

# Env settings

Microsoft Azure

Search resources, services, and docs (G+)

Copilot

accounts@perimatics.c  
WINIGENT (WINIGENT.CO

Home > Microsoft Defender for Cloud | Environment settings > Settings | Defender plans >

## Settings & monitoring

Perimatics Azure Primary Subscription

Continue

When you enable an extension, it will be installed on any new or existing resource, by assigning a security policy.

Defenders plans : **Servers**

Component	Description	Defender plans	Configuration	Status
<b>Log Analytics agent</b> Agent is in deprecation path. <a href="#">Learn more &gt;</a>	Collects security-related configurations and event logs from the machine and stores the data in your Log Analytics workspace for analysis. <a href="#">Learn more</a>		-	<input type="checkbox"/> Off <input type="checkbox"/> On
<b>Vulnerability assessment for machines</b>	Enables vulnerability assessment on your Azure and hybrid machines. <a href="#">Learn more</a>		Selected VA tool: Microsoft Defender vulnerability management <a href="#">Edit configuration</a>	<input type="checkbox"/> Off <input checked="" type="checkbox"/> On
<b>Guest Configuration agent (preview)</b>	Checks machines for security misconfigurations in the OS, applications, and environment settings. This deploys the agent to Azure virtual machines. Hybrid machines connected to Azure Arc already have this agent included in the <a href="#">Azure Connected Machine agent</a> . Learn more about the Guest Configuration agent, in <a href="#">Understand Azure Policy's Guest Configuration</a> .		-	<input checked="" type="checkbox"/> Off <input type="checkbox"/> On
<b>Endpoint protection</b>	Enables protection powered by Microsoft Defender for Endpoint, including automatic agent deployment to your servers, and security data integration with Defender for Cloud. <a href="#">Learn more</a>		-	<input type="checkbox"/> Off <input checked="" type="checkbox"/> On
<b>Agentless scanning for machines</b>	Scans your machines for installed software, vulnerabilities, and secret scanning without relying on agents or impacting machine performance. <a href="#">Learn more</a>		<a href="#">Edit configuration</a>	<input type="checkbox"/> Off <input checked="" type="checkbox"/> On
<b>File Integrity Monitoring</b>	File integrity monitoring (FIM), also known as change monitoring, examines operating system files, Windows registries, application software, Linux system files, and more, for changes that might indicate an attack.		-	<input type="checkbox"/> Off <input type="checkbox"/> On

# Remediate/fix button

[Home](#) > [Resource health](#) >

## Machines should have a vulnerability assessment solution

[Open query](#) [View policy definition](#) [View recommendation for all resources](#)

Not evaluated Risk level ⓘ	maahesh-vm Resource	Unassigned Status								
<div><b>Description</b><p>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.</p></div> <div><b>General details</b><table><tbody><tr><td>Scope  Perimatics Azure Primary Subsc...</td><td>Ticket ID -</td></tr><tr><td>Last change date 6/10/2025</td><td>Freshness  24 Hours</td></tr><tr><td colspan="2">Attack Paths  0</td></tr></tbody></table></div> <div><b>Risk</b><p>Risk factors ⓘ -</p></div> <div><b>Governance</b><table><tbody><tr><td>Recommendation owner ⓘ  Suggested: nishant@perimatics.com</td><td>Due date -</td></tr></tbody></table></div>			Scope Perimatics Azure Primary Subsc...	Ticket ID -	Last change date 6/10/2025	Freshness 24 Hours	Attack Paths 0		Recommendation owner ⓘ Suggested: nishant@perimatics.com	Due date -
Scope Perimatics Azure Primary Subsc...	Ticket ID -									
Last change date 6/10/2025	Freshness 24 Hours									
Attack Paths 0										
Recommendation owner ⓘ Suggested: nishant@perimatics.com	Due date -									

**Take action** **Graph**

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

**Remediate**

Quick fix:  
Select the unhealthy resources and click "Fix" to launch "Quick fix" remediation. [Learn more >](#)  
Note: After the process completes, it may take up to 24 hours until your resources move to the 'healthy resources' tab.

Fix

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

**Recommendation owner and set due date**

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

**Top suggested active user on the affected resource:**  
nishant@perimatics.com  
Nishant R V (Perimatics)

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