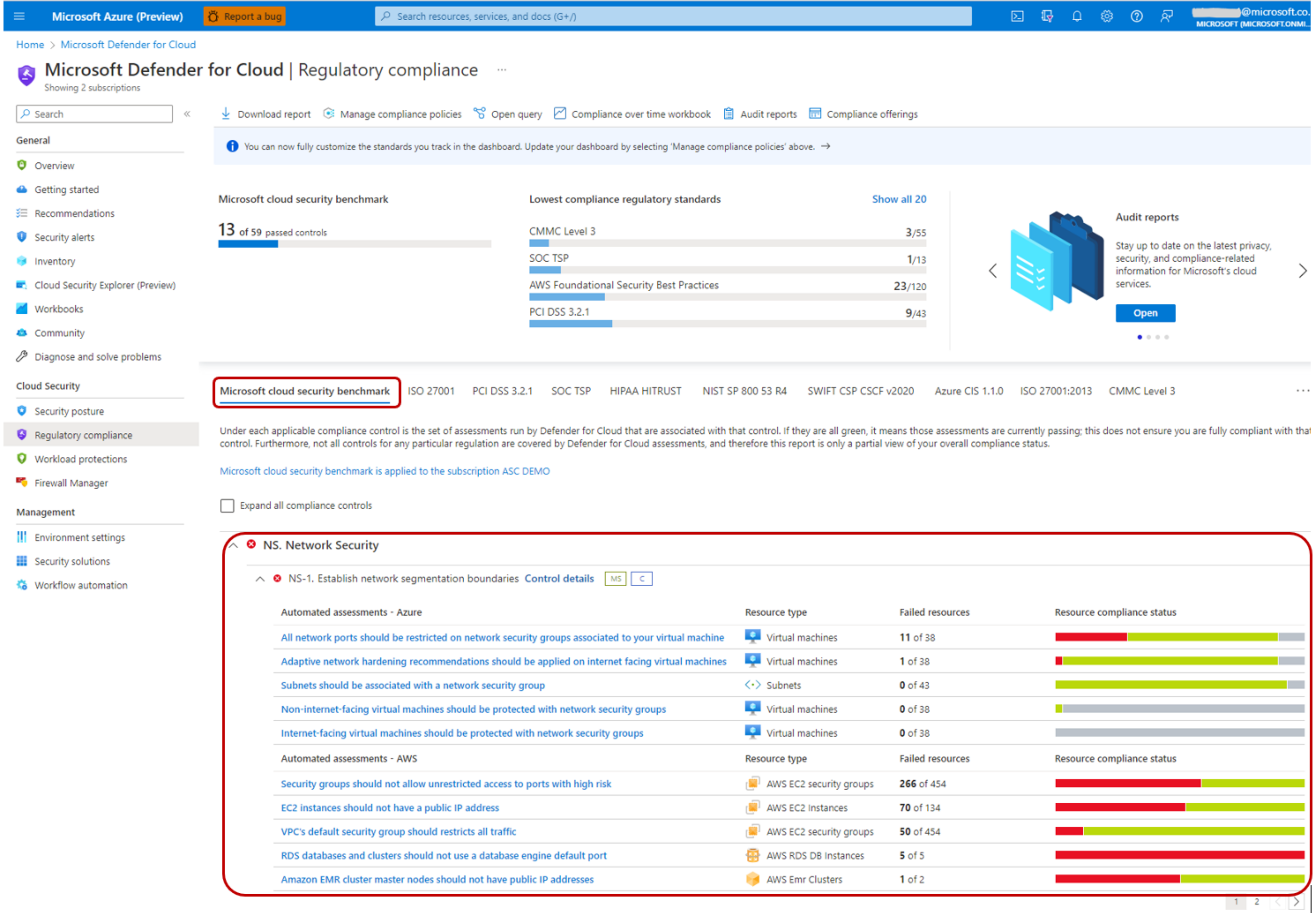
Backup and Recovery (BR)

DevOps Security (DS)

Governance and Strategy (GS)

disclaimer - please refer to source document

Overview of the Microsoft cloud security benchmark | Microsoft Learn



☰
Microsoft Azure (Preview)
Report a bug
Search resources, services, and docs (G+/)
[redacted]@microsoft.co
MICROSOFT (MICROSOFT.ONMI...
Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Regulatory compliance ...

Showing 2 subscriptions

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

Microsoft cloud security benchmark

13 of 59 passed controls

Lowest compliance regulatory standards Show all 20

Standard	Passed
CMMC Level 3	3/55
SOC TSP	1/13
AWS Foundational Security Best Practices	23/120
PCI DSS 3.2.1	9/43

Audit reports

Stay up to date on the latest privacy, security, and compliance-related information for Microsoft's cloud services.

Open

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.

Microsoft cloud security benchmark is applied to the subscription ASC DEMO

☐ Expand all compliance controls

NS. Network Security

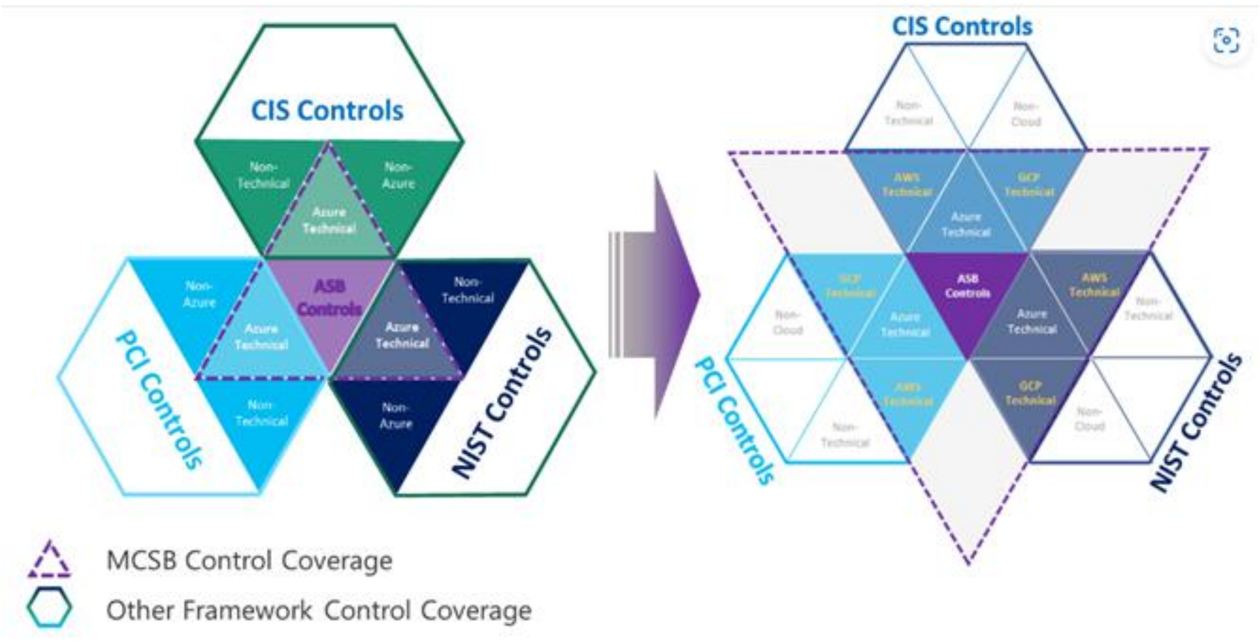
NS-1. Establish network segmentation boundaries **Control details** MS C

Automated assessments - Azure	Resource type	Failed resources	Resource compliance status
All network ports should be restricted on network security groups associated to your virtual machine	Virtual machines	**11** of 38	
Adaptive network hardening recommendations should be applied on internet facing virtual machines	Virtual machines	**1** of 38	
Subnets should be associated with a network security group	Subnets	**0** of 43	
Non-internet-facing virtual machines should be protected with network security groups	Virtual machines	**0** of 38	
Internet-facing virtual machines should be protected with network security groups	Virtual machines	**0** of 38	

Automated assessments - AWS	Resource type	Failed resources	Resource compliance status
Security groups should not allow unrestricted access to ports with high risk	AWS EC2 security groups	**266** of 454	
EC2 instances should not have a public IP address	AWS EC2 Instances	**70** of 134	
VPC's default security group should restricts all traffic	AWS EC2 security groups	**50** of 454	
RDS databases and clusters should not use a database engine default port	AWS RDS DB Instances	**5** of 5	
Amazon EMR cluster master nodes should not have public IP addresses	AWS Emr Clusters	**1** of 2	

[Overview of the Microsoft cloud security benchmark | Microsoft Learn](#)

What's new in Microsoft cloud security benchmark v1



Comprehensive multi-cloud security framework

Automated control monitoring for AWS in Microsoft Defender for Cloud

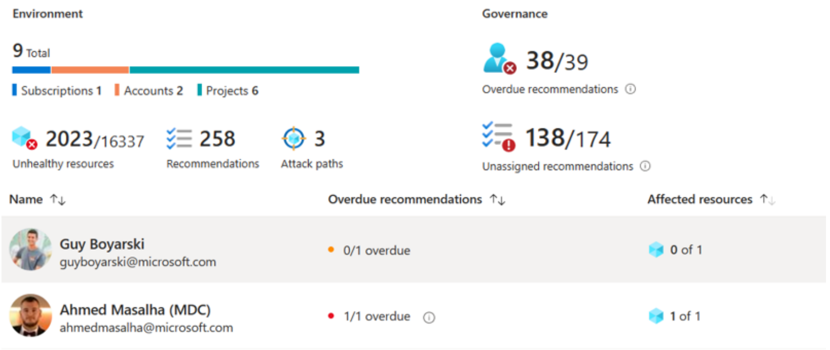
A refresh of the existing Azure guidance and security principles

disclaimer - please refer to source document

Overview of the Microsoft cloud security benchmark | Microsoft Learn

Drive collaboration to improve your security with governance

Security teams can **set accountability** for recommendations, **track their progress, and drive resource owners to action** with notification capabilities



Environment

9 Total

Subscriptions 1 | Accounts 2 | Projects 6

2023/16337 Unhealthy resources

258 Recommendations

3 Attack paths

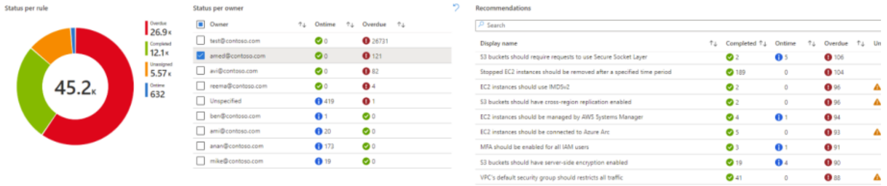
Governance

38/39 Overdue recommendations

138/174 Unassigned recommendations

Name ↑↓	Overdue recommendations ↑↓	Affected resources ↑↓
Guy Boyarski guyboyarski@microsoft.com	● 0/1 overdue	0 of 1
Ahmed Masalha (MDC) ahmedmasalha@microsoft.com	● 1/1 overdue	1 of 1

Workload owners can **focus** on the specific recommendations that require their attention



Status per rule

Status per owner

☐	Owner ↑↓	Ontime ↑↓	Overdue ↑↓
☐	test@contoso.com	✓ 0	! 26731
☑	amed@contoso.com	✓ 0	! 121
☐	avi@contoso.com	✓ 0	! 82
☐	reema@contoso.com	✓ 0	! 4
☐	Unspecified	i 419	! 1
☐	ben@contoso.com	i 1	✓ 0
☐	ami@contoso.com	i 20	✓ 0
☐	anan@contoso.com	i 173	✓ 0
☐	mike@contoso.com	i 19	✓ 0

Recommendations

Search

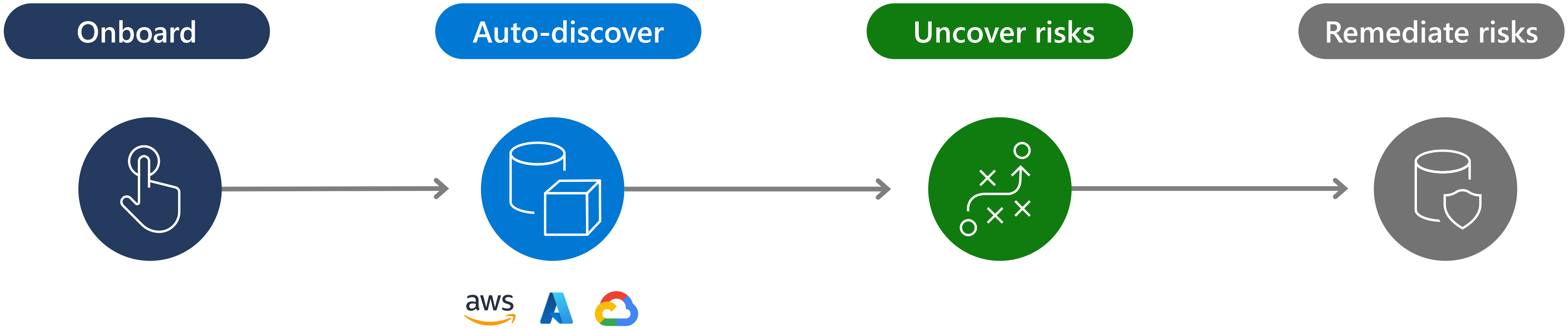
Display name ↑↓	Completed ↑↓	Ontime ↑↓	Overdue ↑↓	Un
S3 buckets should require requests to use Secure Socket Layer	✓ 2	i 5	! 106	
Stopped EC2 instances should be removed after a specified time period	✓ 189	0	! 104	
EC2 instances should use IMDSv2	✓ 2	0	! 96	⚠
S3 buckets should have cross-region replication enabled	✓ 2	0	! 96	⚠
EC2 instances should be managed by AWS Systems Manager	✓ 4	i 1	! 94	
EC2 instances should be connected to Azure Arc	✓ 5	0	! 93	⚠
MFA should be enabled for all IAM users	✓ 3	i 1	! 91	
S3 buckets should have server-side encryption enabled	✓ 19	i 4	! 90	
VPC's default security group should restricts all traffic	✓ 41	0	! 88	⚠

Delegate accountability via built-in governance rules or integrate with ServiceNow ITSM

Fortify sensitive data across clouds

Data-aware security posture

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



Onboard

Auto-discover

Uncover risks

Remediate risks

Agentless onboarding of multicloud data resources, one-click enablement

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

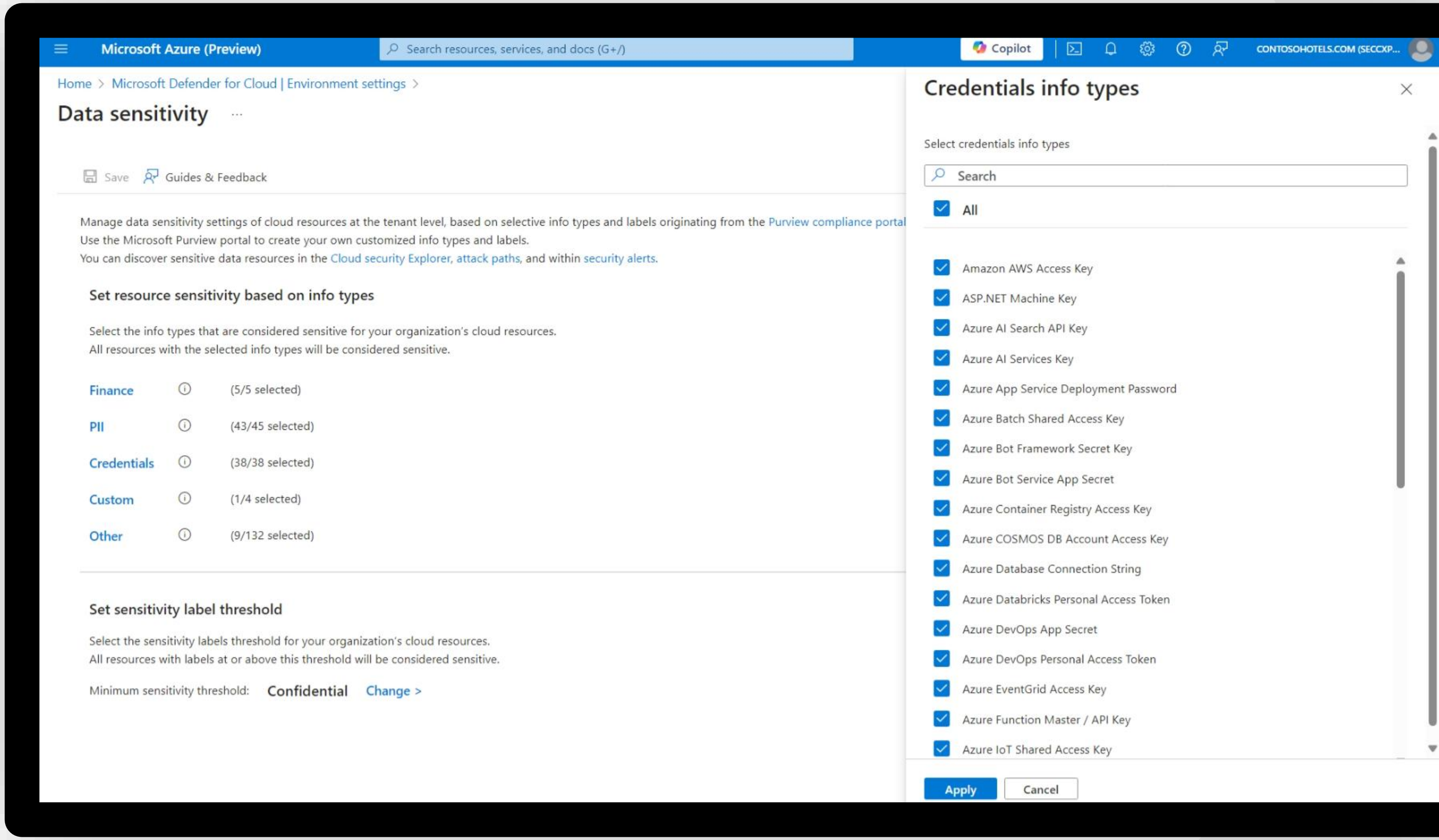
Uncover risks to your data resources through the cloud security explorer and attack path analysis

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

Sensitive data discovery

Data-aware security posture in Defender CSPM

- **Predefined categories of highly sensitive data** such as finance, PII, and credentials
- **Built-in scanning with support** for 100+ sensitive information types
- **Leverage custom sensitive information types** or existing sensitivity labels from Purview Information Protection


Microsoft Azure (Preview)
Search resources, services, and docs (G+/)
Copilot
CONTOSOHOTELS.COM (SECCXP...
Home > Microsoft Defender for Cloud | Environment settings >
Save
Guides & Feedback

Data sensitivity ···

Manage data sensitivity settings of cloud resources at the tenant level, based on selective info types and labels originating from the Purview compliance portal
Use the Microsoft Purview portal to create your own customized info types and labels.
You can discover sensitive data resources in the Cloud security Explorer, attack paths, and within security alerts.

Set resource sensitivity based on info types

Select the info types that are considered sensitive for your organization's cloud resources.
All resources with the selected info types will be considered sensitive.

Finance	(5/5 selected)
PII	(43/45 selected)
Credentials	(38/38 selected)
Custom	(1/4 selected)
Other	(9/132 selected)

Set sensitivity label threshold

Select the sensitivity labels threshold for your organization's cloud resources.
All resources with labels at or above this threshold will be considered sensitive.

Minimum sensitivity threshold: Confidential Change >

Credentials info types

Select credentials info types

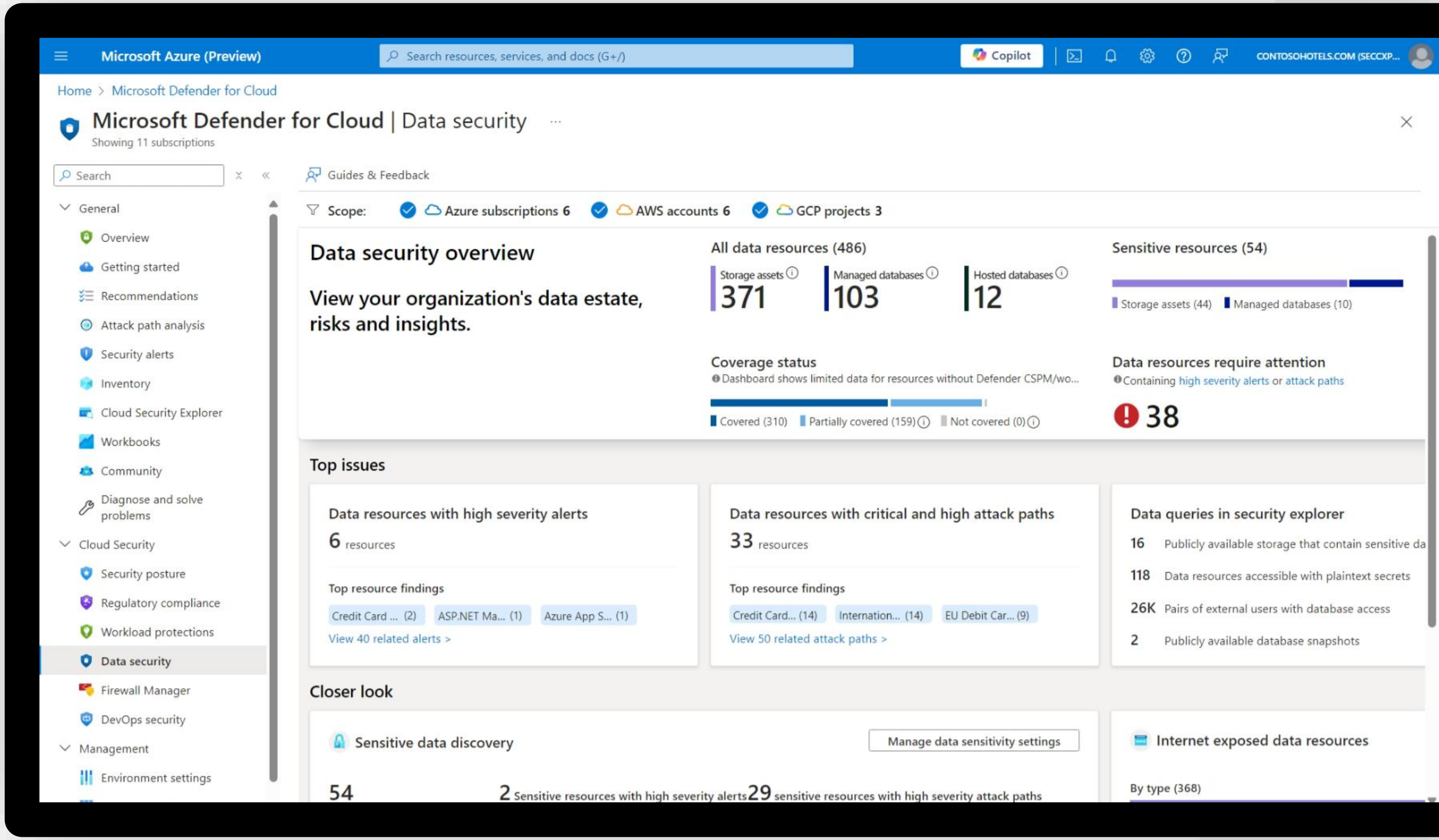
Search

- ☑ All
- ☑ Amazon AWS Access Key
- ☑ ASP.NET Machine Key
- ☑ Azure AI Search API Key
- ☑ Azure AI Services Key
- ☑ Azure App Service Deployment Password
- ☑ Azure Batch Shared Access Key
- ☑ Azure Bot Framework Secret Key
- ☑ Azure Bot Service App Secret
- ☑ Azure Container Registry Access Key
- ☑ Azure COSMOS DB Account Access Key
- ☑ Azure Database Connection String
- ☑ Azure Databricks Personal Access Token
- ☑ Azure DevOps App Secret
- ☑ Azure DevOps Personal Access Token
- ☑ Azure EventGrid Access Key
- ☑ Azure Function Master / API Key
- ☑ Azure IoT Shared Access Key

View insights across your sensitive data stores

Data security dashboard

- **Inventory overview** of your multicloud cloud data estate
- **View top alerts, attack paths, and queries** related to sensitive data stores
- **Discover trends in discovered data stores** such as quantity of sensitive data stores, sensitive information types, sensitivity labels



Microsoft Defender for Cloud | Data security

Showing 11 subscriptions

Scope: ✓ Azure subscriptions 6 ✓ AWS accounts 6 ✓ GCP projects 3

Data security overview

View your organization's data estate, risks and insights.

All data resources (486)

Storage assets	Managed databases	Hosted databases
371	103	12

Sensitive resources (54)

Storage assets (44) Managed databases (10)

Coverage status

Dashboard shows limited data for resources without Defender CSPM/wo...

Covered (310) Partially covered (159) Not covered (0)

Data resources require attention

Containing high severity alerts or attack paths

38

Top issues

Data resources with high severity alerts

6 resources

Top resource findings

Credit Card ... (2) ASP.NET Ma... (1) Azure App S... (1)

View 40 related alerts >

Data resources with critical and high attack paths

33 resources

Top resource findings

Credit Card... (14) Internation... (14) EU Debit Car... (9)

View 50 related attack paths >

Data queries in security explorer

16	Publicly available storage that contain sensitive da
118	Data resources accessible with plaintext secrets
26K	Pairs of external users with database access
2	Publicly available database snapshots

Closer look

Sensitive data discovery

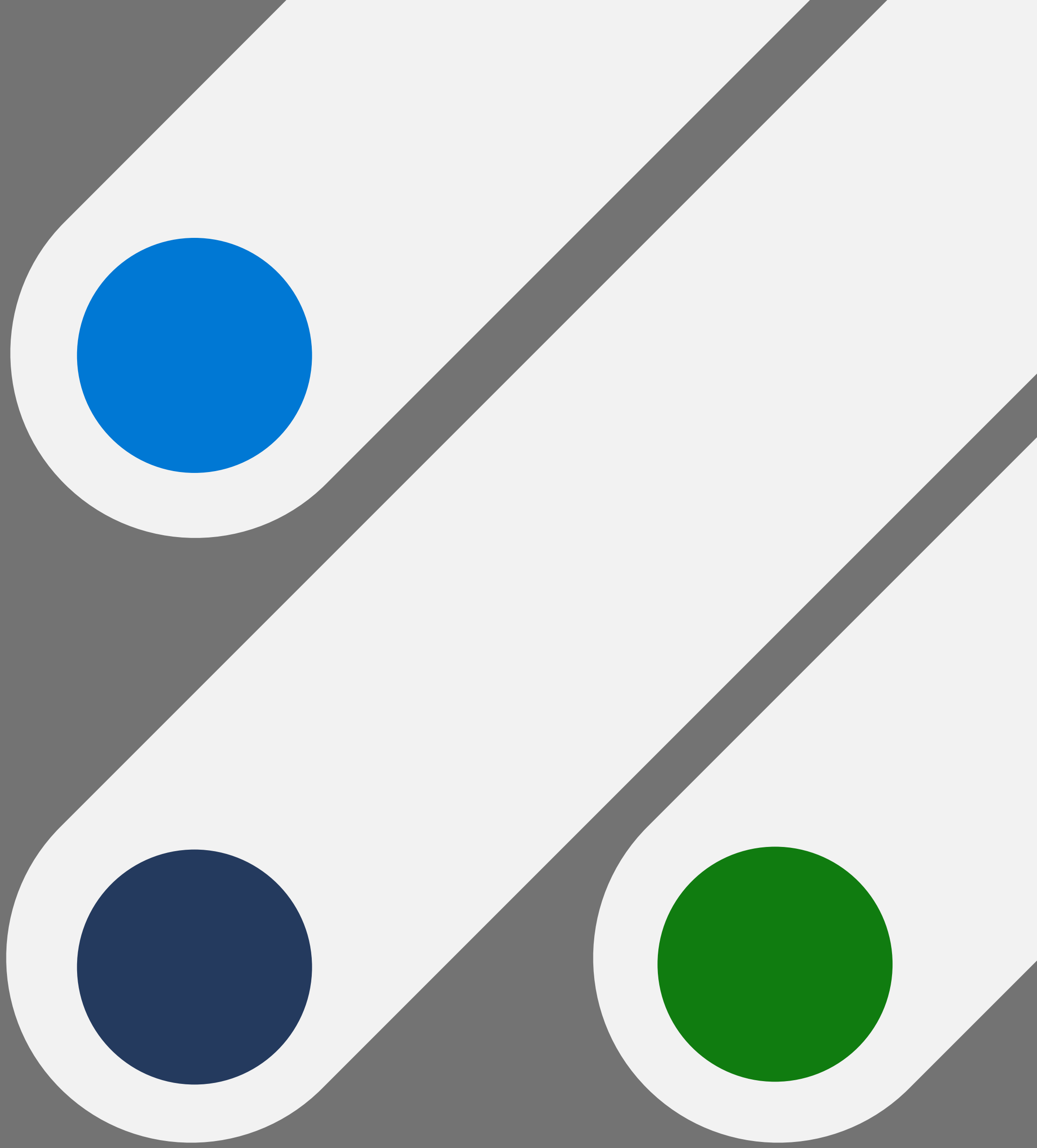
54

2 Sensitive resources with high severity alerts 29 sensitive resources with high severity attack paths

Internet exposed data resources

By type (368)

Prevent future risks by fixing in code



Extend security into software development lifecycle

Security

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

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

Bridging the gap between DevOps and security teams

« »

Development

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

GitHub Advanced Security
Native code security with
GitHub and Azure DevOps

Accelerate risk exploration and mitigation with Microsoft Copilot in Defender for Cloud

In-preview

Simplify the complex

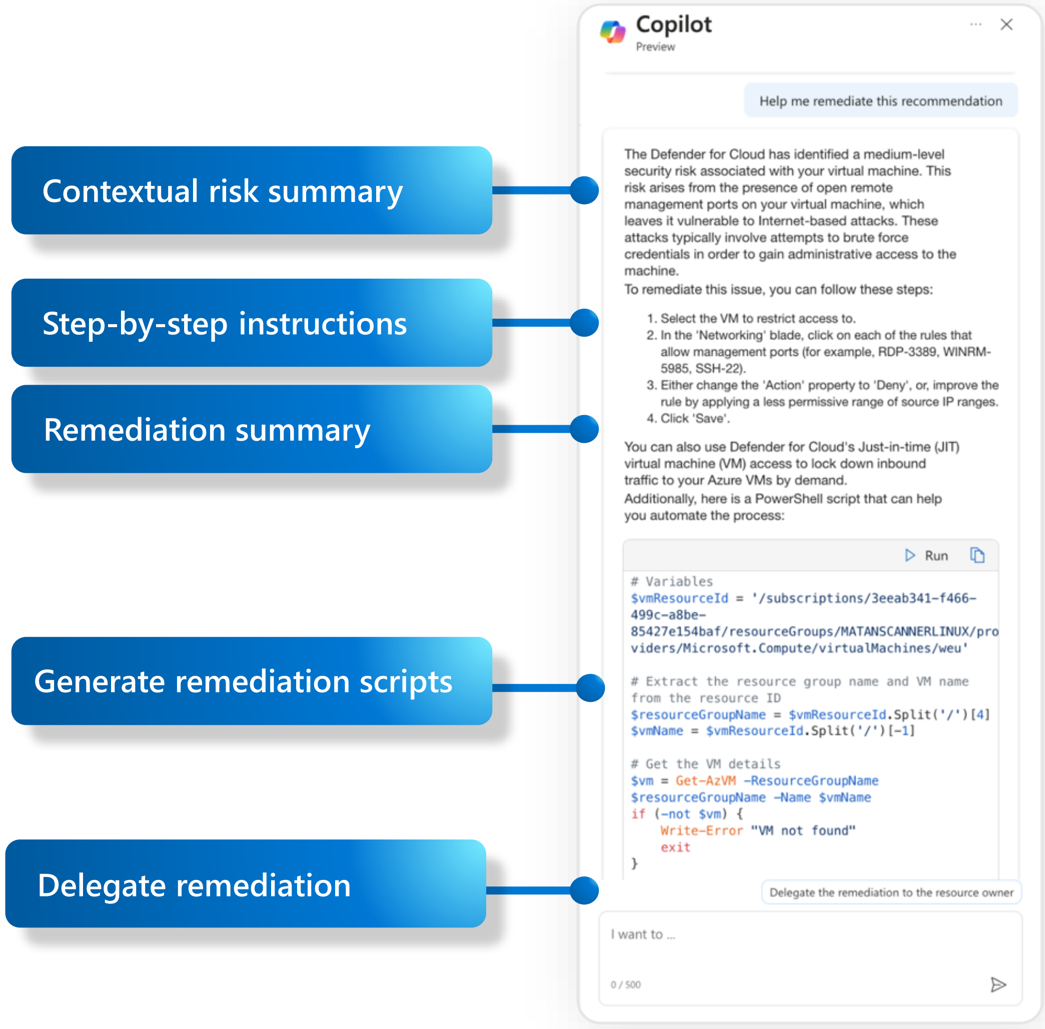
- Risk exploration with natural language queries
- Prioritize multicloud risks based on impact

Catch what others miss

- Analyze risks at scale and get predictive guidance
- Drill into your vulnerabilities

Accelerate remediation

- Generate and deploy remediation actions and scripts
- Delegate remediation via email or pull requests



Contextual risk summary

Step-by-step instructions

Remediation summary

Generate remediation scripts

Delegate remediation

Help me remediate this recommendation

The Defender for Cloud has identified a medium-level security risk associated with your virtual machine. This risk arises from the presence of open remote management ports on your virtual machine, which leaves it vulnerable to Internet-based attacks. These attacks typically involve attempts to brute force credentials in order to gain administrative access to the machine.

To remediate this issue, you can follow these steps:

1. Select the VM to restrict access to.
2. In the 'Networking' blade, click on each of the rules that allow management ports (for example, RDP-3389, WINRM-5985, SSH-22).
3. Either change the 'Action' property to 'Deny', or, improve the rule by applying a less permissive range of source IP ranges.
4. Click 'Save'.

You can also use Defender for Cloud's Just-in-time (JIT) virtual machine (VM) access to lock down inbound traffic to your Azure VMs by demand.

Additionally, here is a PowerShell script that can help you automate the process:

```
# Variables
$vmResourceId = '/subscriptions/3eeab341-f466-
499c-a8be-
85427e154baf/resourceGroups/MATANSCANNERLINUX/pro
viders/Microsoft.Compute/virtualMachines/weu'

# Extract the resource group name and VM name
from the resource ID
$resourceGroupName = $vmResourceId.Split('/')[4]
$vmName = $vmResourceId.Split('/')[-1]

# Get the VM details
$vm = Get-AzVM -ResourceGroupName
$resourceGroupName -Name $vmName
if (-not $vm) {
    Write-Error "VM not found"
    exit
}
```

Delegate the remediation to the resource owner

Microsoft Security

A selection of resources:

https://aka.ms/mcra

Cloud Security Posture Management (CSPM) - Microsoft Defender for Cloud | Microsoft Learn
What's new in Microsoft Defender for Cloud features - Microsoft Defender for Cloud | Microsoft Learn
Pricing - Microsoft Defender for Cloud | Microsoft Azure

https://securitypartners.transform.microsoft.com/multicloud
Partner Incentives
Cloud Security specialization

Microsoft Security

Thank you