Ontinue

ONTINUE MVM
SERVICE DESCRIPTION

Introduction

A key characteristic of mature, effective cybersecurity programs is continuous activity in both defending the attack surface and proactively reducing the attack surface. Ontinue ION enables organizations to defend and reduce their attack surface through a set of continuous practices. To supplement the core practices, the Managed Vulnerability Mitigation (MVM) service focuses on attack surface reduction by identifying known vulnerabilities in your environment and then working with your team to deploy mitigations to avoid exploitation of these vulnerabilities by threat actors. Reducing the number of vulnerabilities, particularly those present in critical assets, enables organizations to avoid attacks that otherwise would have a significant negative impact. It's worth noting that patching is not the only form of mitigation; often compensating controls can be developed for vulnerabilities that cannot be patched or otherwise eliminated.

While the value and benefits of implementing a well-run vulnerability management program are well understood, organizations often face substantial challenges in designing and executing such programs. The MVM service provides you the support and information that to address these challenges, plugging your organization into a set of industry best practices for vulnerability management designed to reduce your overall cyber risk.

Managed Vulnerability Mitigation Service Deliverables

Superior prioritization of vulnerabilities

Obtain prioritization of vulnerabilities that leverages knowledge of your environment combined with the latest threat intelligence. The specific elements that drive prioritization are:

- Known exploits of vulnerabilities: using information from the Cybersecurity and Infrastructure Security Agency (CISA)
- Likelihood of exploit creation: using the latest information found in Metasploit - even if the vulnerability yet to be exploited, its presence in Metasploit serves as an indicator of the likelihood of the vulnerability being exploited soon.
- Knowledge of asset criticality and your environment: we obtain this information from you during onboarding and work with you to ensure it's up to date.

Remediation advisory

The MVM service develops a deep understanding of your environment, and as part of the service can assist your IT staff with the "how" on vulnerability mitigation. Such advisory support can include answering technical questions by chat and email, guidance on patching, guidance on compensating controls, analysis of false positives, and other ad-hoc advisory support related to the mitigation of vulnerabilities.

Proactive notification of new high-risk vulnerabilities

MVM continually monitors for disclosures of critical and high severity vulnerabilities and notifies you if the newly disclosed vulnerabilities pose a high risk to your environment.

Managed Vulnerability Mitigation Reporting

As part of the MVM service, customers will be provided the following information:

<table>
<tr><th colspan="2">Executive Summary</th><th colspan="2">Operational Reporting</th></tr>
<tr><td rowspan="5">Vulnerable devices</td><td>Device vulnerability severity levels</td><td rowspan="7">Top vulnerabilities prioritized by return on mitigation effort</td><td>Top 5 vulnerabilities on critical assets known to be actively exploited, exploits available</td></tr>
<tr><td>Device exploit availability</td><td>Top 5 vulnerabilities on non-critical assets known to be actively exploited, exploits available</td></tr>
<tr><td>Device vulnerability age over time</td><td>Top 5 vulnerabilities that are confirmed to be exploited by CISA, exploits not freely available, found in critical assets</td></tr>
<tr><td>Vulnerable devices by operating system platform</td><td>Top 5 vulnerabilities that are confirmed to be exploited by CISA, exploits not freely available, found in non-critical assets</td></tr>
<tr><td>Vulnerable devices by Windows 10 & 11 version with build lifecycle dates</td><td>Top 5 Recommendations to maximally reduce attack surface</td></tr>
<tr><td colspan="2">Aging statistics (30, 60, 90+ days)</td><td>Top 5 vulnerabilities by total attack surface – assets with highest total count of vulnerabilities</td></tr>
</table>

Quarterly Advisory Session

As part of the Quarterly Advisory Session, MVM customers will have a section dedicated to vulnerability mitigation. This will cover the prioritized list of vulnerabilities that require mitigation and serve as an opportunity to evaluate mitigation performance and areas for improvement.

Tight integration with the core MXDR service

The MVM service is architected and delivered as a natively integrated component of the Ontinue ION service. Examples of the tight integration include:

- MVM data is used for additional context in the core MXDR service whenever appropriate. This includes threat hunts (prevent practice), as well as during investigations and to improve the accuracy, efficacy, and speed of containment actions (detect and respond practices). This ensures vulnerabilities are identified, prioritized, and mitigated as part of your overall security program, rather than in a silo.
- MVM reporting is done via monthly reports and reviewed as part of the same quarterly Advisory Session meeting as the Ontinue ION service. This ensures recommendations are made within the context of the overall recommendations to improve your security posture.
- MVM service delivery is provided by the same designated Cyber Advisor as the MXDR service. This drives the continual localization of the MVM service, tailored to your IT environment and business objectives.

Continuous asset discovery

Microsoft Defender for Endpoint is continually scanning your environment and highlighting any new devices discovered.

Recommendation Log

The MVM service maintains a list of exceptions for vulnerabilities that cannot be mitigated and have been accepted by your organizations as known risks.

Flexible cloud and on-premises deployment

The MVM service is built on Microsoft Defender for Endpoint which can be deployed on Windows, Mac and Linux hosts and servers.

Managed Vulnerability Mitigation Service Scope

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
Defender Vulnerability Management add-on – Additional capabilities for Defender for Endpoint Plan 2 Defender Vulnerability Management Standalone – Full vulnerability management capabilities Defender External Attack Surface Management
Network devices and other IT devices that don't support the Defender for Endpoint agent
Mobile operating systems
IoT/OT environments
Web application scanning

Managed Vulnerability Mitigation Service Technology

The Managed Vulnerability Mitigation Service requires deployment of Defender for Endpoint Plan 2. This service does not include the required Microsoft licenses.

Managed Vulnerability Mitigation Service Operations

The key parties involved in MVM service operations are:

- **Ontinue**: Designated Cyber Advisors, Vulnerability Analysts
- **Customer**: CISO (or equivalent role), IT Security Operations (or equivalent role), IT Team

The engagement and collaboration required of these key parties is crucial to ensuring a successful vulnerability mitigation program where vulnerabilities are identified, qualified, and mitigated on a continual basis to reduce your organizations overall risk.

The MVM service starts with a project kick-off meeting, led by the Cyber Advisor. At the project kick-off meeting, the Cyber Advisor will walk you through the full and ongoing service delivery process and schedule a time for the quarterly review meetings (if not already defined). During this kickoff meeting we will require and review:

- A complete list of all assets that are to be covered by the MVM service.
- Identification of critical assets for the proper prioritization of mitigations
- Establish rules of engagement and identify who at Ontinue works directly with the customer
- Determine customer contacts responsible for mitigation tasks
- Determine who is responsible for the customer's security program and mitigation activity
- Designated customer point of escalation for resolution of asset ownership questions
- Determine escalation contacts for notification of critical vulnerabilities
- Review network topology, asset locations and preventive security controls that are deployed
- How to configure Microsoft Defender for Endpoint for proper operation with our service
- How to grant Ontinue access to the required Microsoft console to deliver the service
- Ontinue to provide briefing on best practices in relation to management tool for Linux or Mac systems (e.g., JAMF or other).
- Ontinue will provide a recommendation log template

Once Microsoft Defender for Endpoint is configured and Ontinue is granted access to the console, your service will start. Our team will be working continuously, as described in the table below

Frequency	Activity
Daily	Monitoring threat intelligence for new, high-risk vulnerabilities relevant to your environment, with notification and remediation advisory as needed
Weekly	Recording and reporting on your Microsoft Exposure score as an indicator of mitigation activities
Monthly	Delivering executive and operational reporting on vulnerabilities to be mitigated
Quarterly	During the Quarterly Advisory Session, there will be a section focused on MVM

Managed Vulnerability Mitigation (MVM) Service Operations Key Parties and Responsibilities

Key Party	Contact	Responsibilities
Ontinue	Cyber Advisor	Serves as your interface for the service in general Leverages data and findings from vulnerability analysts to provide security posture guidance in quarterly status meetings Serves as your point of escalation
	Vulnerability Analysts	Monitors threat intelligence for new, high-risk vulnerabilities relevant to your environment and notifies you as needed Provides remediation advisory and delivers follow up guidance for the vulnerabilities specified above Records and reports on your Microsoft Exposure score weekly
Customer	CISO	Serves as the security strategy and IR policy owner Provides approvals, management reporting, escalation Determines and communicates asset information and criticality to Ontinue for use in prioritizing mitigations
	IT Security Operations	Serves as the peer for the Ontinue Cyber Advisor Takes decisions and provides approval for MVM recommended vulnerability mitigations Communicates changes in the environment that impact the vulnerability mitigation service to the Cyber Advisor
	IT Team	Performs patching and other forms of mitigation on assets including configuration of any required compensating controls Performs end-user follow up and verification if required

Managed Vulnerability Mitigation (MVM) Service – Service Level Objective

SLO	Description	Time	Achievement
Customer notification time of new critical vulnerability	The MVM service will notify customers of new critical vulnerabilities that could impact their environment within 1 business day of the initial disclosure of the vulnerabilities by the source platform or feed.	Within 1 business days	99.99% (monthly)