InsightAppSec Deployment Handbook

Thank you for Advancing Securely with Rapid7. Within this document, you'll find system, network, and functional requirements, a project plan, and additional resources you may need to successfully prepare for your deployment. If you have any additional questions, please send those to your Project Manager or your Security Consultant.

Preparing for Deployment: 2
- Change Control 2
- Multi-Team Stakeholder Participation 2
- Technical Preparation 3
  - Chrome Plugins 3
  - Virtual Machine Requirements 3
  - Recommended Operating Systems InsightAppSec Scan Engine 3
  - Software requirements 5
- Connectivity Preparations 5
  - Your Insight Platform Account 5
  - Architecture Diagram 5
  - Firewall Rules and Network Connectivity Requirements 6
  - Connectivity requirements for (internal) on-premise Scan Engines 1
- Applications & Credentials 1

Project Plan 1

Supplemental Resources 1
- InsightAppSec API 1
- Health Check 1

Preparing for Deployment:

In order for your InsightAppSec deployment to be successful, you **MUST** have the following resources in place prior to the first day or your deployment:

Change Control

It is common for many organizations to employ a change control process around their IT environments. To ensure a successful deployment, change controls must be approved prior to Deployment, to enable implementation and testing of product functionality. Consider mitigation action, for example: if change control has been submitted, but not approved, or an emergency change is required, what course of action can be taken to keep the deployment moving?

Multi-Team Stakeholder Participation

Cybersecurity often involves teams outside of the direct security team deploying the software. For example, an IT team can speak to existing hardware – whereas a provisioning team can speak to how new hardware is onboarded. Managerial staff can additionally provide context around key performance indicators ("KPI")s and required compliance that must be met for things like data retention.

Having several teams involved in the deployment of InsightAppSec will ensure a successful rollout within your environment, allow for cross training and improved understanding of findings.

We recommend that you have representatives from the following teams available during the deployment. They do not need to be present during the entire deployment timeframe, but need to have the flexibility to join at relatively short notice.

- Cybersecurity Managerial staff, providing guidance around KPI's, priorities and reporting needs
- System Administrator capable of installing software if local scan engines are used, and whom can create credentials for testing within target applications
- InsightAppSec Administrator (should be available throughout)
- Network Administrator: capable of modifying and troubleshooting routing or access controls
- Web Application Owners and/or Development Leads: able to provide permission for scanning and context around any findings from scans

Technical Preparation

Chrome Plugins

Part of deployment services involves configuring authentication for your web applications. For any apps with complex authentication, the Rapid7 InsightAppSec Chrome plugin or the Selenium Chrome plugin are required.

https://chrome.google.com/webstore/detail/selenium-ide/mooikfkahbdckldjjndioackbalphokd?hl=en

https://chrome.google.com/webstore/detail/rapid7-appsec-plugin/mnmlipalillmakdiildpclhocfgcddnp?hl=en-US

Virtual Machine Requirements

If any of the app instances within scope are **NOT** accessible publicly, an InsightAppSec scan engine can be deployed within your environment. This is commonly necessary if the application is internal-use only OR an internal-only development/testing environment is being scanned (it is STRONGLY recommended to scan apps in a Dev/UAT environment instead of production).

If you are scanning apps inaccessible from the internet, you **MUST** have a machine available prior to your deployment sessions.

Based on your environment, you may need:

- 1 machine to be used as an IAS Scan Engine

This machines should match the following criteria

System	Proc / Core Count	RAM (GB)	Disk
IAS Engine	4	8	100GB

Recommended Operating Systems InsightAppSec Scan Engine

Rapid7 recommends that you deploy your Engines onto one of the following operating systems *

- English operating system with English/United States regional settings

- 64-bit versions of the following platforms are recommended:
    - Windows Server 2016
    - Windows Server 2019
    - Windows Server 2022

* You will be able to find additional supported operating systems here:
https://docs.rapid7.com/insightappsec/setting-up-an-on-premise-scan-engine/

Software requirements

All of the below software requirements **MUST** be met, or you will not be able to deploy the on-premise scan engine:

- .NET 4.8 (must be this **EXACT** version of .NET)
- Internet Explorer 11 or higher
- To use selenium macro files, you must install Chrome on the same server as the on-premise engine.

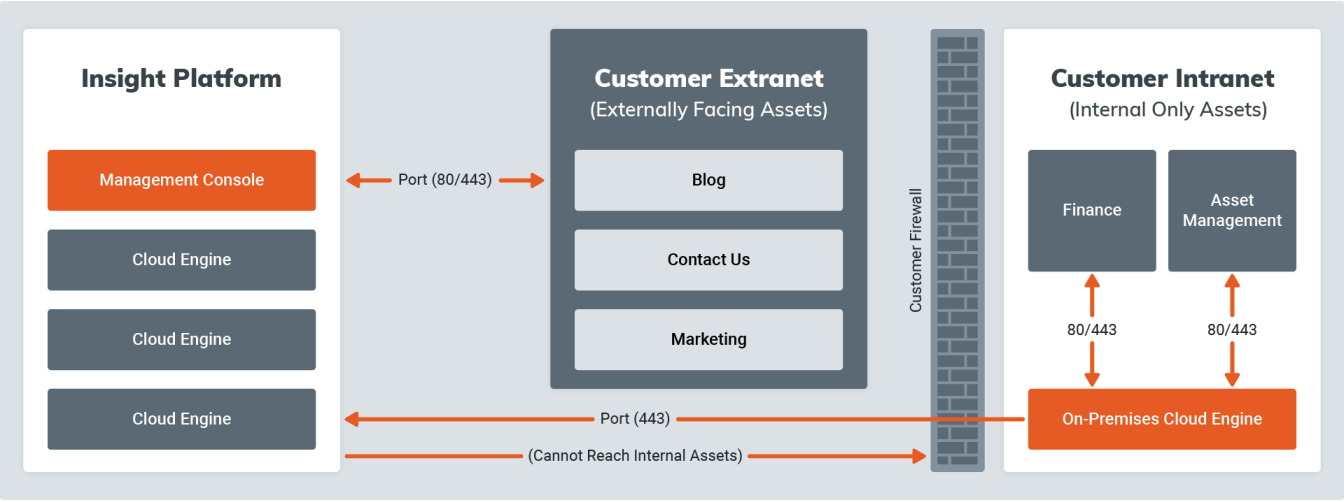
Connectivity Preparations

Your Insight Platform Account

Before the deployment can commence, an Insight Platform account is required. Please visit this URL and verify that you have an account provisioned: insight.rapid7.com/login.

If you do not have access, please contact your Rapid7 representative before the deployment, to ensure that the account is created in-time for your deployment.

Architecture Diagram



Firewall Rules and Network Connectivity Requirements

If your Web application is being scanned from the Rapid7 Cloud Engines, you can expect traffic from the below listed ip addresses. Please ensure that you allow traffic from our Cloud Engines, so that your web application can be scanned successfully.

Note: Region is the data storage region selected in your insightPlatform instance.

Region	Source IPs
US1	34.205.208.125 34.192.183.106 34.224.19.93 34.227.121.223
US2	52.14.12.25 52.14.88.11 3.22.113.166
US3	52.36.241.148 52.36.245.161 44.228.9.4
EU	35.158.144.37 35.156.166.245 172.104.153.232
AU	52.63.190.180 52.62.83.29 139.162.25.220
AP/Tokyo	172.104.83.134 52.68.0.155 54.64.21.140

Connectivity requirements for (internal) on-premise Scan Engines

If you are leveraging a scan engine located in your own environment instead, please ensure that all relevant ports required have been allowed, and that it has the ability to contact the insight platform (domains listed below).

Note: Region is the data storage region selected in your insightPlatform instance.

Source	Destination	Port
Cloud Scan Engines: List of IP Addresses	Your Public Facing Web Applications	80/443*
On-Premises Scan Engine (All Regions)	Your Internal Web Applications (To scan internal applications, see Section 1)	80/443*
On-Premises Scan Engine Region: United States 1	us.appsec.insight.rapid7.com us.engines.appsec.insight.rapid7.com	443
On-Premises Scan Engine Region: United States 2	us2.appsec.insight.rapid7.com us2.engines.appsec.insight.rapid7.com	443
On-Premises Scan Engine Region: United States 3	us3.appsec.insight.rapid7.com us3.engines.appsec.insight.rapid7.com	443
On-Premises Scan Engine Region: Europe	eu.appsec.insight.rapid7.com eu.engines.appsec.insight.rapid7.com	443
On-Premises Scan Engine Region: Canada	ca.appsec.insight.rapid7.com ca.engines.appsec.insight.rapid7.com	443
On-Premises Scan Engine Region: Japan	ap.appsec.insight.rapid7.com ap.engines.appsec.insight.rapid7.com	443
On-Premises Scan Engine Region: Australia & New Zealand	au.appsec.insight.rapid7.com au.engines.appsec.insight.rapid7.com	443

*Not all sites operate over the standard ports (80 and 443). You may need different ports depending on your organization's web applications.

Note: The table above serves as a guide for all known communication requirements. During installation and configuration it is possible to find additional requirements not documented above. Please have a firewall expert available in the event additional rules will need to be created during the engagement.

Applications & Credentials

During the deployment, your consultant will work with you to configure your applications for scanning using the credentials provided (where applicable). You may use this example form to collect what is required for your applications:

Application URL	Environment	Username	Password	Role
rapid7.com	*Dev / UAT / Prod*	*r7user*	*(See Vault)*	*Administrator*

Are any of these environments private? Our cloud engines will not be able to scan inside environments that are not reachable from the Internet. If you web application operates in a private network zone, you will need to ensure that you deploy an on-prem scan engine close to the application. Make sure you have a VM that meets these system and network requirements. Your consultant will help you get the engines in place during your engagement.

Are any of these environments production? Scanning production web applications is ***not*** generally recommended, as it comes with a certain level of risk that the application may be affected in a negative manner (i.e. crashing, fragments of benign data inserted into application or databases, certain data deleted).

To safely scan these applications, it is advised to first scan a development or User Acceptance Testing version of the application, so that any potential side effects of scanning may be uncovered.

Project Plan

We include below a sample project plan for an InsightAppSec Deployment. Timing and order may be customized to your specific environment and needs by your Rapid7 consultant during deployment.

An InsightAppSec deployment is typically delivered in a single session. Depending on the size of your environment and it's complexity, it may however extend across multiple sessions:

Project Kick-Off
Project Kick Off Call, covering the following topics: • Prerequisites discussion • Confirm that customer is able to login to the Insight Platform and can navigate to User Management, to confirm Platform Admin permissions and product access • Firewall rules complete OR verified ability to configure them during deployment calls • Service accounts and/or Web Application accounts in place for scanning OR admin scheduled to attend deployment calls • Change Management approvals for scanning and infrastructure changes • Optional server(s) provisioned and accessible
Deployment Session
Review InsightAppSec Architecture and components
Review goals for Deployment
Discuss User Management • Audit current users, removing any proof-of-concept users that may exist and discussing how platform and product roles relate to the tool
Discuss Engine Management • Discuss how engines and engine groups function • Install engine(s) as needed and pair with the platform • Update any pre-existing engines • For larger customers, designate scanning groups based on technical and geographic requirements
Discuss Blackouts
Discuss Scan Templates • Differences with in-built templates • Risks of scanning • Active vs. Passive modules, and settings for each • If desired, build out scan templates
Discuss Ticketing Integrations If your organization uses Jira Cloud or ServiceNow, we will explain how this works and can integrate insightAppSec with it
Discuss Notifications
Targets & Scanning *(This section is often repeated multiple times throughout the deployment process)*

Discuss Targets ● Pre-existing hosts (webscantest.com and hackazon.webscantest.com) ● Enabling and disabling targets ● Adding Targets and how that impacts what apps can be used ● How scanning affects deletion of apps
Discuss and Create “Apps” ● Uses for “Apps” as containers ● User Permissions
Discuss and Create “Scan Configs” ● Configure the scan config to use authentication, and the proper engine, to scan your applications Authentication discussion may cover one or more types of authentication, such as: ○ No Authentication ○ Macro ○ Traffic ○ Selenium ○ OAuth ○ HTTP Basic/NTLM ○ Bootstrap ○ Session Hijacking
Advanced Scan Parameters: ● Discuss, and modify where needed, the advanced parameters of the scan configuration, such as: ○ HTTP Headers ○ Authentication Validation RegEx ○ Scan Templates ○ WSDL / REST API Scanning ○ Traffic and Macro Application Guidance ○ Advanced Options, such as browser config, ParameterTrainingConfig and the impacts of multilingualism on context-driven, automated form completion
Trigger a scan, and configure schedules ● Review attributes of the scan config page
Troubleshooting
● Show how to access the various logs, such as the operations log, platform event log, and the traffic log. ○ For the traffic log, detail the file naming convention, as well as the contents of the traffic log.
Evaluate Scan Results
● Generating reports from InsightAppSec ● Using queries to sort and prioritize the discovered vulnerabilities ● Review the vulnerabilities pane

• If a valid attack exists, demonstrate the replay capabilities • Dashboards
Post Deployment
• At the end of each day of your deployment, your consultant will send a Status Update detailing what work has been accomplished, what remains, and any risks identified during the engagement. • At the end of the full deployment, you will also receive a survey that will allow you to share feedback with the leadership team on what we did well, and where we can improve.

Supplemental Resources

InsightAppSec API

InsightAppSec offers an application programming interface (API) for working with scans, results, and more. To learn about our API or download our definition document, visit:

help.rapid7.com/insightappsec/en-us/api/v1/docs.html

Health Check

To ensure your team is using InsightAppSec to its fullest potential, schedule a regular health check. Rapid7 consultants will review your scanning coverage, credential usage, scan configurations, and how you are reacting to vulnerabilities.