

Microsoft Defender Vulnerability Management Guide

Defender Vulnerability Management delivers asset visibility, intelligent assessments, and built-in remediation tools for Windows, macOS, Linux, Android, iOS, and network devices. Using Microsoft threat intelligence, breach likelihood predictions, business contexts, and devices assessments, Defender Vulnerability Management rapidly and continuously prioritizes the biggest vulnerabilities on your most critical assets and provides security recommendations to mitigate risk.

Deployment Type

This integration supports **vendor cloud** deployments through **port 443**.

If you already know that your environment supports these deployments, continue to the next step. If you are, please check your organization's compatibility before continuing.

Required Information and Setup

To integrate GreyMatter with Microsoft Defender Vulnerability Management, collect the following details:

- Security Center URL
 - Default: <https://api.securitycenter.microsoft.com>
- Token URL
 - Default: <https://login.microsoftonline.com>
- Client ID
- Client Secret Key
- Tenant ID

Note: Core capabilities for Microsoft Defender Vulnerability Management are included in the [Defender for Endpoint P2 licenses](#). Access the full product through:

- An add-on to Defender for Endpoint P2 or Microsoft 365 E5
- The Defender for Servers P2 license (included)
- Purchasing as a standalone

See instructions below to gather the required information.

Register an application

In the Microsoft Azure console, register an application via the instructions in the [Microsoft documentation](#).

Assign application API permissions

Assign the Application API permissions in the table below.
[Learn how to get access without a user.](#)

Microsoft Defender Vulnerability Management Guide

Note: Permissions must be approved by a resource owner (Admin) after they're added to take effect. [See Microsoft permissions overview.](#)

Generate Client Secret

[Generate a client secret](#) for the integration credentials.

Permissions and Functionality

Permissions

GreyMatter Capability	Action(s)	Required Permission
Asset Inventory	Fetch Assets	Vulnerability.Read.All Machine.Read.All
Respond	Enrich Vulnerability	Vulnerability.Read.All

Respond

Playbook Name	Description	Required Input Variables
Enrich Vulnerability	Returns vulnerability information such as description, severity, and affected machines. In the Microsoft Defender platform, navigate to “Endpoints” > “Vulnerability Management” > “Weaknesses” to view vulnerability information.	CVE ID Example: CVE-2025-8901

Asset Inventory

Asset Inventory provides a comprehensive overview of your digital environment by integrating directly with Microsoft Defender Vulnerability Management, providing real-time insights into what assets you own, their status, and potential risks. Specifically, it pulls a list of machines and any vulnerabilities from Microsoft Defender.

Disclaimer: All customer data is classified and handled as ‘Confidential’ (as outlined in our Data Classification & Handling Policy). Customer data is restricted to authorized personnel only based on their business need. ReliaQuest uses least privilege and role-based access controls via Active Directory to provision and manage access. Please see our Access Control Policy for more information. ReliaQuest employees are also required to sign confidentiality agreements as part of their employment.