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

Scope of Service

Managed Vulnerability Management

The mission of Rapid7’s Managed Vulnerability Management (Managed VM) service is to leverage our security experts to programmatically deliver the people and processes our customers need to effectively manage and reduce their security risk.

By working as your partner 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 while ensuring our customers maintain visibility into program activities and deliverables enabling them to effectively communicate and report on their security posture internally.

This document will outline the scope of Rapid7’s Managed VM service and how we plan to reach our stated mission, including:

- Managed VM Service Overview
- Technology Overview
- Security Expertise
- Process
- Rapid7 Responsibilities and Requirements
- Customer Responsibilities and Requirements

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

Managed Vulnerability Management Service Overview

Rapid7’s Managed Vulnerability Management (Managed VM) Program provides a comprehensive picture of threat exposures and global criteria for risk prioritization to facilitate timely remediation across your environment.

Rapid7 Managed VM 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 Managed VM provides your team tailored recommendations to manage, execute, and optimize remediation across your environment—cloud, virtual, remote, local, and containerized infrastructure—to strengthen your overall security posture and lower your risk exposure.

Vulnerability scans will be configured on a monthly cadence for (up to) the number of IPs addresses 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 in such a way as to minimize any interruption to the normal operation of the customer 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 Managed VM service includes:

- Hosted, and operationally managed, InsightVM console
- Scan configuration, continuous tuning, and scheduling for up to the contracted number of IP addresses
- Monthly scanning of contracted IP addresses
- Scan validation by our Managed Vulnerability Management Team to ensure successful scan completion with optimal coverage
- Monthly service reports as detailed in the "Remediation and Reporting" section below
- Monthly Remediation prioritization and guidance
- Recurring Monthly Meeting with Cybersecurity Advisor
- Periodic Business Review with Cybersecurity Advisor to discuss program trends, best practices, and recommendations for program advancement
- Customer access to the InsightVM service management console, allowing full visibility and access to service features and reporting at any time

Technology Overview

The Rapid7 Managed VM service leverages and runs on Rapid7 InsightVM which allows you to identify blindspots, discover previously undiscovered devices on your network, pinpoint vulnerable points, prioritize what matters most, and improve your overall proactive security posture. Our resident experts utilize threat intelligence to have the most up to date threat data, which helps them better advise on how to prioritize and remediate against today's vulnerabilities that may impact your environment.

InsightVM has many more supported integrations including: leading SIEM, ticketing, credential management, network topology, firewall, GRC tools, and many others. This helps your products work better together to collectively improve ROI from your existing security infrastructure while granting the Rapid7 team greater visibility into threats across your environment. Certain InsightVM features and custom integrations may not be supported by the Managed VM hosted console and/or would be considered out of scope for the Managed VM service.

Rapid7 Cloud Technology Architecture and Capabilities

- **Insight Cloud**: Responsible for all log management, data processing, enrichment, and storage of customer data. Each customer instance on the Insight cloud is isolated from other instances.

- **Insight VM:** Rapid7's technology is the backbone of your Managed VM offering utilized to identify, prioritize, and combines real-time threat intelligence insights with a deep understanding of your environment to manage vulnerability discovery through remediation and measurement.

- **Rapid7 Threat Intelligence Engine:** Primary Rapid7-developed intelligence paired with additional third-party sources to enrich prioritization and remediation processes.

Software Deployment and Configuration

- **InsightVM and Console:** Rapid7 Managed VM provides full customer access to a hosted InsightVM console and the Insight cloud platform which includes access to functionality such as project remediation tracking, goals and SLAs tracking, dashboard cards, and query filter reporting. Through the console, your team can take action without contacting your Cybersecurity Advisor while the Rapid7 Managed VM team maintains complete visibility. As part of Managed VM service deployment, Rapid7 will be responsible for initial installation and configuration of the InsightVM application and console in our hosted infrastructure.

- **Insight Scan Engine(s):** This application, used with the Security Console, helps discover and collect network asset data and scans them for vulnerabilities and policy compliance. You are responsible for deployment and maintenance of any on-premises Insight scan engines.

- **Insight Agent (optional but recommended):** Lightweight software you can install on supported assets—in the cloud or on-premises—to easily centralize and monitor data to identify vulnerabilities. This same agent can also be leveraged by other Rapid7 services such as InsightIDR or our Managed Detection and Response (MDR) service, if applicable. You are responsible for deployment and maintenance of Insight Agents.

Rapid7 Security Expertise

Cybersecurity Advisor

Overview

Your Cybersecurity Advisor ("CA") is your main point of contact for the Rapid7 Managed VM service. They are your trusted security partner—from initial technology deployment through remediation and ongoing security consultation—to shepherd your organization's security maturity. From the onset of your contract, your CA will collaborate with you to understand your goals with respect to how Managed VM fits within your security program. 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 continuous 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
- Periodic Business Reviews
- Monthly measurements of program progress using in-product metrics
- Leading VM Technology

All of these help measure collaborative progress of your vulnerability management program.

Cybersecurity Advisors will be assigned during onboarding and are available during normal business hours (based on the assigned CA's local time zone) by phone, tickets, and email. Severity 1 Support issues may be directed to Rapid7 Technical Support 24x7 at https://www.rapid7.com/contact/. 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	Online, Phone, or Screen Share	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
Periodic Business Review/Executive Business Review (PBR/EBR)	Periodically	Online, Phone or Screen Share	CA will hold one scheduled meeting (up to one hour in length) with customer stakeholders to provide a summary of service performance and present recommendations for how to further advance the customer's maturity. The CA will review: • Service trends and observations • Performance against goals • Best practices Note: The PBR replaces that month's Monthly Meeting. Once annually, the PBR may be tailored to a customer executive audience as an EBR upon request.
Customer Requested Meeting	Ad-Hoc, requested through Online Support Portal and	Online, Phone, or Screen Share	Meeting with CA to address concerns or questions regarding the service.

	subject to CA availability		
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 InsightVM product issues should be directed to Rapid7 Technical Support.

Threat Intelligence and Research Team

As the first vulnerability management provider to become a CVE numbering authority, Rapid7 understands your changing network, threat landscape, and impact to your specific business with Managed VM. The underlying technology is heavily influenced by our Threat Intelligence and Research teams to better help you defend against the changing landscape of malicious attackers' ability to attack your environment.

Our Rapid7 Threat Intelligence researcher team identifies new attacker trends across the global threat landscape and uses these findings to create in-product detection mechanisms for new vulnerabilities, exploits, and attack campaigns. These detections primarily leverage information from Rapid7's Metasploit Project, the most used pen testing tool for offensive security, and Project Sonar, an internet-wide survey across different services and protocols, to gain insights into global exposure to common and new exploitable vulnerabilities.

Rapid7's Threat Intelligence team supports the CA's with analysis and new information that we automatically include in InsightVM and apply to our vulnerability scans both on a routine and an ad-hoc basis.

Process

Tool Deployment and Management

The Rapid7 Managed VM Security Team will virtually deploy your InsightVM console with a standard configuration containing one console with any number of customer-maintained engines or engine pools. Non-standard configurations require custom scoping and may incur additional charges. Once the hosted and on-premises portions of the solution are deployed, your Cybersecurity Advisor will verify the service components of the environment with you and your team.

The Managed VM Security Team will perform the contracted vulnerability scanning against the initial IP address ranges designated based on your defined goals at the onset of your interaction. Throughout your service term, the Managed VM Security Team provides additional and ongoing tuning, hosted infrastructure maintenance, and updating of the hosted product components as associated software and hardware updates are available. Rapid7 will be responsible for managing and adapting the scan schedule to complete within reasonable business constraints. In some instances, you may need to access the InsightVM product; your Cybersecurity Advisor will continue to manage permissions and access to the product for those who have been approved.

During your initial onboarding, a number of goals are determined collaboratively. Tracking and scoring related to these goals is provided monthly and revisited during the scheduled Periodic Business Review with your CA. 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 Asset Assessments. Determining whether target assets are live can be useful in environments that contain large numbers of assets, which can be difficult to track. The first step in checking for vulnerabilities is to make sure scan coverage will encompass all the assets in your organization. Your CA will help identify these assets and additional information about the assets in your organization by conducting discovery. Once this is completed, they will work collaboratively with you to develop an ongoing vulnerability scanning schedule that suits your business and program.

Targeted Scanning. At points throughout your service, as the threat landscape changes or for compliance-specific reasons, you may need to scan different types of assets for different purposes and at different times than your pre-defined scanning schedule.

- **Ad-Hoc, Internal Scans**: Leveraging their product access privileges, customers may conduct ad-hoc, internal scans at any time (exclusive of product maintenance windows) with consultation on prioritization of findings available from your CA during their normal business hours.
- **External Scans:** External scans may be conducted as part of the monthly cadence or on an ad-hoc basis. These should be scheduled in coordination with the assigned CA based on customer requirements and external Rapid7 hosted scan engine availability.

Scan reviews are conducted with your CA on your scheduled monthly call to recommend a remediation plan for the assets and help reduce your risk. These regularly-scheduled reviews focus on specific areas of infrastructure and compliance needs.

Risk Prioritization Using Real Risk and Data Validation

Granular Scoring. Rapid7 Managed VM is fueled by Live Monitoring and Adaptive Security capabilities in InsightVM, which give your vulnerability management program fresh data and risk scores that are more granular than the industry standard. This degree of insight provides a deeper understanding of what attackers look for when targeting their attacks. Additionally, this scoring maps to your specific risk environment to include asset criticality, business-level criticality, and threat landscape criticality. Using our Real Risk Score cross-referenced by CVSS scores, Rapid7 threat intelligence, and criticality risk for your business, InsightVM offers a high fidelity approach to actionable prioritization.

With Rapid7's Live Monitoring of exposures, remediation can be reduced to a matter of minutes when applying an aggressive patching strategy. Managed VM utilizes this live feed so that the recommendations use the most recent data.

Vulnerability Scan Validation. Scan Validation provides confirmation that a scan returns high-fidelity results. This validation also ensures all remediation recommendations can be prioritized based on criticality and impact as to provide your team the guidance to make informed decisions for where to focus your remediation.

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.

Remediation and Reporting

Remediation Guidance. A vulnerability report is provided by your CA to stakeholders as part of the monthly meeting cadence. This review includes an analysis of the overall results in the context of your unique environment, prioritization based on the previous discussion, and advice on remediation best practices and business impact if it's not remediated quickly.

The CA is also able to help you establish remediation workflows within InsightVM that your team can leverage to track remediation and manage the progress to resolution. InsightVM allows you to integrate these workflows into the systems your team most uses, like ticketing systems (such as Atlassian Jira, ServiceNow ITSM, or email) or less structured methods to pass on the recommended actions.

Measuring progress. Managed VM allows your team to monitor the success of your vulnerability management program with trending data based on program goals from InsightVM dashboards. Overall program progress will be reviewed periodically and customers may receive a Periodic or Executive Business Review to perform a month-over-month retrospective that tracks progression against the success scorecard, to assess return on investment and effectiveness through qualitative analytics based on industry standards.

Reporting Deliverables. Once per month, the Managed VM Security Team will generate a report of validated findings for approved scans completed during the monthly scanning cycle. Generated reports are posted to the Rapid7 secure file transfer system for access within three business days of the end of the monthly scanning cycle. The reports may be provided in CSV or PDF format. These reports include:

- **Service Reports:** Metrics and context surrounding analysis activities, technology health, and findings summaries for an at-a-glance overview of Managed VM activities. Reports are often role-based and incorporate asset and vulnerability filters to help you with more than just prioritization and remediation. They also show auditors how your security environment has changed over time to confidently demonstrate compliance to regulations. Provided service reports include:

Report Name	Description
Audit Report	Provides comprehensive details about discovered assets, vulnerabilities, and users.
Executive Overview	Provides a high-level view of security data, including general results information and statistical charts.
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.

- **Ad-Hoc Threat Intelligence Reports:** When Rapid7's Threat Intelligence infrastructure or third-party threat intelligence partners identify new vulnerabilities or detection patterns, the Rapid7 team may publish a highly targeted analysis of the threat and its potential impact.
- **Reporting to the Executive and Board Level Teams**. One of the biggest challenges Security teams experience is managing up. Our CA will blend the cadenced interactions to develop a Periodic Business Review Scorecard and Executive Summary that confidently communicates the ongoing VM program progress to executive leadership and board. This includes trending analysis, a measurement against program goals, forward-looking program improvements, and other areas you've determined are important to communicate. Your CA will prepare this view with your primary point of contact, review it and present it directly to executives or the board if needed.

Technology Uptime

Rapid7 InsightVM follows the same uptime availability reflected by Rapid7's overall Insight Cloud Platform Service Level Agreement located at https://www.rapid7.com/legal/sla/.

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	Provision and manage Rapid7 cloud services in the technology stack.
4	Work with the customer-designated point of contact to schedule scans and other jointly coordinated service deliverables.

5	Complete and provide all in-scope service deliverables.
6	Delivery of all reports via the Rapid7 secure file transfer system in accordance with this Scope of Service.
7	Provide continued guidance for vulnerability analysis and prioritization as the threat landscape changes.
8	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 on-premises Rapid7 technology and the Rapid7 Insight cloud platform.
2	Deploy Insight Agent (optional) and scan engines and remedy gaps and dependencies in scanning operations.
3	Designate a Project Manager/point of contact to work with Rapid7.
4	Complete the Deployment Survey prior to starting the deployment.
5	Deploy required and optional customer site technology stack components.
6	Ensure all key network, security, or other customer personnel are accessible for interviews or meetings as necessary for Services.
7	Provide Rapid7 with a list of relevant documentation (i.e., policies, procedures, diagrams, flow charts, etc.) necessary for Services.
8	Ensure availability of customer site deployed technology including Insight Collector (optional), scan engines (required), and the Insight Agent (optional) as well as their ability to report to Rapid7 infrastructure.
9	Update the Rapid7 Insight Agent (if auto-updating is not enabled.) The Rapid7 Managed VM service supports the current version of the Insight Agent and up to two previous versions as signified by a change in the ones (x), tenths (y) or hundreds (z) of a version (x.y.z).
10	Allocate and configure space in one or more virtual computing platforms, and install Insight Collector(s), Insight Scan Engines, and other components as required .
11	Notify Rapid7 of any personnel, technology, event source, or point of contact changes or modifications.
12	For assets not using the Insight Agent, properly permissioned credentials will be provided to Rapid7 to conduct reliable vulnerability scanning.

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. 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.

Appendix

Managed VM Responsibilities Matrix

	InsightVM Product Only	Managed Vulnerability Management Service				
	Customer	Rapid7	Customer Main PoC	Customer Asset Owners	Customer IT	Customer C-Suite
Service Deployment						
InsightVM Application & Console Deployment / Maintenance	✓	✓				
Insight Scan Engine(s) Deployment & Maintenance	✓		✓	✓	✓	
Insight Agent Deployment	✓		✓	✓	✓	
Program Definition						
Define Goals and SLAs	✓		✓			✓
Define Asset Scope	✓		✓			✓
Define Internal Remediation Groups	✓		✓			
Scan Configuration & Execution						
Configure Scans	✓	✓				
Schedule Scans	✓	✓				
Inform Asset Owners	✓		✓			
Scan	✓	✓				
Monitor Stability	✓		✓	✓	✓	
Report any issues	✓		✓	✓	✓	
Troubleshoot any issues	✓	✓	✓	✓	✓	
Refine scan scope or template	✓	✓	✓			
Receive Scan Results	✓	✓				
Reporting & Remediation						
Run Reports	✓	✓				

Analyze Scan Results	✓	✓				
Provide Input and Remediation Recommendations	✓	✓				
Can/Wont Fix	✓		✓	✓	✓	
Action Plan for Won't Fix	✓		✓			
Accept Risk	✓					✓
Build Projects	✓	✓	✓			
Run Targeted Remediation Reports	✓	✓				
Define corrective actions of Will Fix	✓		✓	✓	✓	
Corrective Action Plan	✓		✓	✓	✓	
Implement Fix	✓				✓	
Discuss alternatives if fix doesn't work	✓		✓	✓	✓	