Rapid7
120 Causeway Street
Suite 400
Boston, MA
02114
rapid7.com

Scope of Service

Managed Vulnerability Management - Basic (MVM Basic)

Rapid7's MVM Basic service leverages Rapid7 security expertise and technology to help customers programmatically manage and reduce their security risk.

By partnering with your team to understand your business goals, network, and assets, our goal is to deliver the peace of mind, focus, and consistency that customers expect from a managed service and to enable your team to effectively communicate and report on your security posture internally.

This document will outline the scope of Rapid7's MVM Basic service and how we plan to reach our stated mission, including:

- MVM Basic Service Overview
- Technology Overview
- Rapid7 Security Expertise
- MVM Basic Delivery Process
- Rapid7 Responsibilities and Requirements
- Customer Responsibilities and Requirements

Any responsibilities or actions not explicitly defined in this Scope of Service is not part of the Rapid7 Managed VM service.

MVM Basic Service Overview

Rapid7's MVM Basic offering provides a comprehensive picture of threat exposures and global criteria for risk prioritization to facilitate timely remediation across your environment.

Rapid7 MVM Basic is tailored to help you build, operationalize, or advance your current security program by implementing our proven three-pronged approach covering **Technology**, **Security Expertise**, and **Process**. Rapid7 MVM Basic provides your team tailored recommendations to manage, execute, and

optimize remediation across your environment—cloud, virtual, remote and local infrastructure—to strengthen your overall security posture and lower your risk exposure.

Vulnerability scans will be configured on a monthly cadence for up to 2500 IPs addresses as outlined on your order form. If intrusion detection/prevention systems (IPS/IDS) or web application firewalls (WAF) are in use, you must make exceptions to accept the originating IP address of the scanning tool/engine in order for Rapid7 to perform the scans. If this is not possible, then the scan should be originated from a network location that prevents IDS/IPS/WAF interference. Verification of the existence of or level of controls in place for IDS/IPS/WAF is outside the scope of the Rapid7 Managed VM service.

Scans will be configured to minimize interruption to the normal operation of your environment and will provide the depth of insight and risk context appropriate to your organization's needs. This is accomplished by gathering relevant data via regular vulnerability scans and delivering detailed actionable reports.

Scope of Service

The Rapid7 MVM Basic service includes:

- Monthly scanning of up to 2,500 IP addresses
- Scan configuration, continuous tuning, and scheduling for contracted IP addresses
- Monthly service reports as detailed in the "Remediation and Reporting" section below
- Monthly Remediation prioritization and guidance
- Recurring Monthly Meeting with Cybersecurity Advisor

Note: MVM Basic does not include Customer access to the Rapid7-hosted management console.

Technology Overview

MVM Basic service leverages and runs on Rapid7 Nexpose which allows you to identify blindspots, discover previously undiscovered devices on your network, pinpoint vulnerable assets, prioritize what matters most, and improve your overall security posture. Our resident experts utilize threat intelligence to have the most up-to-date threat data to help Cybersecurity Advisors better advise you on how to prioritize and remediate against vulnerabilities that could impact your environment.

- **Nexpose:** Rapid7's technology is the backbone of our MVM Basic offering and is designed to support the entire vulnerability management lifecycle. The Nexpose vulnerability scanner is used to identify, prioritize, and report your risk and combines real-time threat intelligence insights with a deep

understanding of your environment to manage vulnerability discovery through remediation and measurement.

- **Nexpose Scan Engine(s):** You are responsible for deployment and maintenance of any on-premises scan engines. Scan engines can be used for "traditional" target/host vulnerability and configuration analysis, but are also instrumental in network segment host discovery and detection. The output can be used as a primary or supplemental source to aid attack surface mapping for both your internal and external attack surface.

Rapid7 Security Expertise

Cybersecurity Advisor

Overview

Your Cybersecurity Advisor ("CA") is your main point of contact for the Rapid7 MVM Basic service. They are your trusted security partner to shepherd your organization's security maturity through remediation and ongoing security consultation. From the onset of this Scope of Service, your CA will collaborate with you to understand how Managed VM fits within your security program goals. The knowledge gained from these discussions will drive the contextual output of your program deliverables. During monthly meetings with your CA, there will be an opportunity for feedback resulting in holistic program development. All of this helps adapt existing policies and procedures to maximize our joint risk remediation efforts.

Throughout service delivery, your CA will communicate and drive discipline and vulnerability program improvements by using:

- Specific and adaptive product reporting
- Monthly measurements of program progress using in-product metrics

Each of these helps measure collaborative progress of your vulnerability management program.

Cybersecurity Advisors will be assigned after onboarding and are available during normal business hours (based on the assigned CA's local time zone) by phone, tickets, and email. For the fastest response, support tickets may also be raised via the Rapid7 Customer Portal at insight.rapid7.com/login.

You can find the Rapid7 Support Guidebook here:
https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-customer-support-guidebook.pdf

Engagement

During the course of the Managed VM service your team will engage primarily with your assigned CA. This resource is available to answer any questions about the Managed VM service and offer security advisorship as your security maturity improves. Outlined below are frequent interaction touchpoints that you will have with your CA:

Communication	Frequency	Method	Description
Monthly Meeting	Monthly	Videoconference or Phone	CA will hold one scheduled meeting (up to one hour in length) with customer stakeholders monthly to: • Review monthly reports and metrics • Discuss remediation prioritization, guidance, and progress • Answer questions about how to mature the overall program
Customer Requested Meeting	Ad-Hoc, requested through Online Support Portal*	Videoconference or Phone	You may request a meeting with your CA to address intended outcomes or questions regarding the service.
Customer Questions	Ad-Hoc	Online Support Portal	You may leverage the online Support Portal to request help or to voice concerns and questions related to the Managed VM service. Underlying Nexpose product issues should be directed to Rapid7 Technical Support.

* Subject to CA availability

MVM Basic Procedures

Tool Deployment and Management

The Rapid7 Managed VM Services Team will remotely deploy your Nexpose console with a standard configuration and any number of customer-deployed and maintained engines or engine pools. Nonstandard configurations are not supported.

Once the hosted and on-premises portions of the solution are deployed, your Cybersecurity Advisor will conduct a thorough walkthrough to introduce and verify the environment with you and other relevant stakeholders.

The Managed VM Team will perform the contracted vulnerability scanning against the contracted IP address ranges based on the goals defined at the onset of your services engagement. Throughout your service term, the Managed VM Team provides additional and ongoing tuning, hosted infrastructure maintenance, advises respective client teams on customer-maintained equipment updates and required maintenance, and fully administers necessary updates to those components that are hosted by Rapid7 as updates are made available. Rapid7 assumes responsibility for managing and adapting the scan schedule to operate within reasonable business constraints.

During your initial onboarding, goals are determined collaboratively. Tracking and scoring related to these goals are provided monthly Your CA will provide information pertaining to monthly scanning and remediation with a customer-designated primary and/or secondary point of contact.

Collect Data Across Your Ecosystem

Regular Discovery/Coverage Assessments. The first step in checking for vulnerabilities or configuration weaknesses is to make sure scan coverage encompasses all targeted assets in your organization. Your CA will help identify these assets as well as additional metadata by conducting periodic coverage analysis. Once this is completed, they will work collaboratively with you to maintain an ongoing vulnerability scanning schedule that suits your business and program.

Risk Prioritization using Real Risk and Data Validation

Granular Scoring. Using our Real Risk Score cross-referenced by CVSS scores, and criticality risk for your business, MVM Basic offers a high fidelity approach to actionable prioritization as well as an input into broader VM program and security investment decisions.

Vulnerability Prioritization. As part of the service, Rapid7 will assist with creating contextualized prioritization for customers using the provided Rapid7-driven research and analytics. By tracking exploited CVEs and trends in the real world, your CA correlates these trends against discovered vulnerabilities within the environment. Your CA will assist with grouping assets that can be tagged by location and ownership to see varying levels of risk and priority, thus driving greater risk reduction from finite security and IT operations resources.

Remediation and Reporting

Remediation Guidance. A vulnerability report is provided by your CA to customer stakeholders as part of the monthly meeting cadence. This review includes an analysis and prioritization of the overall results in the context of your unique environment and Rapid7 threat intelligence insights, and advice on remediation best practices and potential business impact if left unaddressed.

Reporting Deliverables. MVM Basic reporting provides metrics and context surrounding analysis activities, technology health, and findings summaries for an at-a-glance overview of your security posture. Once per month, the Managed VM Security Team will generate a report of findings for approved scans completed during the monthly scanning cycle. Your Cybersecurity Advisor will deliver reports monthly via the Rapid7 secure file transfer system based on the date preference determined with you. Reports are provided in PDF format (or CSV format upon request). These reports include:

Report Name	Description
Audit Report	Provides comprehensive details about discovered assets, vulnerabilities, and users.
Highest Risk Vulnerabilities	Provides information and metrics about ten (10) discovered vulnerabilities with the highest risk scores.
Remediation Plan	Provides detailed remediation instructions for each discovered vulnerability.
Risk Scorecard	Grades sets of assets based on risk and provides data and statistics for determining risk factors.
Top Remediations with Details	Lists top remediations as prioritized by vulnerability-related criteria that you select. Also provides steps for each remediation and lists each affected asset.

Data Retention

Vulnerability scan data will be retained for a maximum of twelve (12) months from the date of the scan. Rapid7 has no obligation to retain vulnerability scan data beyond the contract expiration date for MVM Basic Service.

Joint Requirements for Ensuring Success

The Rapid7 Managed VM service is delivered as a partnership between Rapid7 and each customer. To realize the full value of Rapid7 Managed VM, it is critical that both Rapid7 and your organization share in the responsibilities of the partnership. Below are each party's responsibilities and requirements for the effective delivery of the Managed VM service.

Rapid7 Responsibilities and Requirements

	Responsibilities and Requirements
1	Assist the customer with subject matter expertise to deploy the various required and optional Managed VM technology stack components.
2	Provide a named security advisor ("Cybersecurity Advisor") as the point of contact for the Managed VM relationship and a supporting CA team to help accelerate security maturity.
3	Work with the customer-designated point of contact to schedule scans and other jointly coordinated service deliverables.
4	Complete and provide all in-scope service deliverables.
5	Delivery of all reports via the Rapid7 secure file transfer system in accordance with this Scope of Service.
6	Provide continued guidance for vulnerability analysis and prioritization as the threat landscape changes.
7	Notify you of any CA or service delivery changes to Rapid7 Managed VM service.

Customer Responsibilities and Requirements

	Responsibilities and Requirements
1	Ensure network connectivity between the customer's on-premise equipment and the Rapid7 technology.
2	Designate a Project Manager/point of contact to work with Rapid7.
3	Complete the Deployment Survey prior to starting the deployment.
4	Deploy required customer site technology stack components, such as the Nexpose Scan Engine.
5	Ensure all key network, security, or other customer personnel are accessible for interviews or meetings as necessary for Services.

6	Provide Rapid7 with a list of relevant documentation (i.e., policies, procedures, diagrams, flow charts, etc.) necessary for Services.
7	Ensure availability of customer site-deployed scan engines (required) as well as their ability to report to Rapid7 infrastructure.
10	Properly permissioned credentials will be provided to Rapid7 to conduct reliable vulnerability scanning.
11	Notify Rapid7 of any personnel, technology, event source, or point of contact changes or modifications.

Terms and Conditions

This Scope of Service is governed by Rapid7's standard Master Services Agreement available at https://www.rapid7.com/legal/terms/ unless the parties have a fully executed Master Services Agreement which supersedes such standard terms. Any changes in materials or scope of work as defined in this document must be agreed upon in writing by you and Rapid7. Customer-deployed software and related services are governed by the Rapid7 Terms of Service available at https://www.rapid7.com/legal/terms/

Rapid7 may modify this Scope of Service at any time by posting a revised version here,, which modifications will become effective as of the first day of the calendar month following the month in which they were first posted.