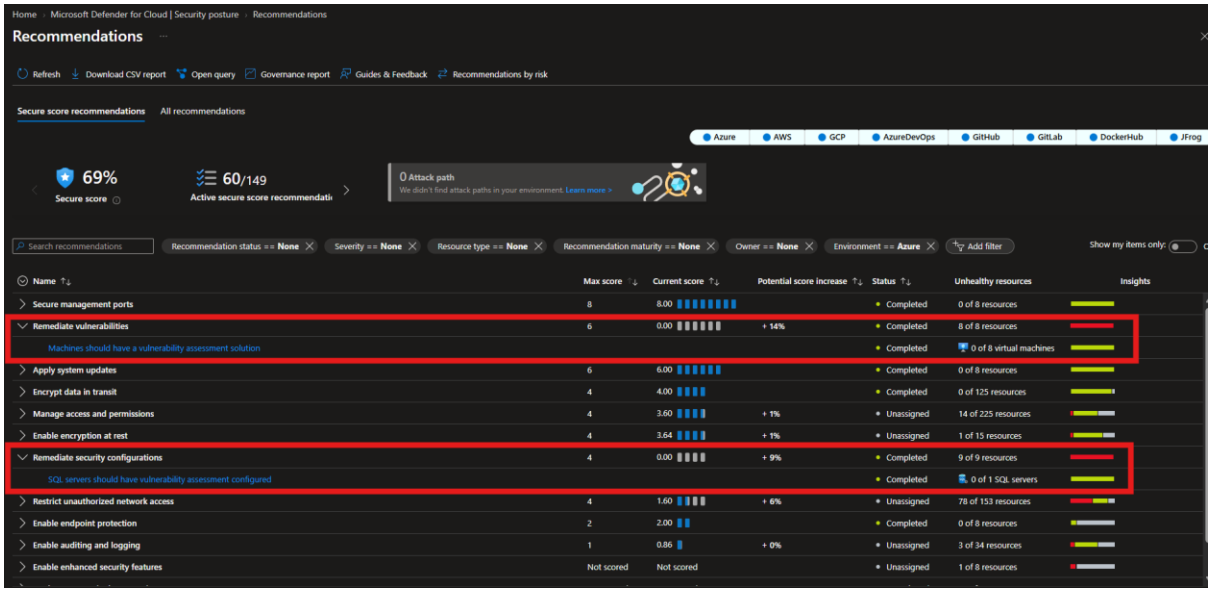
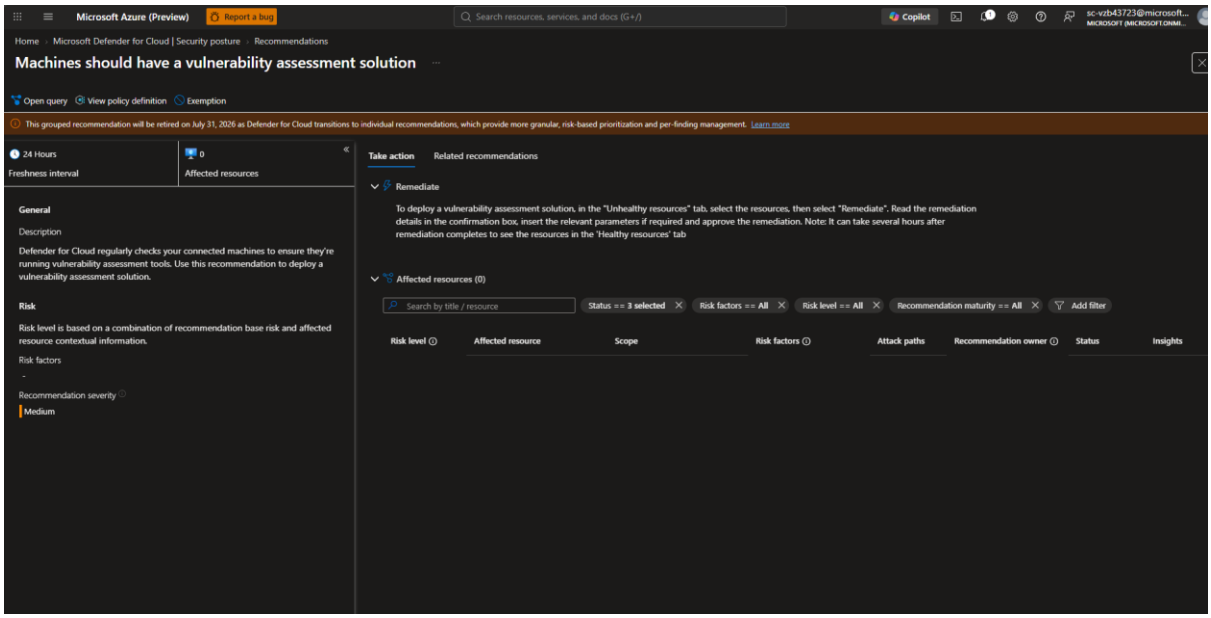
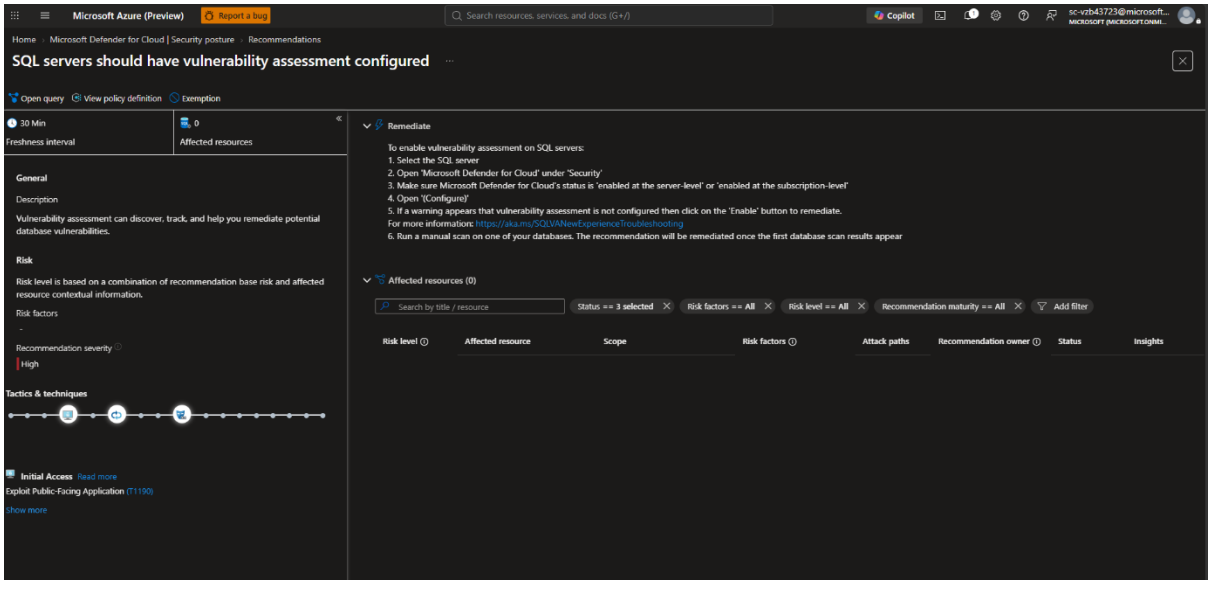

Home › Microsoft Defender for Cloud | Security posture › Recommendations
Recommendations
Refresh
Download CSV report
Open query
Governance report
Guides & Feedback
Recommendations by risk
Secure score recommendations
All recommendations
Azure
AWS
GCP
AzureDevOps
GitHub
GitLab
DockerHub
JFrog
69%
Secure score
60/149
Active secure score recommendati
0 Attack path
We didn't find attack paths in your environment. Learn more >
Search recommendations
Recommendation status == None
Severity == None
Resource type == None
Recommendation maturity == None
Owner == None
Environment == Azure
Add filter
Show my items only:
Name
Max score
Current score
Potential score increase
Status
Unhealthy resources
Insights
Secure management ports 8 8.00 Completed 0 of 8 resources
Remediate vulnerabilities 6 0.00 + 14% Completed 8 of 8 resources
Machines should have a vulnerability assessment solution Completed 0 of 8 virtual machines
Apply system updates 6 6.00 Completed 0 of 8 resources
Encrypt data in transit 4 4.00 Completed 0 of 125 resources
Manage access and permissions 4 3.60 + 1% Unassigned 14 of 225 resources
Enable encryption at rest 4 3.64 + 1% Unassigned 1 of 15 resources
Remediate security configurations 4 0.00 + 9% Completed 9 of 9 resources
SQL servers should have vulnerability assessment configured Completed 0 of 1 SQL servers
Restrict unauthorized network access 4 1.60 + 6% Unassigned 78 of 153 resources
Enable endpoint protection 2 2.00 Completed 0 of 8 resources
Enable auditing and logging 1 0.86 + 0% Unassigned 3 of 34 resources
Enable enhanced security features Not scored Not scored Unassigned 1 of 8 resources


Microsoft Azure (Preview)
Report a bug
Search resources, services, and docs (G+/)
Copilot
Home › Microsoft Defender for Cloud | Security posture › Recommendations
Machines should have a vulnerability assessment solution
Open query
View policy definition
Exemption
This grouped recommendation will be retired on July 31, 2026 as Defender for Cloud transitions to individual recommendations, which provide more granular, risk-based prioritization and per-finding management. Learn more
24 Hours
Freshness interval
0
Affected resources
General
Description
Defender for Cloud regularly checks your connected machines to ensure they're running vulnerability assessment tools. Use this recommendation to deploy a vulnerability assessment solution.
Risk
Risk level is based on a combination of recommendation base risk and affected resource contextual information.
Risk factors
-
Recommendation severity
Medium
Take action
Related recommendations
Remediate
To deploy a vulnerability assessment solution, in the "Unhealthy resources" tab, select the resources, then select "Remediate". Read the remediation details in the confirmation box, insert the relevant parameters if required and approve the remediation. Note: It can take several hours after remediation completes to see the resources in the 'Healthy resources' tab
Affected resources (0)
Search by title / resource
Status == 3 selected
Risk factors == All
Risk level == All
Recommendation maturity == All
Add filter
Risk level
Affected resource
Scope
Risk factors
Attack paths
Recommendation owner
Status
Insights


Microsoft Azure (Preview)
Report a bug
Search resources, services, and docs (G+/)
Copilot
Home › Microsoft Defender for Cloud | Security posture › Recommendations
SQL servers should have vulnerability assessment configured
Open query
View policy definition
Exemption
30 Min
Freshness interval
0
Affected resources
General
Description
Vulnerability assessment can discover, track, and help you remediate potential database vulnerabilities.
Risk
Risk level is based on a combination of recommendation base risk and affected resource contextual information.
Risk factors
-
Recommendation severity
High
Tactics & techniques
Initial Access Read more
Exploit Public-Facing Application (T1190)
Show more
Remediate
To enable vulnerability assessment on SQL servers:
1. Select the SQL server
2. Open 'Microsoft Defender for Cloud' under 'Security'
3. Make sure Microsoft Defender for Cloud's status is 'enabled at the server-level' or 'enabled at the subscription-level'
4. Open '(Configure)'
5. If a warning appears that vulnerability assessment is not configured then click on the 'Enable' button to remediate.
For more information: https://aka.ms/SQLVANewExperienceTroubleshooting
6. Run a manual scan on one of your databases. The recommendation will be remediated once the first database scan results appear
Affected resources (0)
Search by title / resource
Status == 3 selected
Risk factors == All
Risk level == All
Recommendation maturity == All
Add filter
Risk level
Affected resource
Scope
Risk factors
Attack paths
Recommendation owner
Status
Insights