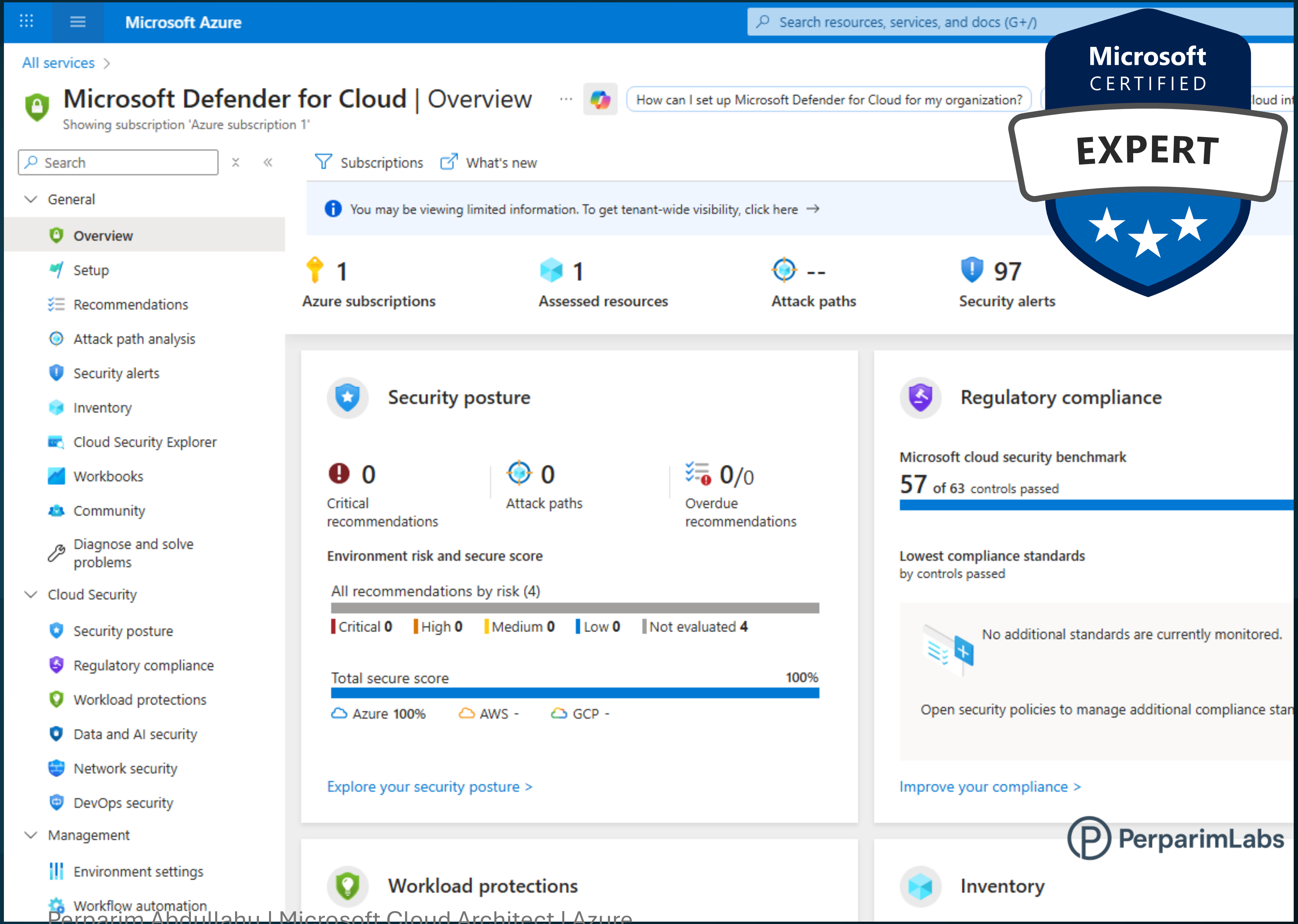
Elevate Your Cloud Security Posture with Microsoft Defender for Cloud

- CSPM
- Secure Score
- Regulatory Compliance
- Workload Protection



Microsoft Azure

Search resources, services, and docs (G+/)

All services >

Microsoft Defender for Cloud | Overview

Showing subscription 'Azure subscription 1'

How can I set up Microsoft Defender for Cloud for my organization?

Search

General
- Overview
- Setup
- Recommendations
- Attack path analysis
- Security alerts
- Inventory
- Cloud Security Explorer
- Workbooks
- Community
- Diagnose and solve problems

Cloud Security
- Security posture
- Regulatory compliance
- Workload protections
- Data and AI security
- Network security
- DevOps security

Management
- Environment settings
- Workflow automation

Subscriptions   What's new

You may be viewing limited information. To get tenant-wide visibility, click here →

1	1	--	97
Azure subscriptions	Assessed resources	Attack paths	Security alerts

Security posture

0	0	0/0
Critical recommendations	Attack paths	Overdue recommendations

Environment risk and secure score

All recommendations by risk (4)

Critical 0 | High 0 | Medium 0 | Low 0 | Not evaluated 4

Total secure score 100%

Azure 100%   AWS -   GCP -

Explore your security posture >

Regulatory compliance

Microsoft cloud security benchmark

57 of 63 controls passed

Lowest compliance standards by controls passed

No additional standards are currently monitored.

Open security policies to manage additional compliance stan

Improve your compliance >

Workload protections

Inventory

Microsoft CERTIFIED EXPERT

PerparimLabs

What Is Cloud Security Posture Management (CSPM)?

CSPM helps organizations continuously evaluate and improve their cloud security posture.

Key capabilities:

- Detect misconfigurations and security gaps
- Map your environment to standards (NIST, CIS, PCI, ISO)
- Provide actionable recommendations
- Strengthen identity, data, apps & infrastructure security
- Reduce attack paths across workloads

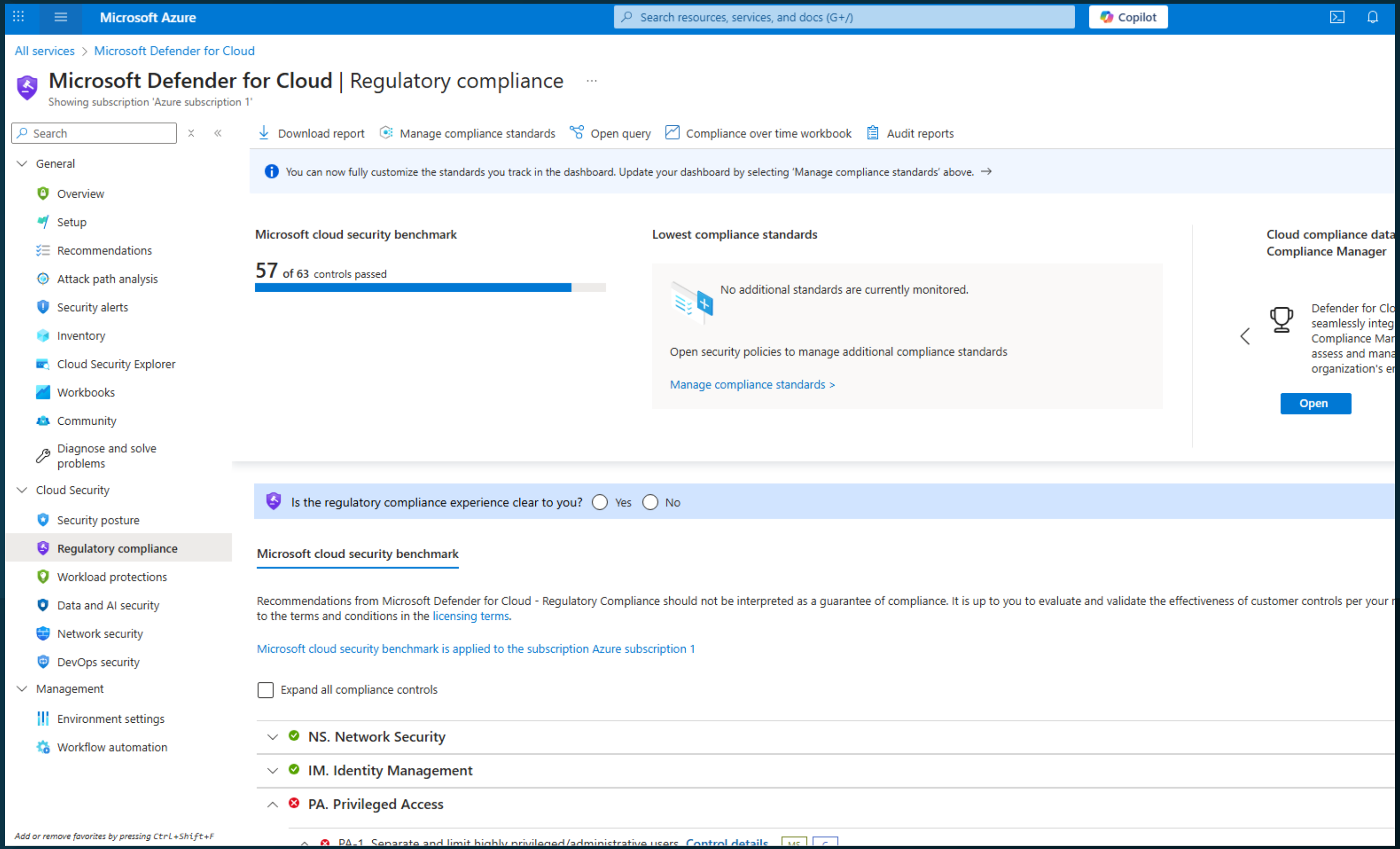
PerparimLabs

Regulatory Compliance Overview

Microsoft Defender for Cloud includes a **Regulatory Compliance dashboard** showing your security posture against industry frameworks.

You can view:

- Total controls passed vs. controls failed
- Each framework’s compliance percentage
- Detailed control-level recommendations
- Required actions to strengthen security



Microsoft Defender for Cloud | Regulatory compliance

Showing subscription 'Azure subscription 1'

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

Microsoft cloud security benchmark

57 of 63 controls passed

Lowest compliance standards

No additional standards are currently monitored.

Open security policies to manage additional compliance standards

Manage compliance standards >

Cloud compliance data
Compliance Manager

Defender for Clo
seamlessly integ
Compliance Mar
assess and mana
organization's e

Is the regulatory compliance experience clear to you? ○ Yes ○ No

Microsoft cloud security benchmark

Recommendations from Microsoft Defender for Cloud - Regulatory Compliance should not be interpreted as a guarantee of compliance. It is up to you to evaluate and validate the effectiveness of customer controls per your r to the terms and conditions in the licensing terms.

Microsoft cloud security benchmark is applied to the subscription Azure subscription 1

□ Expand all compliance controls

✓ NS. Network Security

✓ IM. Identity Management

✗ PA. Privileged Access

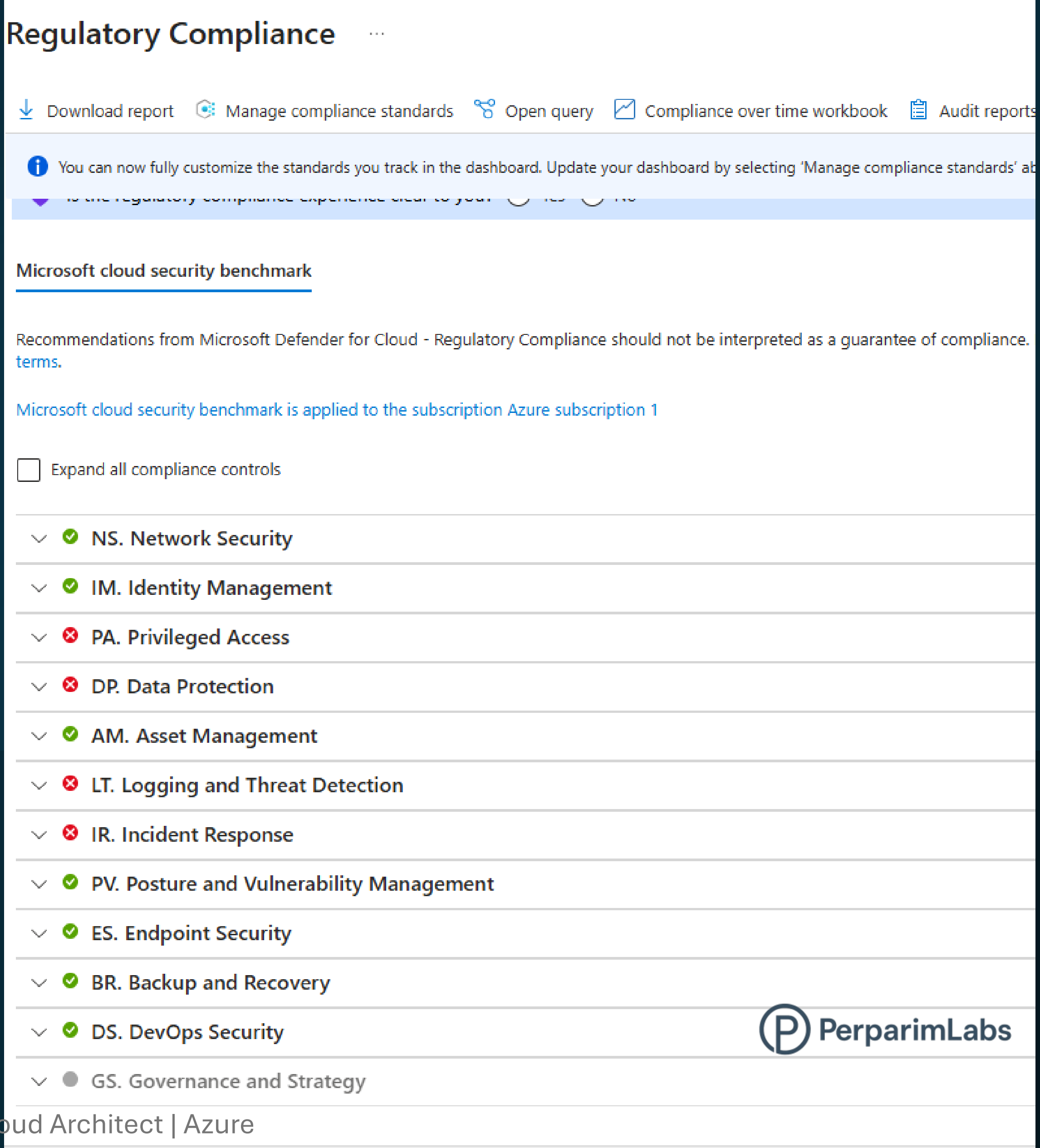
✗ PA-1. Separate and limit highly privileged/administrative users Control details

Microsoft Cloud Security Benchmark (MCSB)

MCSB is Microsoft’s unified security framework for securing cloud workloads.

MCSB provides:

- A Microsoft-defined baseline for cloud security
- Mapping to NIST, CIS, PCI-DSS, ISO 27001 & more
- Secure-by-default guidance for identity, network, logging, workloads
- A measurable way to evaluate your Azure environment



Regulatory Compliance ···

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

Is the regulatory compliance experience clear to you? ○ Yes ○ No

Microsoft cloud security benchmark

Recommendations from Microsoft Defender for Cloud - Regulatory Compliance should not be interpreted as a guarantee of compliance. terms.

Microsoft cloud security benchmark is applied to the subscription Azure subscription 1

□ Expand all compliance controls

- ✓ NS. Network Security
- ✓ IM. Identity Management
- ✗ PA. Privileged Access
- ✗ DP. Data Protection
- ✓ AM. Asset Management
- ✗ LT. Logging and Threat Detection
- ✗ IR. Incident Response
- ✓ PV. Posture and Vulnerability Management
- ✓ ES. Endpoint Security
- ✓ BR. Backup and Recovery
- ✓ DS. DevOps Security
- ● GS. Governance and Strategy

Understanding Benchmark Controls

When expanding an MCSB category, you can view:

✓ Controls you meet

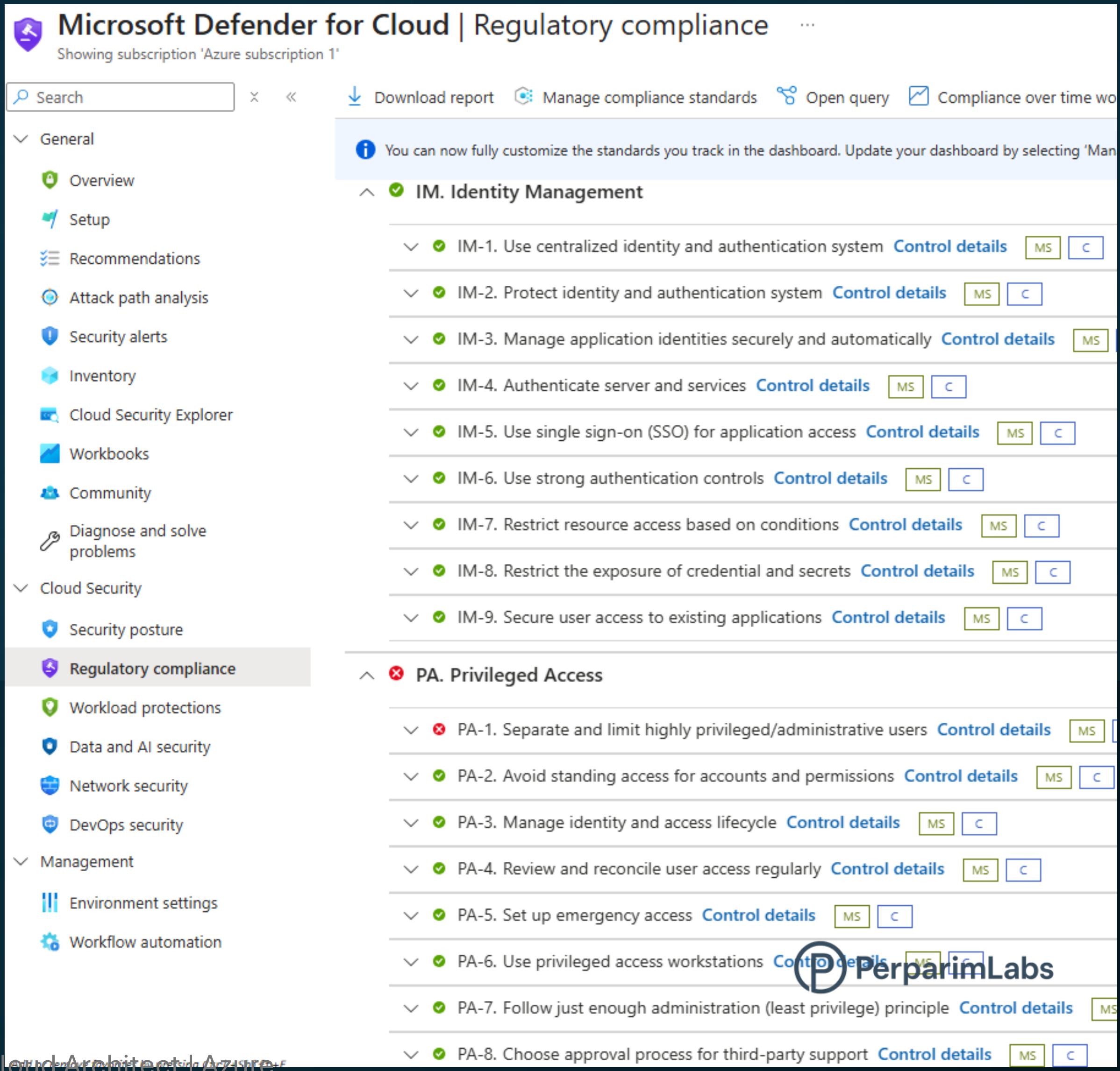
✓ Controls you fail

✓ Control details (evidence, requirements, automated checks)

✓ Microsoft actions (auto-/semi-automated in future updates)

✓ Manual actions your team must configure

Architect note:
A fresh tenant will naturally fail most controls — this is expected and realistic.



Microsoft Defender for Cloud | Regulatory compliance ...

Showing subscription 'Azure subscription 1'

You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Man

✓ 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
- ✓ IM-4. Authenticate server and services Control details MS C
- ✓ IM-5. Use single sign-on (SSO) for application access Control details MS C
- ✓ IM-6. Use strong authentication controls Control details MS C
- ✓ IM-7. Restrict resource access based on conditions Control details MS C
- ✓ IM-8. Restrict the exposure of credential and secrets Control details MS C
- ✓ IM-9. Secure user access to existing applications Control details MS C

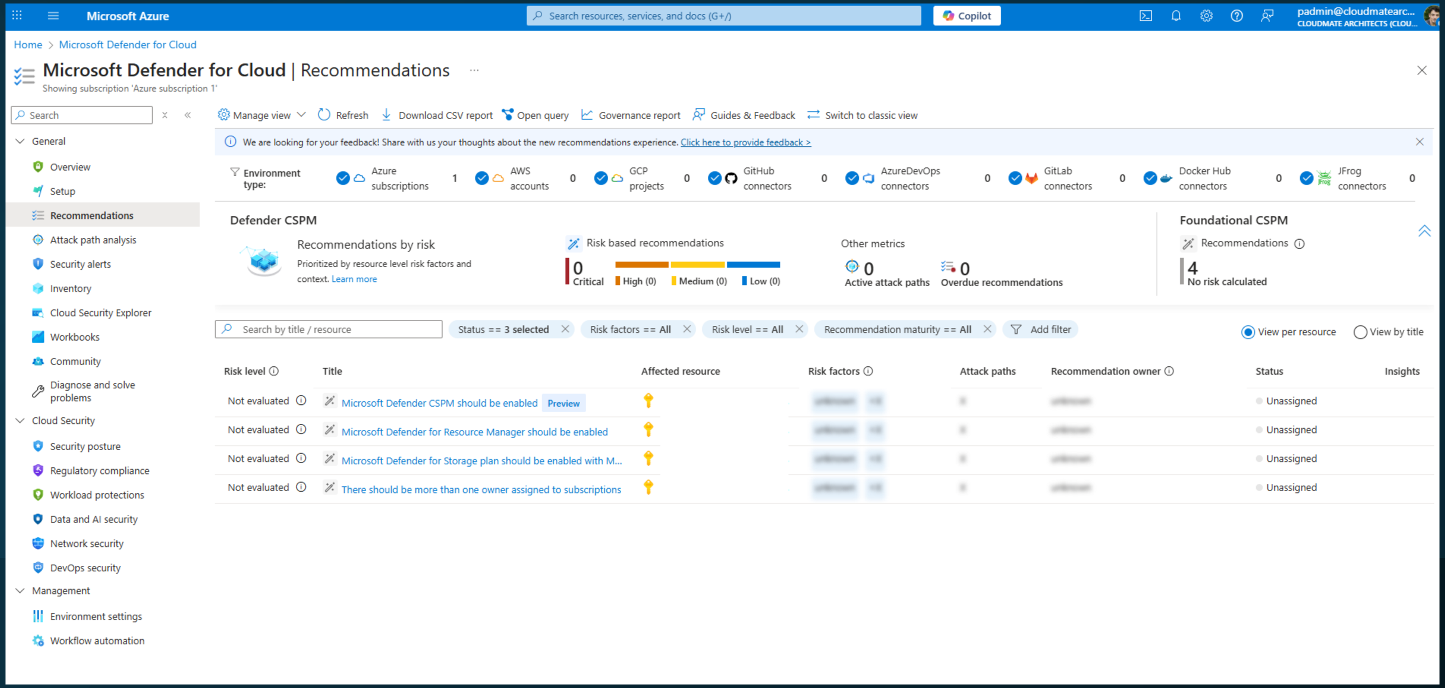
✗ PA. Privileged Access

- ✗ PA-1. Separate and limit highly privileged/administrative users Control details MS
- ✓ PA-2. Avoid standing access for accounts and permissions Control details MS C
- ✓ PA-3. Manage identity and access lifecycle Control details MS C
- ✓ PA-4. Review and reconcile user access regularly Control details MS C
- ✓ PA-5. Set up emergency access Control details MS C
- ✓ PA-6. Use privileged access workstations Control details MS C
- ✓ PA-7. Follow just enough administration (least privilege) principle Control details MS
- ✓ PA-8. Choose approval process for third-party support Control details MS C

Strengthening Compliance

Microsoft Defender for Cloud guides you in improving compliance by:

- Showing exactly *what needs fixing*
- Explaining why each control matters
- Providing remediation steps
- Highlighting automated vs. manual actions
- Tracking progress over time



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
padmin@cloudmatearc...
CLOUDMATE ARCHITECTS (CLOU...

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Recommendations

Showing subscription 'Azure subscription 1'

We are looking for your feedback! Share with us your thoughts about the new recommendations experience. Click here to provide feedback >

Environment type: Azure subscriptions 1 · AWS accounts 0 · GCP projects 0 · GitHub connectors 0 · AzureDevOps connectors 0 · GitLab connectors 0 · Docker Hub connectors 0 · JFrog connectors 0

Defender CSPM

Recommendations by risk

Prioritized by resource level risk factors and context. Learn more

Risk based recommendations: 0 Critical · High (0) · Medium (0) · Low (0)

Other metrics: 0 Active attack paths · 0 Overdue recommendations

Foundational CSPM

Recommendations: 4 No risk calculated

Search by title / resource · Status == 3 selected · Risk factors == All · Risk level == All · Recommendation maturity == All · Add filter

● View per resource ○ View by title

Risk level	Title	Affected resource	Risk factors	Attack paths	Recommendation owner	Status	Insights
Not evaluated	Microsoft Defender CSPM should be enabled Preview					Unassigned	
Not evaluated	Microsoft Defender for Resource Manager should be enabled					Unassigned	
Not evaluated	Microsoft Defender for Storage plan should be enabled with M...					Unassigned	
Not evaluated	There should be more than one owner assigned to subscriptions					Unassigned	

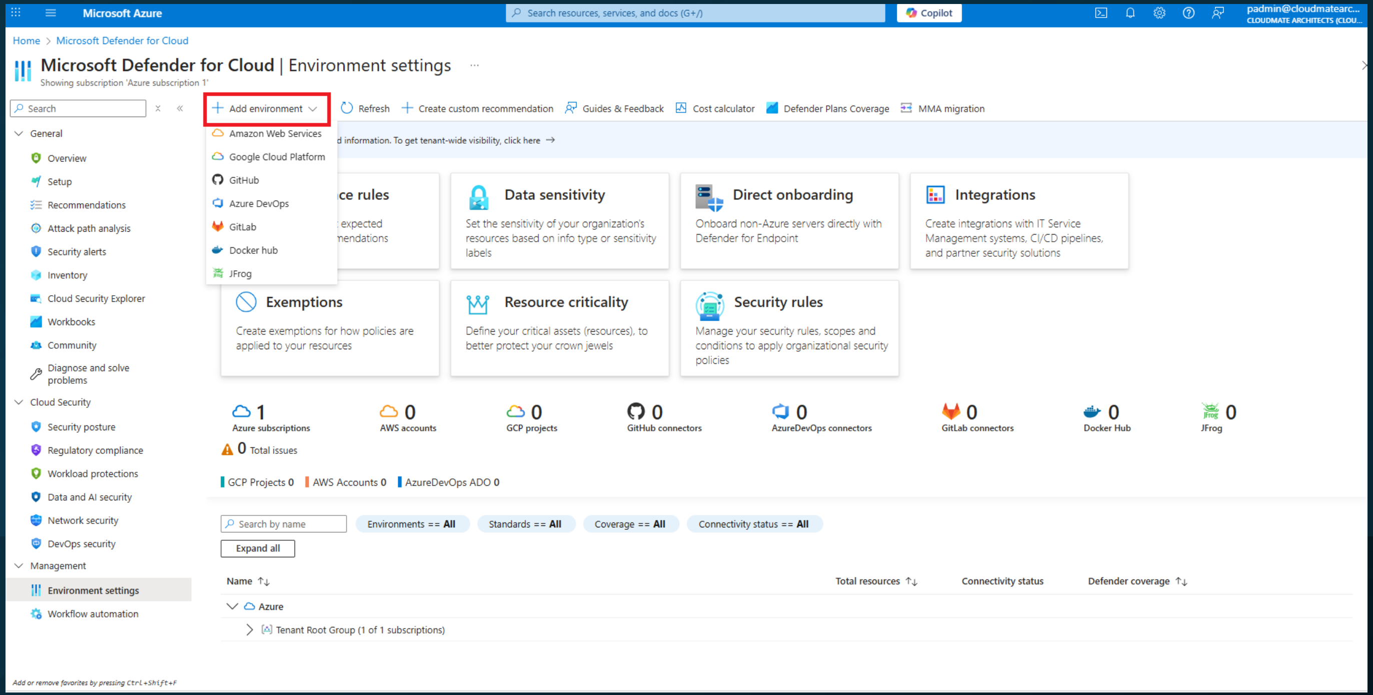
Multicloud Compliance

Defender for Cloud supports **Azure, AWS, GCP, GitHub, Azure DevOps**.

Through **Manage Compliance Policies**, you can:

- Add multicloud environments
- Evaluate compliance across all clouds
- Centralize governance into a single pane of glass
- Improve posture consistently across hybrid setups

This is powerful for enterprise and SC-100 architecture.



Microsoft Defender for Cloud | Environment settings

Showing subscription 'Azure subscription 1'

d information. To get tenant-wide visibility, click here →

ce rules

expected
mendations

Data sensitivity

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

Direct onboarding

Onboard non-Azure servers directly with Defender for Endpoint

Integrations

Create integrations with IT Service Management systems, CI/CD pipelines, and partner security solutions

Exemptions

Create exemptions for how policies are applied to your resources

Resource criticality

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

Security rules

Manage your security rules, scopes and conditions to apply organizational security policies

1 Azure subscriptions | 0 AWS accounts | 0 GCP projects | 0 GitHub connectors | 0 AzureDevOps connectors | 0 GitLab connectors | 0 Docker Hub | 0 JFrog

0 Total issues

GCP Projects 0 | AWS Accounts 0 | AzureDevOps ADO 0

Environments == All | Standards == All | Coverage == All | Connectivity status == All

Name ↑↓	Total resources ↑↓	Connectivity status	Defender coverage ↑↓
Azure			
Tenant Root Group (1 of 1 subscriptions)			

Add or remove favorites by pressing Ctrl+Shift+F

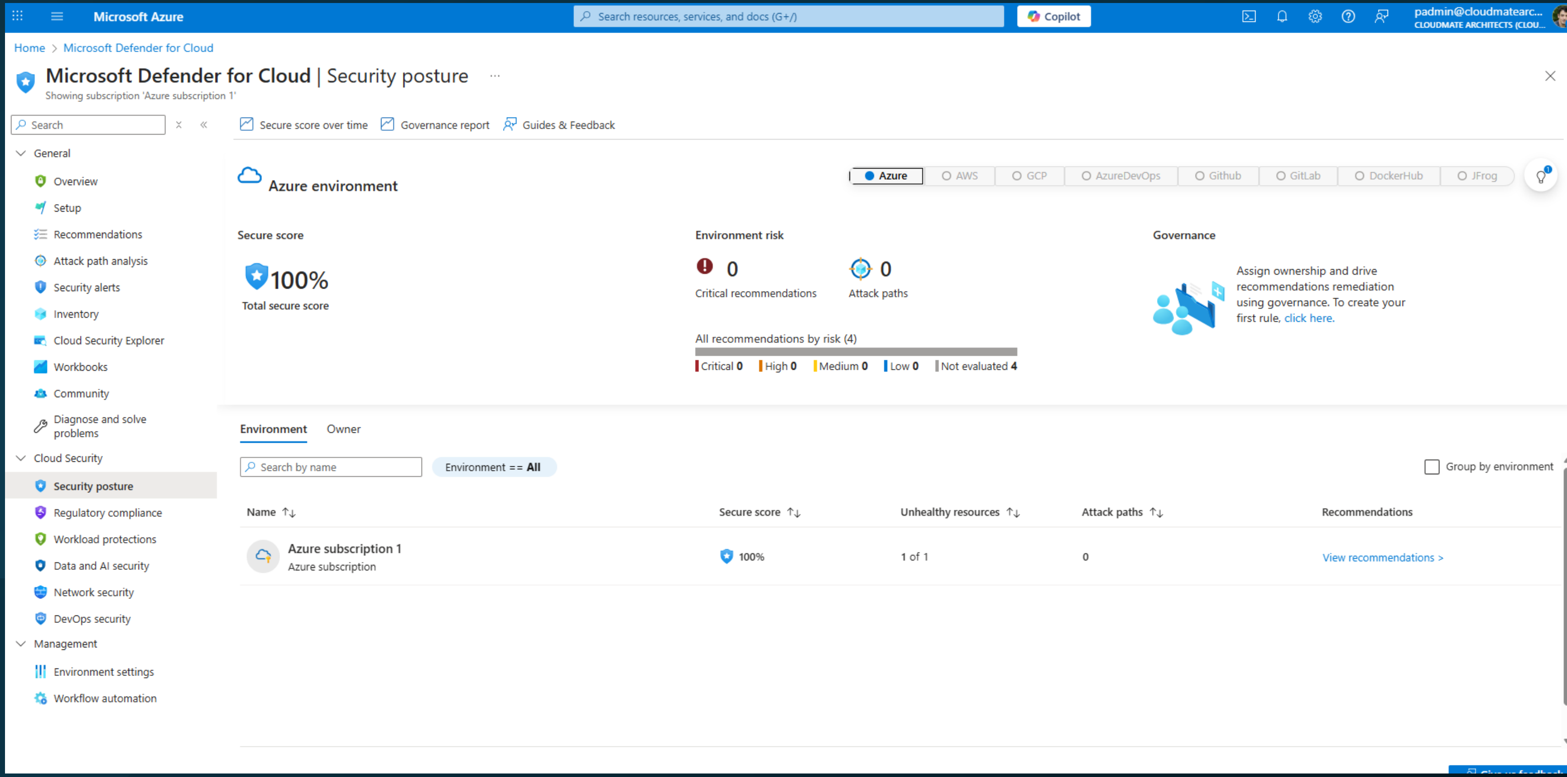
What Is Secure Score?

Secure Score measures how protected your cloud environment is.

Evaluates:

- Identity controls
- Resource configurations
- Data protections
- App security
- Infrastructure posture

A low score in a new tenant is **normal**.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
padmin@cloudmatearc...
CLOUDMATE ARCHITECTS (CLOU...
Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud | Security posture

Showing subscription 'Azure subscription 1'

Azure environment

Secure score

100%

Total secure score

Environment risk

0 Critical recommendations

0 Attack paths

All recommendations by risk (4)

Critical 0 | High 0 | Medium 0 | Low 0 | Not evaluated 4

Governance

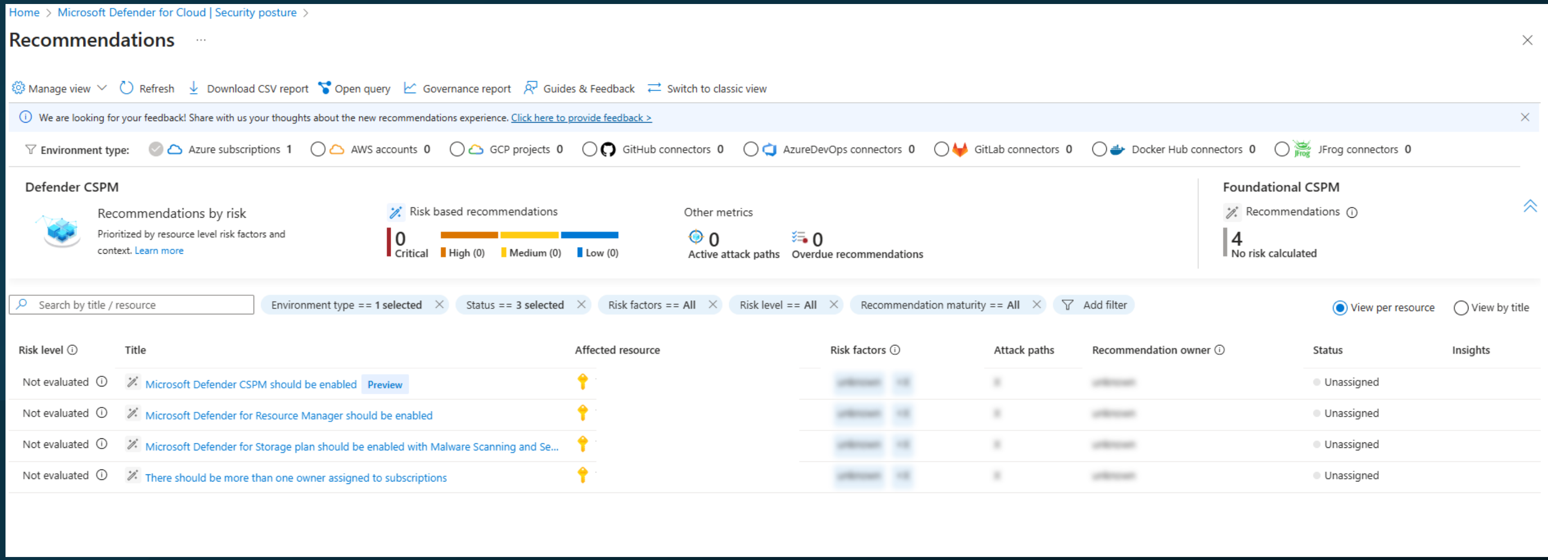
Assign ownership and drive recommendations remediation using governance. To create your first rule, click here.

Name	Secure score	Unhealthy resources	Attack paths	Recommendations
Azure subscription 1 Azure subscription	100%	1 of 1	0	View recommendations >

Using Recommendations to Strengthen Security

Each recommendation includes:

- Affected resources
- Impact on Secure Score
- Step-by-step remediation
- Alternative options (exemptions)



Home > Microsoft Defender for Cloud | Security posture >

Recommendations ···

Manage view ⌄ | Refresh | Download CSV report | Open query | Governance report | Guides & Feedback | Switch to classic view

We are looking for your feedback! Share with us your thoughts about the new recommendations experience. Click here to provide feedback >

Environment type: ● Azure subscriptions 1 ○ AWS accounts 0 ○ GCP projects 0 ○ GitHub connectors 0 ○ AzureDevOps connectors 0 ○ GitLab connectors 0 ○ Docker Hub connectors 0 ○ JFrog connectors 0

Defender CSPM

Recommendations by risk

Prioritized by resource level risk factors and context. Learn more

Risk based recommendations: 0 Critical | High (0) | Medium (0) | Low (0)

Other metrics: 0 Active attack paths | 0 Overdue recommendations

Foundational CSPM

Recommendations: 4 No risk calculated

Search by title / resource | Environment type == 1 selected | Status == 3 selected | Risk factors == All | Risk level == All | Recommendation maturity == All | Add filter

● View per resource ○ View by title

Risk level	Title	Affected resource	Risk factors	Attack paths	Recommendation owner	Status	Insights
Not evaluated	Microsoft Defender CSPM should be enabled Preview		[redacted]	[redacted]	[redacted]	Unassigned	
Not evaluated	Microsoft Defender for Resource Manager should be enabled		[redacted]	[redacted]	[redacted]	Unassigned	
Not evaluated	Microsoft Defender for Storage plan should be enabled with Malware Scanning and Se...		[redacted]	[redacted]	[redacted]	Unassigned	
Not evaluated	There should be more than one owner assigned to subscriptions		[redacted]	[redacted]	[redacted]	Unassigned	

Accounts with Owner permissions must have MFA enabled.

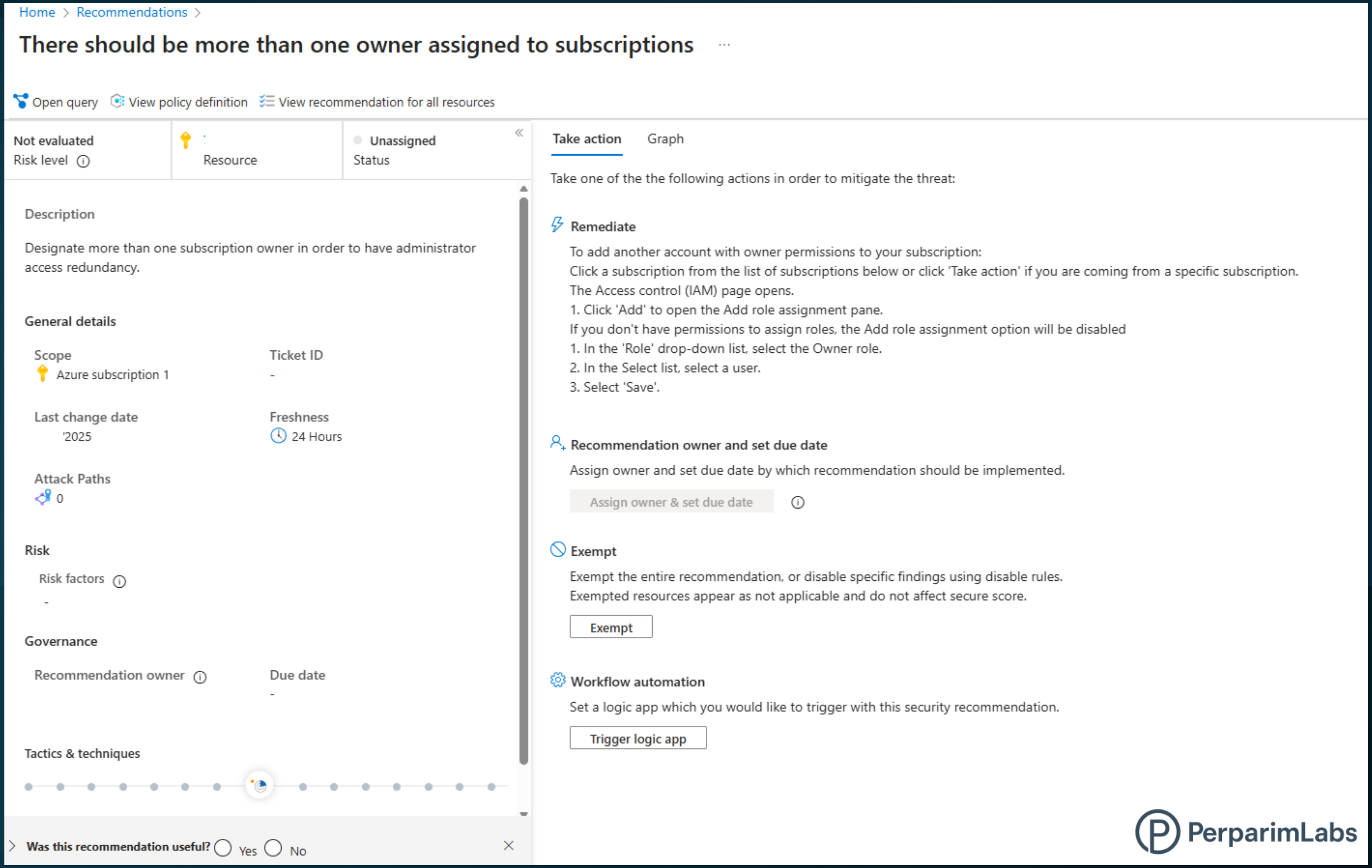
Recommendations guide you from misconfiguration → secure posture.

Security Improvement View

Defender for Cloud → Recommendations

You should now see:

The warning **“There should be more than one owner assigned to subscriptions”**



Home > Recommendations >

There should be more than one owner assigned to subscriptions ...

Open query | View policy definition | View recommendation for all resources

Not evaluated
Risk level ⓘ

Resource

Unassigned
Status

Description

Designate more than one subscription owner in order to have administrator access redundancy.

General details

Scope Azure subscription 1	Ticket ID -
Last change date '2025	Freshness 24 Hours
Attack Paths 0	

Risk

Risk factors ⓘ
-

Governance

Recommendation owner ⓘ	Due date -

Tactics & techniques

Was this recommendation useful? ○ Yes ○ No

Take action | Graph

Take one of the the following actions in order to mitigate the threat:

Remediate

To add another account with owner permissions to your subscription:
Click a subscription from the list of subscriptions below or click 'Take action' if you are coming from a specific subscription.
The Access control (IAM) page opens.
1. Click 'Add' to open the Add role assignment pane.
If you don't have permissions to assign roles, the Add role assignment option will be disabled
1. In the 'Role' drop-down list, select the Owner role.
2. In the Select list, select a user.
3. Select 'Save'.

Recommendation owner and set due date

Assign owner and set due date by which recommendation should be implemented.

Assign owner & set due date ⓘ

Exempt

Exempt the entire recommendation, or disable specific findings using disable rules.
Exempted resources appear as not applicable and do not affect secure score.

Exempt

Workflow automation

Set a logic app which you would like to trigger with this security recommendation.

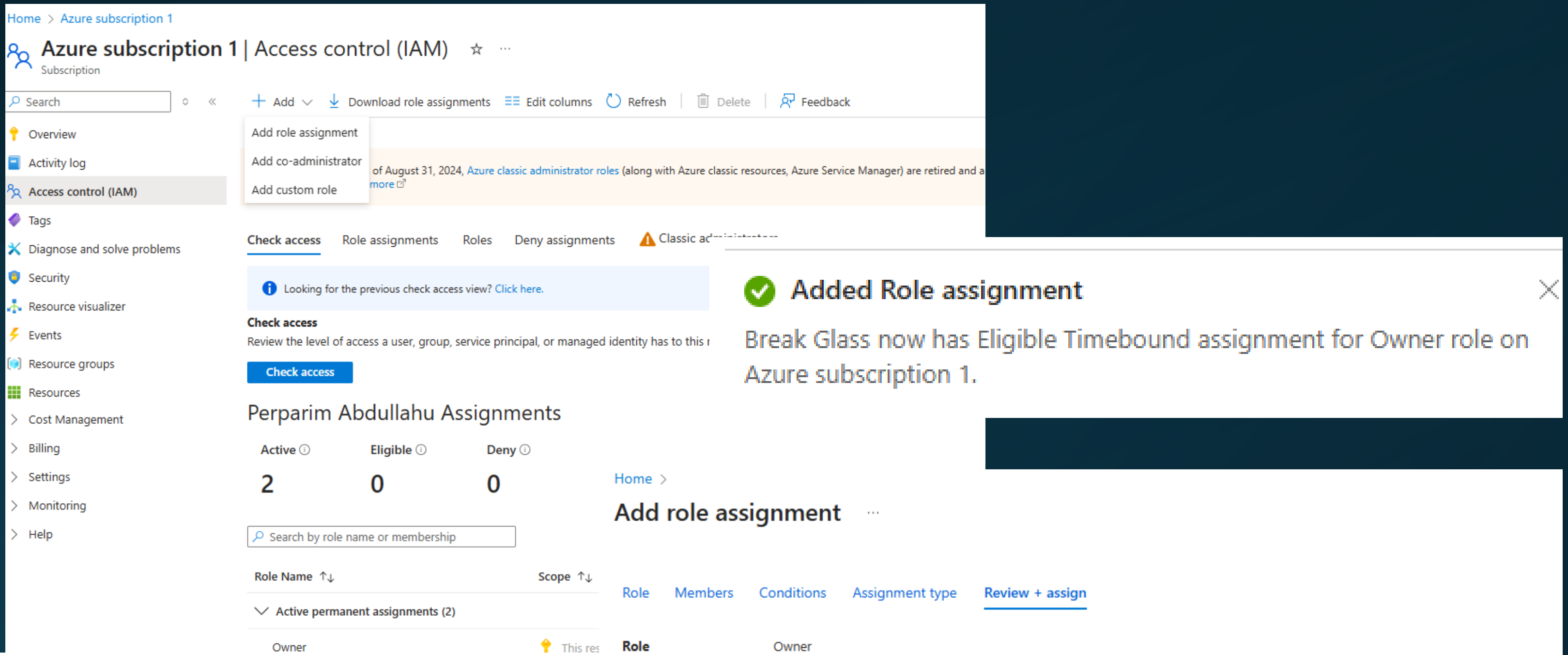
Trigger logic app

PerparimLabs

Privileged Access Governance with PIM

To reduce standing administrative privileges, Owner access is assigned using **Privileged Identity Management (PIM)** with **time-bound eligibility**.

A **Break Glass account** is maintained for emergency access scenarios, aligning with Zero Trust and least-privilege principles.



Home > Azure subscription 1

Azure subscription 1 | Access control (IAM)

Subscription

of August 31, 2024, Azure classic administrator roles (along with Azure classic resources, Azure Service Manager) are retired and a more

Looking for the previous check access view? Click here.

Check access

Review the level of access a user, group, service principal, or managed identity has to this r

Check access

Perparim Abdullahu Assignments

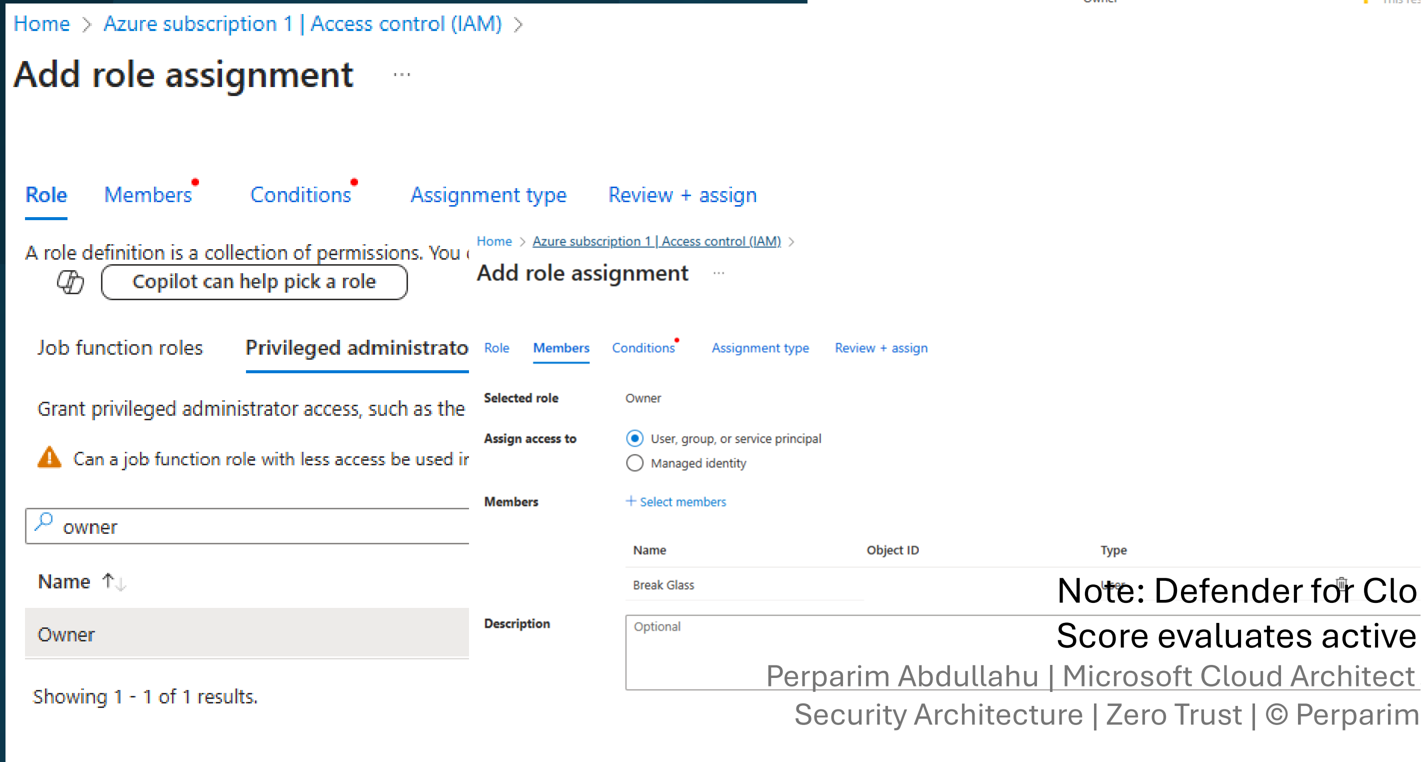
Active	Eligible	Deny
2	0	0

Search by role name or membership

Role Name ↑↓	Scope ↑↓
Active permanent assignments (2)	
Owner	This res

Added Role assignment

Break Glass now has Eligible Timebound assignment for Owner role on Azure subscription 1.



Home > Azure subscription 1 | Access control (IAM) >

Add role assignment

A role definition is a collection of permissions. You c

Copilot can help pick a role

Grant privileged administrator access, such as the

Can a job function role with less access be used ir

owner

Name ↑↓
Owner

Showing 1 - 1 of 1 results.

Home > Azure subscription 1 | Access control (IAM) >

Add role assignment

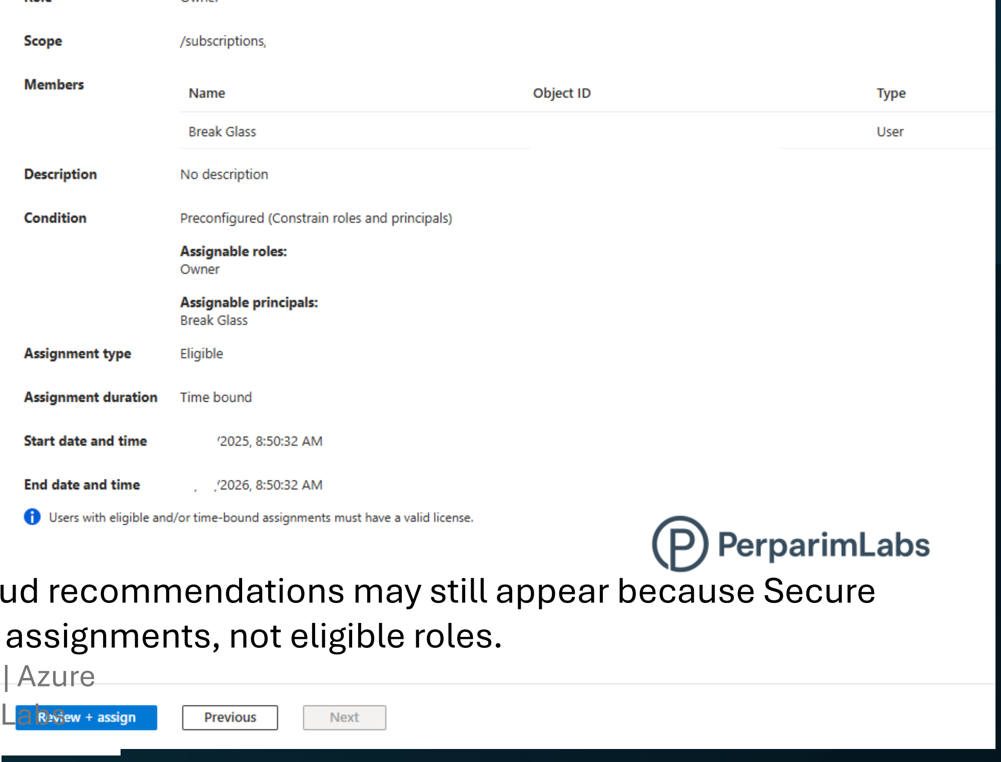
Selected role Owner

Assign access to ● User, group, or service principal ○ Managed identity

Members + Select members

Name	Object ID	Type
Break Glass		

Description Optional



Home >

Add role assignment

Role Owner

Scope /subscriptions,

Members

Name	Object ID	Type
Break Glass		User

Description No description

Condition Preconfigured (Constrain roles and principals)

Assignable roles:
Owner

Assignable principals:
Break Glass

Assignment type Eligible

Assignment duration Time bound

Start date and time '2025, 8:50:32 AM

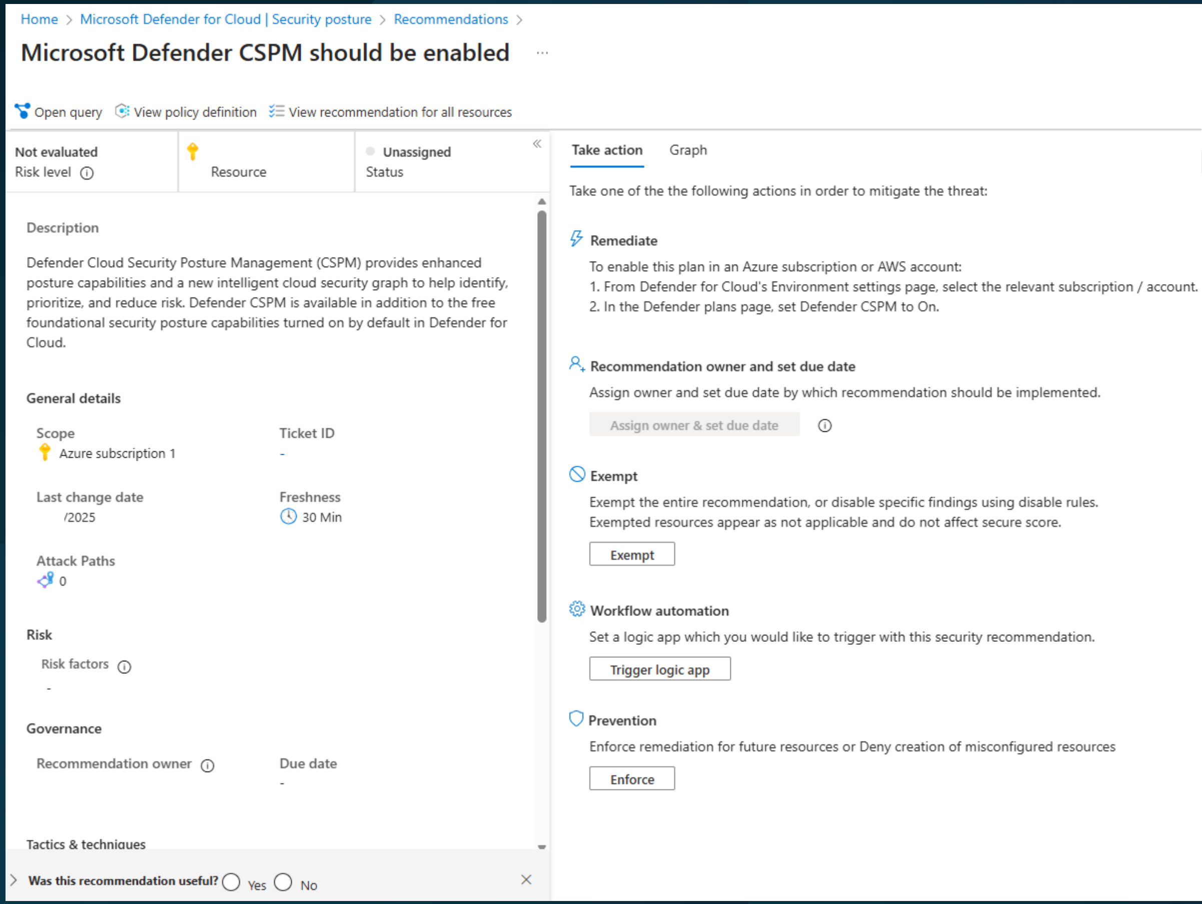
End date and time '2026, 8:50:32 AM

Users with eligible and/or time-bound assignments must have a valid license.

Note: Defender for Cloud recommendations may still appear because Secure Score evaluates active assignments, not eligible roles.

CSPM Recommendations Screen (Paid Features)

- Microsoft Defender CSPM should be enabled
- Defender Plans with pricing ($5/resource/month)



Home > Microsoft Defender for Cloud | Security posture > Recommendations >

Microsoft Defender CSPM should be enabled

Open query
View policy definition
View recommendation for all resources

Not evaluated Risk level	Resource	Unassigned Status

Description

Defender Cloud Security Posture Management (CSPM) provides enhanced posture capabilities and a new intelligent cloud security graph to help identify, prioritize, and reduce risk. Defender CSPM is available in addition to the free foundational security posture capabilities turned on by default in Defender for Cloud.

General details

Scope: Azure subscription 1

Ticket ID: -

Last change date: /2025

Freshness: 30 Min

Attack Paths: 0

Risk

Risk factors: -

Governance

Recommendation owner

Due date: -

Tactics & techniques

Was this recommendation useful? ○ Yes ○ No

Take one of the the following actions in order to mitigate the threat:

Remediate

To enable this plan in an Azure subscription or AWS account:

1. From Defender for Cloud's Environment settings page, select the relevant subscription / account.
2. In the Defender plans page, set Defender CSPM to On.

Recommendation owner and set due date

Assign owner and set due date by which recommendation should be implemented.

Exempt

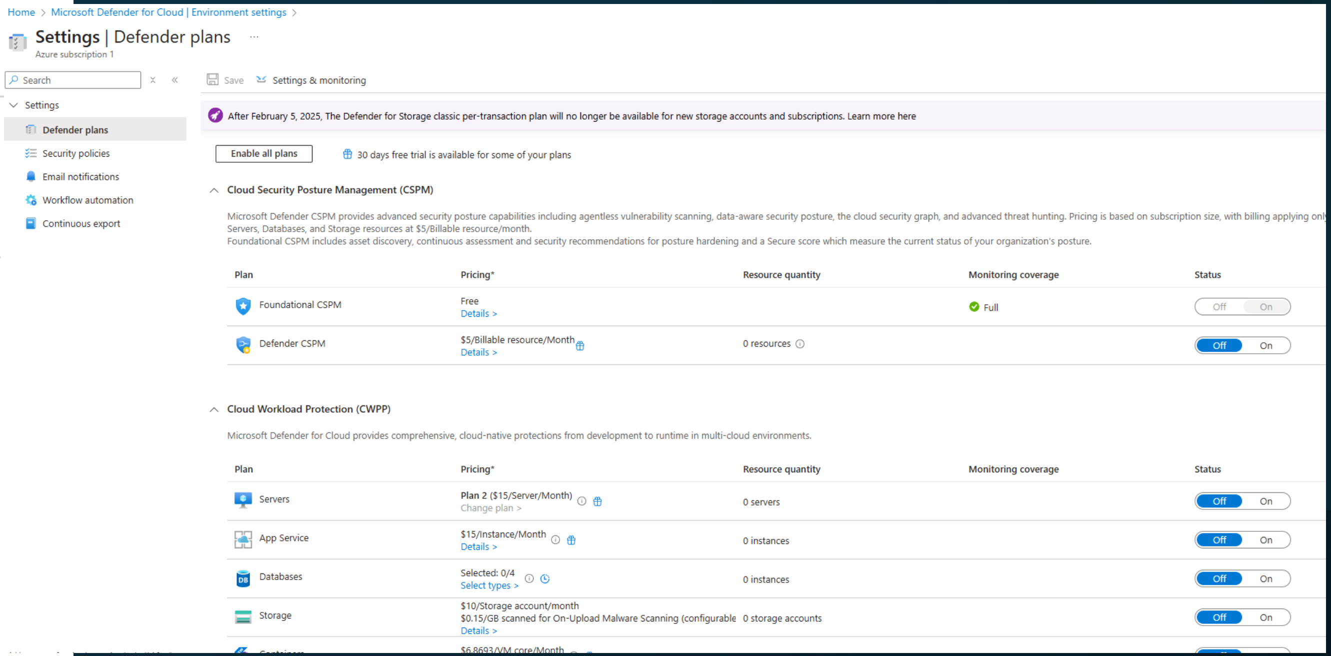
Exempt the entire recommendation, or disable specific findings using disable rules. Exempted resources appear as not applicable and do not affect secure score.

Workflow automation

Set a logic app which you would like to trigger with this security recommendation.

Prevention

Enforce remediation for future resources or Deny creation of misconfigured resources



Settings | Defender plans

Azure subscription 1

After February 5, 2025, The Defender for Storage classic per-transaction plan will no longer be available for new storage accounts and subscriptions. Learn more here

30 days free trial is available for some of your plans

Cloud Security Posture Management (CSPM)

Microsoft Defender CSPM provides advanced security posture capabilities including agentless vulnerability scanning, data-aware security posture, the cloud security graph, and advanced threat hunting. Pricing is based on subscription size, with billing applying onl
Servers, Databases, and Storage resources at $5/Billable resource/month.
Foundational CSPM includes asset discovery, continuous assessment and security recommendations for posture hardening and a Secure score which measure the current status of your organization's posture.

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Foundational CSPM	Free Details >		✓ Full	Off On
Defender CSPM	$5/Billable resource/Month Details >	0 resources		Off On

Cloud Workload Protection (CWPP)

Microsoft Defender for Cloud provides comprehensive, cloud-native protections from development to runtime in multi-cloud environments.

Plan	Pricing*	Resource quantity	Monitoring coverage	Status
Servers	Plan 2 ($15/Server/Month) Change plan >	0 servers		Off On
App Service	$15/Instance/Month Details >	0 instances		Off On
Databases	Selected: 0/4 Select types >	0 instances		Off On
Storage	$10/Storage account/month $0.15/GB scanned for On-Upload Malware Scanning (configurable Details >	0 storage accounts		Off On
Containers	$6.8693/VM core/Month			

Note: Defender CSPM and other workload protection plans are paid offerings. In this demo I am showing where they appear in the UI but I did NOT activate any paid plans.

Key Takeaways – Microsoft Defender for Cloud

- Microsoft Defender for Cloud provides a centralized view of security posture across subscriptions and workloads
- Secure Score highlights actionable recommendations to reduce risk and improve baseline security
- Regulatory compliance and Microsoft Cloud Security Benchmark help measure alignment with security standards
- Foundational posture management is available at no cost, while advanced CSPM and workload protections are optional paid capabilities
- Architects must balance security improvements with cost, scope, and business requirements