Ontinue

ONTINUE MVM
SERVICE DESCRIPTION

Table of Contents

1. ABOUT THIS DOCUMENT

This service description of Ontinue Managed Vulnerability Mitigation (MVM) provides an overview of how the service enables customers to focus on the highest risk vulnerabilities in their environment. **Managed Vulnerability Mitigation (MVM) is available exclusively as an add-on to customers of the ION Managed Extended Detection and Response (MXDR) service**. Subject to ordering and payment of applicable fees, this Ontinue MVM service description is incorporated into the Master Services Agreement available at www.ontinue.com/msa, or if applicable the agreement executed by and between Ontinue and Customer for ION Services ("MSA"). Notwithstanding anything to the contrary, the Customer acknowledges and agrees that Ontinue may modify or update the MVM Service over time, provided that any such modifications or updates do not materially degrade the security or function of the MVM Service.

This document covers the following:

Section	Description
Managed Vulnerability Mitigation Service	A high-level explanation of the MVM service.
Managed Vulnerability Mitigation Technology	The technology deployments and licenses that are either prerequisites or recommendations for using the service.
Managed Vulnerability Mitigation Service Launch	The details of how the service is operationalized for customers, designed to deliver value from the start.
Managed Vulnerability Mitigation Service Operations	How MVM operates, including the responsibilities on both the Ontinue and customer side.

2. MANAGED VULNERABILITY MITIGATION SERVICE

Managed Vulnerability Mitigation (MVM) is an add-on service to the ION MXDR service and is centered on vulnerability telemetry from Microsoft Defender for Endpoint. The MVM service offers customers vulnerability prioritization, based on their organization approach to risk helping customers better mitigate the risk of vulnerabilities in their IT environment.

Risk assessment is subject to customer input and is specifically connected to Customer providing and maintaining an accurate inventory of critical IT assets.

3. MANAGED VULNERABILITY MITIGATION TECHNOLOGY

Technology License Requirements for MVM

Technology	License and pricing	Comments
Microsoft Defender for Endpoint	Defender for Endpoint Plan 2 license	Many Microsoft licensing SKUs include the Microsoft Defender for Endpoint License: Microsoft Defender for Server Plans 1 and 2 includes Microsoft Defender for Endpoint Plan 2. The full list of possibilities is detailed here.

Technology Deployment Requirements for MVM

Technology requirements for MVM are aligned with the requirements for the core ION MXDR service.

4. MANAGED VULNERABILITY MITIGATION SERVICE LAUNCH

MVM customers benefit from a fast and easy launch as the service is built to leverage existing components of the ION MXDR service. Specifically, **MVM uses vulnerability telemetry from Microsoft Defender for Endpoint**, a requirement of the ION MXDR service.

Key Party	Contact / Entity	Launch Responsibilities
Ontinue ION	Cyber Advisors	Review the technical implementation of the service, including appropriate configurations.
	Customer Success Managers	Serve as the contact for all non-technical requests.
	Vulnerability Analysts	Set up automated reporting.
Customer	CISO or Head of Security or equivalent	Serve as the security strategy and IR policy owner. Provide operational approvals. Serve as a key point of escalation.
	IT Security Operations	Provide technical approvals (depending on organization). Ensure accuracy of critical asset inventory.
	IT Team or designated MSP/CSP	Provide technical approvals (depending on organization).

5. MANAGED VULNERABILITY MITIGATION SERVICE OPERATIONS

Key Party	Contact / Entity	Ongoing Operational Responsibilities
Ontinue ION	Cyber Advisors	Serve as the point of contact on vulnerability questions and remediation guidance. Serve as the customer interface for the service in general. Ensure ongoing, correct technical implementation of all Ontinue services.
	Customer Success Managers	Serve as the contact for all non-technical requests. Ensure that customer needs are heard, and feedback is integrated into MVM where appropriate and relevant. Proactively deliver updates on MVM's continuous development and ensure expectations alignment.
	Vulnerability Analysts	Serve as the subject matter expert on vulnerability mitigation. Ensure ongoing accuracy of automated reports.
Customer	CISO or Head of Security or equivalent	Serves as the security strategy and IR policy owner. Provides approvals, serves as a key point of escalation.
	IT Security Operations	Notify Ontinue of any IT environment changes that may affect the execution of the MVM service. Ensure accuracy of critical asset inventory. Execute mitigation measures (depending on organization).
	IT Team or designated MSP/CSP	Execute mitigation measures (depending on organization). Perform end-user follow up and verification if required

Scope of MVM Service Operations

Within MVM Service Scope
Vulnerability management for endpoints with Defender for Endpoint (Plan 2 license required)
Support for Windows, Linux, and Mac operating systems Defender Vulnerability Management – core capabilities (part of Defender for Endpoint Plan 2) Device discovery Device inventory Vulnerability assessment Configuration assessment Risk-based prioritization Remediation tracking Continuous monitoring Software assessment Software usage insights

Outside of MVM Service Scope
Microsoft Defender Vulnerability Management – premium capabilities Microsoft Defender External Attack Surface Management Microsoft Defender for Cloud CSPM
Network devices and other IT devices that do not support the Defender for Endpoint agent
Mobile operating systems
IoT/OT environments
Web application scanning

MVM Notifications and Reporting

High Risk Notification

High Risk Notifications are **near real-time, automated notifications** delivered by the MVM service **when a newly disclosed Common Vulnerabilities and Exposures (CVE) event represents a high risk to the customer environment**. A newly disclosed CVE might not be present in a customer environment, and thus irrelevant. On the other hand, when a newly disclosed CVE is present (or widespread) in a customer environment, especially on critical assets, it is key to act quickly. Therefore, the notification is triggered if, and only if, a new CVE is both present and risky to the customer.

High Risk Notification - Overview	
Delivery Frequency	As often as needed, but not more than once in 24 hours.
Trigger	An Ontinue Risk Score (explained below) greater than 5.
Delivery channel	Email only

A High Risk Notification contains the following information:

High Risk Notification - Information	
CVE Identifier	An alphanumeric string that identifies a publicly disclosed vulnerability.
CVE Description	A high-level description of the vulnerability.
CVE Impact Summary	An explanation of the impact that a successful exploit of the vulnerability would have on a customer.
CVE Age	The number of days between when the CVE is reported on any devices within the customer environment and when the CVE was first published.
Number of Affected Devices	The count of critical and total devices in the environment affected by the CVE, with a link to Defender pointing to those devices.
Ontinue Risk Score	A proprietary risk score, on a scale of 1 to 10 (1 being lowest risk, 10 being highest risk), calculated by taking into consideration Ontinue's Exploitation Impact Score and Exploitation Likelihood Score. This includes, but is not limited to, the use of the Exploit Prediction Scoring System (EPSS) from FIRST.

Weekly Security Posture Report

Weekly Security Posture Reports offer customers an overview of how their security posture has changed over the past 7 days. This includes a summary, various exposure metrics, key vulnerabilities to address, and a list of the week's High Risk Notifications.

Weekly Security Posture Report – Overview	
Delivery frequency	Weekly
Delivery channel	Email only

A Weekly Security Posture Report contains the following information:

Weekly Security Posture Report – Information	
Summary	Summarizes what happened over the week.
Last Week's High Risk Notifications	A full list of high risk notifications from the week, in a summary table that includes the main information of each notification.
Security Recommendations	A list of recommendations to improve the Microsoft Exposure Score.
Top 5 Most Critical Vulnerabilities	A report on the most critical vulnerabilities based on Ontinue's Exploitation Likelihood Score, Exploitation Impact Score and Risk Score.
Top 5 Devices with Most Critical Vulnerabilities	A report on the most vulnerable assets monitored by Defender for Endpoint.
Incidents Related to Top 5 Devices	Incidents from the current week related to the most vulnerable devices.

MVM Monthly Action Report

MVM Monthly Action Reports are designed to enable customers to tackle areas of high risk in their IT environment by highlighting the top 5 vulnerabilities identified based on a range of criteria. Additional views of risk are included in the report, such as the top CVEs by number of instances and assets with the highest count of vulnerabilities. The Cyber Advisor reviews the MVM Action Report jointly with the customer.

Monthly MVM Action Report – Overview	
Delivery frequency	Monthly
Delivery channel	Microsoft Teams and/or email

The MVM Action Report contains the following information:

Monthly MVM Action Report – Information	
Executive Reporting	Delivers a high-level overview of the organization's risk posture. Includes Ontinue's proprietary risk scoring as well as Microsoft Secure Scores.
Operational Reporting	Delivers tailored recommendations on which CVEs to mitigate, including guidance on how to mitigate. The recommendations are grouped into top 5 categories, segmented by asset criticality. The Operational Reporting section also includes a recap of all the High Risk Notifications that were delivered during the reporting period.

MVM Monthly Detailed Vulnerabilities Spreadsheet

The MVM Monthly Detailed Vulnerabilities Spreadsheet provides a comprehensive listing of all vulnerabilities identified in the IT environment, with operational details such as Device IDs. For easy filtering and sorting, this report is delivered as a spreadsheet.

Monthly MVM Detailed Vulnerabilities Report – Overview	
Frequency	Monthly
Delivery channel	Microsoft Teams and/or email

6. MANAGED VULNERABILITY MITIGATION LICENSING MODEL

Managed Vulnerability Mitigation (MVM) is licensed per unit. A unit is calculated as follows:

- 1 unit = 1 Authorized User (up to 5 devices per individual user licensed for Microsoft Defender for Endpoint).
- 1 unit = 1 server protected by Defender for Cloud / Servers.