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

Scope of Service

Managed AppSec

Rapid7's Managed Application Security (AppSec) service leverages our application security experts to programmatically deliver the people and processes our customers need to effectively manage and reduce their application security risk.

By working as your partner to understand your business goals, applications, and environments, 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 application security posture internally.

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

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

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

Managed AppSec Service Overview

Rapid7's Managed AppSec service provides customers with a comprehensive picture of their threat exposures along with global criteria for risk prioritization in order to facilitate timely remediation of their application security vulnerabilities.

Rapid7 Managed AppSec 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 AppSec provides your team tailored recommendations to manage, execute, and optimize remediation of identified web application vulnerabilities to strengthen your overall security posture and lower your risk exposure.

Scans will be configured monthly for the number of applications under management by Rapid7. If intrusion detection/prevention systems (IPS/IDS) or web application firewalls (WAF) are in use, the customer 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 applications is outside the scope of the Rapid7 Managed AppSec service.

Scans will be configured in such a way as to minimize any interruption to the normal operation of the customer environment and to provide the depth of insight and risk context appropriate to the customer 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 AppSec service includes:

- Scan configuration, scheduling, and continuous tuning of contracted applications
- Monthly dynamic application security testing (DAST) scans of contracted applications[1]
- Vulnerability validation by our Managed Application Security Team to remove false positive findings and suppress duplicate findings, leaving only actionable vulnerabilities
- Monthly vulnerability report
- Monthly remediation prioritization and guidance
- Monthly Meeting with Customer Advisor
- Customer "read-only" access to the InsightAppSec service management console, allowing visibility to service activity and reporting.

Technology Overview

The Rapid7 Managed AppSec service leverages and runs on Rapid7 InsightAppSec and includes additional techniques that allow Rapid7 to identify vulnerabilities as an attacker would, prioritize what matters most, and improve your overall proactive security posture.

[1] Each contracted application will be scanned in a single environment. The total number of scan configurations may not exceed 125% of the total number of applications under management. For example, Rapid7 will support up to 15 scan configurations for a customer with 12 applications under management.

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.

- **InsightAppSec:** Rapid7's technology is the backbone of your Managed AppSec offering utilized for vulnerability identification and prioritization and providing a deep understanding of your environment to manage vulnerability discovery, prioritization, and remediation. InsightAppSec is Rapid7's proven, SaaS-based DAST tool combining powerful application crawling and attack capabilities and flexible scan configuration options to ensure comprehensive coverage of applications, including support for modern application frameworks like SPAs and APIs. InsightAppSec also supports the scanning of internal applications (e.g. pre-production instances) with a scan engine deployed on premises.

Security Expertise

Rapid7 will provide knowledgeable security experts to perform application security testing using Rapid7's InsightAppSec DAST scanning product. Rapid7's Managed Application Security team, which includes an English-speaking Managed Service Customer Advisor (CA), will complete these scanning activities, deliver the reports to the customer and provide remediation recommendations based on industry best practices and software development life cycles.

Customer Advisor

Overview

The Customer Advisor ("CA") is the customer's main point-of-contact for the Rapid7 Managed AppSec service. This named resource works with the customer's team as a strategic security partner—from initial technology deployment through incident remediation and ongoing security consultation—to shepherd each customer organization's security maturity.

From the onset of your contract, your CA will work with you to address your goals and success criteria for Managed AppSec. The output of this will be a monthly cadenced scan schedule and 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 the service, the CA will communicate with the customer's designated point of contact to provide updates on service delivery, reporting, metrics, and application security posture to drive discipline, application security program improvements, and ensure we are addressing the customer's security goals.

Customer Advisors will be assigned during onboarding and are available during normal business hours (based on the assigned CA's local time zone) by phone and email.

Engagement

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

Communication	Frequency	Method	Description
Monthly Meeting	Monthly	Video conference or Phone	CA will hold one scheduled meeting (up to one hour in length) with customer stakeholders monthly to: - Review monthly vulnerability report - Discuss remediation prioritization and guidance - Answer questions about how to mature the overall program
Customer Requested Meeting	Ad-Hoc, requested through Online Support Portal and subject to CA availability	Video conference or Phone	Meeting with CA to address concerns or questions regarding the service.
Customer Questions	Ad-Hoc	Rapid7 Online Support Portal	You may leverage the online Support Portal to request help or voice customer concerns/questions.

Process

Service Onboarding and Deployment

Introduction of the Rapid7 team to the customer's authorized contacts. A review of applications to be scanned and a 30-60-90 day timeline review will be conducted to ensure overall alignment. Lastly,

communication channels will be discussed and a primary and a secondary point of contact will be designated by the customer to work with the Rapid7 Customer Advisor.

Scan Engine Deployment. If internal applications are under contract for management, the Managed Application Security Team will work with the primary and/or secondary customer points of contact to coordinate deployment of internal scan engines on the customer premise. This includes the customer granting Rapid7 access to the customer's network to facilitate this action.

Schedule monthly meetings with customer. The CA will provide communication and information pertaining to the scanning and remediation of applications under management with the designated primary and secondary customer points of contact.

Current Web Application Security Posture and Program Assessment

Review processes and procedures. The assigned CA will work with the customer to understand the customer's environment and workflows to best facilitate achievement of the customer's application security program goals and success criteria.

Scan Schedules and Continuous Tuning. Once targets have been identified and initial discovery has been completed, Rapid7's Managed Application Security Team will make best effort attempts to configure scan in such a way as to achieve optimal coverage of the site. The Managed Application Security Team will also coordinate scheduling of scans to accommodate business or infrastructure needs.

Monthly Scanning. Information security threats and vulnerabilities are constantly evolving, and ongoing vigilance is required. Monthly scans will be performed as scheduled for contracted applications. The vulnerability scanning will identify vulnerabilities in the targeted web applications at the point in time that the review occurs. Application swapping is not supported as part of the monthly scan cadence.

Prioritization Using Real Risk Impact

Scan validation provides confirmation that a scan is high-fidelity. This validation thoroughly reviews the accuracy of the scans and attempts to ensure the scan completes with optimal coverage. This validation also extends to ensure all remediation recommendations are prioritized based on criticality and impact as to provide your team the guidance to make informed decisions for where to focus your remediation.

Vulnerability Validation. After scans have been completed, Rapid7's Managed Application Security Team will attempt to validate any "High," "Medium," or "Low" severity vulnerability findings (as defined by Rapid7 in the Managed AppSec attack policy) from the scan. This will be accomplished using various tools or analyzing the scan data directly to eliminate findings that are false positives or contextually have no

impact to the business. The Managed Application Security Team will also make best efforts to align vulnerability findings with the business's concerns regarding web application security.

Vulnerability Remediation Validation. If you believe you have pushed a fix for a specific verified finding on a contracted application, you may request a revalidation of the finding via the Rapid7 online Support portal. Revalidation requests must include a link to the finding in InsightAppsec.

Vulnerability Prioritization. As part of the service, Rapid7 will assist with creating contextualized prioritization for customers. The Managed Application Security Team will prioritize vulnerabilities identified from scans. The prioritization will be focused on the criticality of the application as defined by the customer and the default severity of vulnerabilities (or combinations of vulnerabilities) in InsightAppSec unless otherwise configured to meet customer's needs.

Reporting and Remediation Guidance

Reporting. Once per month, the Managed Application 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 Services Portal for customer access within seven (7) calendar days of the end of the monthly scanning cycle. The reports may be provided in formats that include but are not limited to CSV, HTML, PDF, or XLSX. Report format, content, and layout are subject to change as the InsightAppsec technology and/or the Managed AppSec service evolve. Changes will be implemented at the discretion of the Managed Application Security team.

Remediation Guidance. The Managed Application Security Team will support vulnerability response actions across the enterprise for validated “High,” “Medium,” and “Low” severity findings. Scan results, reports (including any reporting issues or anomalies), and remediation guidance will be reviewed with the customer by their assigned CA during the scheduled monthly meeting.

Joint Requirements for Ensuring Success

The Rapid7 Managed AppSec service is delivered as a partnership between Rapid7 and each customer. To realize the full value of Rapid7 Managed AppSec, 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 effective delivery of the Managed AppSec service.

Rapid7 Responsibilities and Requirements

	Responsibilities and Requirements
1	Provide a named security advisor ("Customer Advisor") as the point-of-contact for the Managed AppSec relationship and help accelerate the customer's security maturity.
2	Assist with initial service deployment and implementation.
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 Services Portal in accordance with this Scope of Service.
6	Notify you of any CA or service delivery changes to Rapid7 Managed AppSec service.

Customer Responsibilities and Requirements

	Responsibilities and Requirements
1	Designate a Project Manager/point of contact to work with Rapid7.
2	Ensure all key network, security, or other customer personnel are accessible for interviews or meetings as necessary for Services.
3	Provide Rapid7 with a list of relevant documentation (i.e., policies, procedures, diagrams, flow charts, etc.) necessary for Services.
4	Install virtual machines and/or software in the customer environment as requested by Rapid7 to enable delivery of Managed AppSec service.
5	Provide Rapid7 with necessary access to the customer systems and applications in scope. This includes allowing scans to run without interference from web application firewalls or filters designed to block specific scanning injections.
6	Access the InsightAppSec service management console in a "read only" manner unless explicitly reviewed and approved by the assigned Rapid7 CA.

Additional Terms

This Scope of Service is governed by Rapid7's standard Master Services Agreement, and any other terms and conditions, as applicable, available at https://www.rapid7.com/legal/terms/ unless the parties have a fully executed Master Services Agreement which supersedes such standard 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.