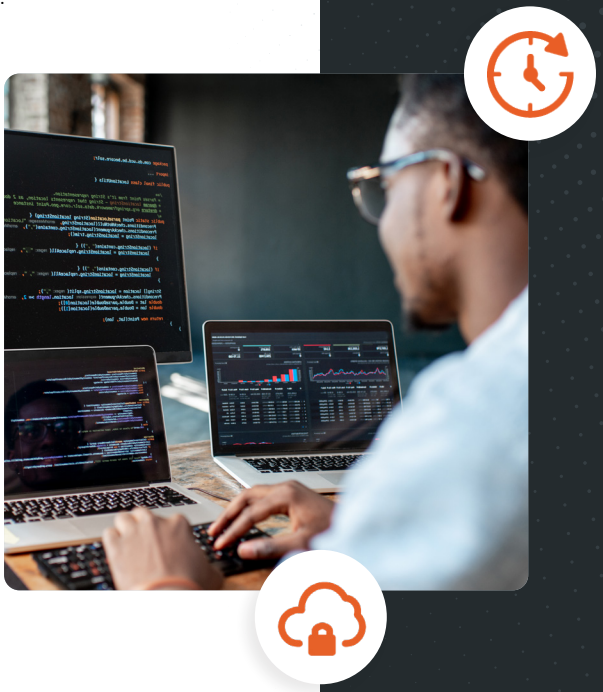
InsightIDR Deployment Services

Rapid7's InsightIDR deployment services brings together key Rapid7 capabilities and security expertise to accelerate customers time-to-value with Rapid7 products. It also lays the foundation for ongoing security health outcomes.

This document will outline the scope of Rapid7's Implementation Success Package and how we plan to reach our stated mission, including:

Any responsibilities or actions not explicitly defined in this service brief are not part of the deployment services.



Scope of Service

The Rapid7 InsightIDR deployment service includes:

Customer Expectations

The success of the customer's onboarding experience depends on their active engagement and partnership. The customer is responsible for providing the following to ensure successful implementation:

- Primary point of contact
- Project participants contact information

Technical Deployment

The technical deployment is designed to assist your team in leveraging InsightIDR with the goal of ensuring the health of the installation, providing team enablement, and, if indicated, providing recommendations for expansion.

Insight Platform Foundation

InsightIDR deployment includes an overview of the Insight Platform and configuration in line with Rapid7 best practices. Platform configuration includes:

- Review and implementation of recommended multi-factor authentication (MFA) and single sign-on (SSO) configurations (as applicable)
- Review of Insight Platform best practices for administration and auditing
- Establishment of Insight Agent deployment strategy

InsightIDR Deployment Overview

InsightIDR deployment services consist of establishing initial configuration of the product. Deployment has the dual goals of establishing a baseline configuration and enabling your team to ensure you maintain oversight as your environment evolves.

Specific activities during deployment:

- Discuss the placement, resource requirements and connectivity for the InsightIDR collectors and agents.
- Deploy and Pair up to one (1) collector.
- Discuss best practice implementation of InsightIDR core event sources.
- Discuss other forensically relevant event sources.
- Configure one (1) of each core event source and provide enablement on how to configure remaining core event sources independently. Note that some environments, particularly those that are fully cloud-based, may not deploy all traditional core event sources. Applicable core event sources include:
- Active Directory (1), LDAP (1), DHCP (1), VPN (1), Firewall (1)
- Review and configure product settings.
- Demonstrate log search capabilities and how to perform basic LEQL queries using our powerful search language Log Entry Query Language (LEQL).
- Review dashboards and reporting.
- Discuss alerts, investigation workflow, and threat feeds.
- Review and discuss capturing custom logs and using the custom data parser.
- Review and discuss automation workflows.
- Review and discuss custom alert creation.
- Review and discuss Network Traffic Analysis.

InsightIDR Customer Expectations

Activities are dependent on the customer completing all prerequisite steps prior to the deployment engagement. Configuration items missing prerequisites will be covered on a theoretical basis and self-service resources for implementation will be provided. No additional time will be scheduled to account for missing prerequisites during initially scheduled meetings.

Deployment services will provide advice but is unable to directly configure or guarantee the following are completed during the engagement:

- Configuration of one (1) of each core event source
- SSO if the SSO administrator is not present on the deployment call with change-management steps completed

**Note: Deployment is limited to the installation of Rapid7 products and does not include prerequisites such as provisioning physical or virtual resources/servers.*

About Rapid7

Rapid7 is creating a more secure digital future for all by helping organizations strengthen their security programs in the face of accelerating digital transformation. Our portfolio of best-in-class solutions empowers security professionals to manage risk and eliminate threats across the entire threat landscape from apps to the cloud to traditional infrastructure to the dark web. We foster open source communities and cutting-edge research–using these insights to optimize our products and arm the global security community with the latest in attacker methodology. Trusted by more than 11,000 customers worldwide, our industry-leading solutions and services help businesses stay ahead of attackers, ahead of the competition, and future-ready for what's next.

RAPID7

PRODUCTS

Cloud Security
XDR & SIEM
Threat Intelligence
Vulnerability Risk Management
Application Security
Orchestration & Automation
Managed Services

CONTACT US

rapid7.com/contact

To learn more or start a free trial, visit: https://www.rapid7.com/try/insight/