RAPID7

WHITEPAPER

Insight Cloud Security

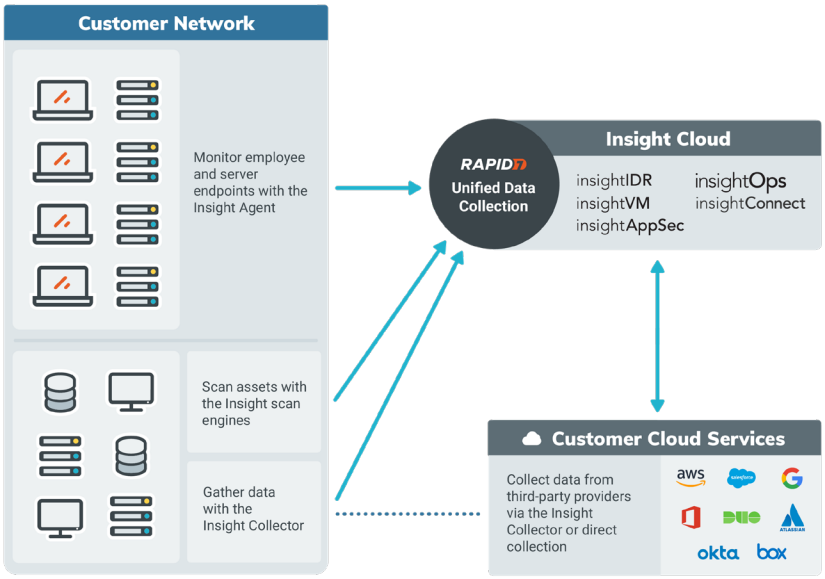
| Q3 2019

TABLE OF CONTENTS

Overview

The Rapid7 Insight cloud provides data collection, visibility, analytics, and automation to establish a shared point-of-view between security, IT operations, and development teams. Our cloud platform delivers one-click access to Rapid7's vulnerability management, application testing, incident detection and response, and log management solutions. This document introduces the architecture, security mechanisms, and technical foundations that make up the Rapid7 Insight cloud.

INSIGHT CLOUD ARCHITECTURE



Data Collection

The Insight cloud offers multiple options for collecting data across your IT environment. Whether you use collectors, the Rapid7 Insight Agent, scan engines, or direct connections to our platform, our unified data collection enables your teams to collect data once and use it across multiple products on the Insight cloud. Once configured, data sources continuously collect data, enabling teams to collaborate effectively as they analyze shared data, alert on risk vectors, and automate remediation and breach response.

Collectors

Rapid7 uses collectors to gather information from on-premises and cloud networks to securely transfer data to the Insight cloud. Collectors sit behind the client's firewall, respond to changes in the environment, and securely transmit relevant data to our platform for analysis.

Collectors were designed with the following core tenets in mind:

- Only administrators can configure collectors.
- All data is secured during the transmission process, which uses strong encryption protocols.
- Data transferred from each separate collector is uniquely identified and stored and cannot be accessed by any third parties.

During installation, a collector reaches up to the Insight cloud and hands off the shared secret (activation key) by performing a challenge-response handshake. Once the initial handshake is complete, a unique pair of cryptographic keys will be generated. These crypto keys are used for all subsequent collector to Insight cloud communications.

The collector relies on a TLS connection (HTTPS) to communicate with the Insight cloud. Specifically, the collector is explicitly coded to trust only certificates that have a signature chain that can be vetted by one of the Java trust store Certificate Authorities (CAs). Once the challenge-response handshake is complete, the collector is ready to accept command and control instructions from the Insight cloud. For security reasons, the collector always reaches out to the Insight cloud; the Insight cloud cannot reach through the client's firewall and initiate a conversation.

Rapid7 Insight Agent

The universal Insight Agent is lightweight software you can install on any asset—in the cloud or on-premises—to easily centralize and monitor data on the Insight cloud. The Insight Agent gives you endpoint visibility and detection by collecting real-time system information—including basic asset identification information, running processes, and logs—from your assets and sending this data back to the Insight cloud for analysis. The Insight Agent can be installed directly on Windows, Linux, or Mac assets. Each Insight Agent only collects data from the endpoint on which it is installed.

The Insight Agent authenticates using TLS client authentication. When you deploy the Insight Agent, the deployment includes a private SSL key representing your organization. This key is used to authenticate and authorize your agent with the Insight cloud.*

The agent can communicate directly to the Insight cloud, or proxy communication through existing web proxies or collectors on your network. Finding the best route to the Insight cloud occurs automatically or can be configured in advanced use cases.

**For InsightOps log data, an API token is used to authenticate the Insight Agent instead of TLS client authentication. Log data is encrypted in transit via TLS.*

Scan Engines

On-premises scan engines are used by InsightVM and InsightAppSec to scan Rapid7 customers' environments by finding and remotely connecting to systems to retrieve asset information.

InsightVM scan engines perform vulnerability scans of your networks and report results back to the InsightVM console using TLS 1.2 (HTTPS). Engines can be distributed across internal networks, public networks, and cloud providers. Scan engines provide strategic views of your network from an attacker's perspective. In deciding how and where to deploy scan engines, you choose how you would like to "see" your network. Scan engines can be configured to perform authenticated scans to check for software applications and packages and to verify patches.

InsightAppSec scan engines allow scanning internal web

applications that aren't accessible to the public Internet. Engines connect to the web applications you configure and report results back to the Insight cloud. For security reasons, the InsightAppSec scan engine always reaches out to the Insight cloud for instructions; the Insight cloud cannot reach through the client's firewall and initiate a scan.

Insight Orchestrator

The Insight Orchestrator is installed in your environment to gain access to on-premises products, services, and tools. The Orchestrator enables automation capabilities across the Insight cloud, including in InsightConnect, InsightIDR, and InsightVM.

Similarly to the collector, the Orchestrator relies on a TLS 1.2 connection (HTTPS) to communicate with the Insight cloud. The communication from the Orchestrator to the Insight cloud is cryptographically signed via ECDSA with a challenge token that expires every 30 seconds and refreshes on each call to the Insight cloud. This ensures the validity and origin of messages received from the Orchestrator.

tCell Agent

The tCell Agent integrates with your web application and web server code to monitor all incoming requests and block malicious requests that can attack your application. The agent sends data to the Insight Platform using a revocable API key over TLS.

Cloud Collection and Integrations

Rapid7 collects some data directly via a connection with the Insight cloud. The Insight cloud can connect to third parties on your behalf, such as container registries for InsightVM.

You can also send data directly to us via our APIs or with one of our software libraries or extensions, such as the InsightOps application logging libraries.

For details on the collection methods and specific data collected for each product, please visit help.rapid7.com.

Credential Storage

To generate value and collect data, our products require access to credentials with a high level of privilege on your networks. Credentials are stored differently depending on where and how they are used. Credentials are always encrypted before being stored in the Insight cloud. Where possible—such as when collecting data with collectors—credentials can only be decrypted by on-premises components and not the Insight cloud itself.

Collectors

All credentials used by a collector to obtain data from your local environment are strongly encrypted in a manner that prevents the passwords from being decrypted based on the information stored in the cloud. Every collector installation generates a unique public/private key pair that is then split across environments. The public key is uploaded to the cloud, and the private key is stored locally on the collector. When writing the private key to the local disk, the collector encrypts the private key contents. The private key can only be decrypted using information obtained via successful communication with the Rapid7 Insight cloud, thus only active, live collectors with healthy communication with the cloud can access the private key.

Whenever a credential is added to a collector, the credential is encrypted using an RSA 4096-bit public key associated with the specific collector where the credential is being deployed. It is then persisted in the database within a client-specific database schema. Once the credential is stored, the Insight cloud no longer has access to the cleartext credential. When that particular collector needs to use a credential, the encrypted password is retrieved from the cloud, and decrypted within the collector using that collector's private key. The password is used in memory and cleared without ever being stored to disk. A collector can only request access to the credentials necessary for the event sources configured on that collector.

InsightVM Console

The InsightVM security console, the on-premises component of InsightVM, stores encrypted credentials used for authenticated scanning unless the user utilizes a credential management system that the InsightVM console can integrate with (e.g. CyberArk). InsightVM does not store scan credentials in the Insight cloud.

Orchestrators

The Insight Orchestrator protects credentials similarly to collectors. As part of registration with the cloud, orchestrators generate RSA 4096-bit private and public keys. Only the public key is uploaded to the cloud, while the private key is stored locally on the orchestrator. When added, credentials are encrypted using the orchestator's public key. The Insight cloud will transmit-as-needed the encrypted credentials to the Insight Orchestrator, where they can be decrypted using the orchestrator's private key and used to communicate with third party integrations in a secure manner.

Orchestrators only utilize credentials specifically encrypted for them, and are only issued encrypted credential data that is relevant to the current set of tasks.

Cloud Collection and Integration

Credentials used for cloud based data collection or cloud based integrations are securely stored within the Insight cloud. Credentials are encrypted using AWS Key Management Service (KMS) and the ciphertext is stored in the Insight platform. Credentials are decrypted using KMS when needed and the cleartext is temporarily stored in memory, never written to disk.

For example, the Insight cloud stores credentials to enable:

- Integrations with JIRA, ServiceNow, and Slack
- Container downloads from container registries
- Website scanning using InsightAppSec direct collection

Data Processing and Storage

Rapid7's commitment to helping security and technology practitioners reduce risk requires us to collect and process an enormous amount of data. The Insight cloud's analytics engine relies on various NoSQL and relational databases, as well as S3 and other AWS services to process and store your data.

Geographic Location

The Insight cloud offers different regions for storage to help you comply with policies or preferences for the physical storage location of your data. Customers can select from five cloud regions. Rapid7 will not move data from the region you select, and data is not replicated across other regions.*

- United States
- Canada
- Europe – Germany and Ireland
- Japan
- Australia

*Log search data for InsightIDR customers provisioned before September 2017 is stored in Europe.

Encryption at Rest

All data processed and stored is encrypted at rest using various file or disk level encryption mechanisms.* Data is encrypted using industry standard AES-256 encryption with keys managed through AWS's Key Management Service (KMS). Where possible, Rapid7 utilizes AWS's services to manage encryption at rest (e.g. S3, EBS, RDS, etc.). When not possible, Rapid7 utilizes block level encryption provided by LUKS. All data is protected by strict access controls.

*Some raw InsightIDR data ingested before July 2018 and stored in S3 is not encrypted at rest. This data is protected by strict IAM access controls.

Encryption in Transit

Data sent to and from the Insight cloud—including data collected by collectors, agents, and engines; data ingested via APIs and plugins*; and interaction with the user interface —is encrypted with TLS (HTTPS). Collectors, agents, engines, and plugins are configured to verify and require a valid TLS certificate issued by a trusted certificate authority.

*InsightOps libraries allows you to send data encrypted with TLS, but you can also send log data over unencrypted connections to support legacy connections.

Data Separation

To offer you horizontally scalable solutions without any risk of one customer accessing another's data, Rapid7 designed the Insight cloud around secure, multi-tenant services from its inception. Each organization is assigned its own relational database schema within database instances. Data stored in object stores or distributed file systems is tokenized using a unique UUID that logically separates each customer's data from each other.

Data Reliability

The Insight cloud is composed of a collection of disparate server types that host a set of services that enable Rapid7 products. Each service is designed to scale horizontally. Each layer of the data collection and processing pipeline is designed to be fault-tolerant and to continue to operate in the event of reliability issues with our cloud environment. If one component of the Insight cloud is unavailable, other components will store data until the component is available again. All persisted data is stored redundantly so that the loss of a single server or an entire availability zone should not result in data loss. All infrastructure is monitored for performance, availability, and reliability. Operations staff are available 24/7 to respond to incidents.

In addition to a redundant and fault-tolerant architecture, customer data is backed up in a variety of ways. Rapid7 relies on Amazon S3 for storing data backups. Backups are not replicated outside of the region customers selected when creating their Insight account, but data is replicated across multiple data centers within the region. S3 can withstand the concurrent loss of data in two different facilities. Artifacts from critical stages of the data processing pipeline are backed up as data is processed. Log data backup occurs in real time as it is ingested. Automatic database backups occur daily.

Data Destruction

If you opt to leave a Rapid7 service, you'll have the opportunity to collect and transfer any data that is possible to export.* Should you request deletion of the data, the Rapid7 team will initiate the process within 14 days. When a user is using multiple Rapid7 products and leaves or cancels a product which makes use of shared data, the shared data is not deleted if any other shared data products are still enabled for that user's account. Rapid7's data retention policy and standard define the maintenance and retention of data in compliance with applicable governmental and regulatory requirements and industry best practices.

*Data export tools exist for InsightVM and InsightOps.

Physical Security

AWS Data Centers

Data is stored in AWS data centers located inside nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors, and all physical access by employees is logged and audited routinely. When an employee no longer has a business need for these privileges, their access is immediately revoked, even if they continue to be an employee of Amazon. Datacenter access and information is only provided to employees and contractors who have a legitimate business need for such privileges. All visitors and contractors are required to present identification and are signed in and continuously escorted by staff. More information can be found here: aws.amazon.com/compliance/data-center/controls.

Rapid7 Offices

There are various risk-mitigating physical and logical security controls in place, such as security guards at front desks or locked office entrances controlled by electronic badge access. Other controls include automatic screen locking, full-drive encryption on laptops, and a clean desk policy. All visitors must check in first when they enter Rapid7 facilities and must be escorted when entering sensitive areas.

Access to Data

Ensuring your data is used only in a manner consistent with your expectations is a responsibility Rapid7 takes very seriously. For this reason, policies including two-factor authentication, jump hosts, service segregation, and per-service permissions ensuring least-privilege access methodologies are applied.

Data Types

Rapid7 may collect certain types of data to help us improve our solutions and services. We have defined rules for what, when, and how we use this data.

Security System Data

This data is collected to deliver the Insight cloud platform. The elements collected vary by product and include data such as user, network, vulnerability, incident, asset, and log data. This data resides on the Insight cloud and is what populates the dashboards and products you use. Rapid7 will never sell, rent, or trade your Security System Data.

Usability Data

In order to provide our solutions and services to you, we must collect certain usage data. This helps us ensure that our solutions and services are operating correctly and that you are having the best possible experience with our products. The types of Usability Data we collect include:

- Device and connection data (e.g. browser type, operating system version, network speed)
- User and system behavior (e.g. commonly used features, user activity, configuration process)
- Product logs (e.g. web server, java, and Rapid7 generated logs for troubleshooting)
- Organizational data (e.g. customer industry, location, number of users)
- Other relevant machine data

We collect data about the solutions you use and how you use them, such as how often you access our products and which features you use most frequently. This is done in an effort to improve your experience with our solutions. For example, we may use this data to highlight additional capabilities or offer tips relating to features you are already using, to make our solutions more intuitive, or to enhance the solution's most popular features. The Usability Data collected never includes Security System Data such as user, network, vulnerability, incident, or asset data.

Who from Rapid7 can access your data?

- Sales, Marketing, and other customer support teams have access to contact information, sales data, and Usability Data for product support and product analytics.
- Sales and Solution Engineers only have access to your Security System Data if you choose to use a production environment for a proof-of-concept.
- Support, Software Developers, and Operations Engineers have limited access to data to support application development and troubleshooting. Rapid7 collects Usability Data to help us improve our solutions and services and Security System Data to deliver the Insight cloud.

Access Control

Rapid7 provisions all network and application access using the principle of least privilege. All access requests are documented and approved by system owners. Reviews of Insight cloud production access are conducted quarterly by the Cloud Operations team to ensure the level of access is commensurate with least-privilege required to perform job responsibilities.

Additionally, Rapid7 requires two-factor authentication for remote management access to our jump hosts and our backend production systems and environments. In accordance with NIST recommendations, Rapid7 explicitly disallows SMS and phone call-based two-factor authentication for remote management. This two-factor authentication includes multiple factors at each step (e.g., connection to jump host AND connection to backend servers). VPN or direct corporate LAN access is required before connecting to jump hosts, and a valid jump host session is required before connecting to any production infrastructure.

Application Security

Rapid7 products on the Insight cloud are designed to fit securely into your environment and adhere to security best practices. Rapid7 takes several steps to protect against common attack vectors and regularly performs application security testing, vulnerability scanning, and penetration testing.

Single Sign-On

Products that authenticate via the Insight cloud share the same user database and authentication mechanisms. Customers who use multiple Insight products benefit from the Insight cloud's single sign-on (SSO) functionality, needing only to sign in to the Insight cloud platform once to access all of their Insight products. Additionally, customers can customize some aspects of their user account authentication policies, such as multi-factor authentication prompt settings. User account credentials for the Insight cloud are hashed using Bcrypt with a high number of iterations to protect the credential.

Web application sessions are maintained via a randomly generated session ID that is at least 128-bits in length. Sessions are protected against session fixation by assigning a new session ID when authenticating. Sessions IDs are exchanged via HTTP cookies. Session Cookies have the "Secure" and "HttpOnly" attributes set, ensuring session IDs are only transmitted over HTTPS and preventing client-side scripts from accessing the cookie. Sessions expire after 30 minutes of inactivity.

Customers with on-premises InsightVM consoles authenticate to the Software-as-a-Service (SaaS) portion of InsightVM via their console. The InsightVM console supports local authentication, LDAP, Active Directory, SAML, and Kerberos authentication. Local two-factor authentication can be enabled as well. User account credentials used for local authentication to the security console are salted and hashed, with RSA being employed as part of the hashing process.

Role Based Access Control (RBAC)

The Insight cloud supports global roles that apply to all products* on the Insight cloud platform, and specific roles applicable to specific products. Rapid7 is always working to add new roles and permissions to our products, including the ability to customize RBAC for your needs.

Global Roles:

- **Platform Admin:** Full control over all products. Platform admins have full access to user management, including adding and deleting users, viewing all data, and performing all functions. This role can also manage product trials.
- **Product Admin:** Full control over a single product. Product admins can view all data, perform all edit functions, and access any admin functions within their product.
- **Product Read/Write User:** Able to access all or most features within a product except for administration of users and some settings. Able to modify data and/or some settings.
- **Product Read-Only User:** Able to access some features within a product with read-only access.

*RBAC for InsightVM is controlled via the on-premises InsightVM console. InsightVM uses customizable fine grained roles and permissions that differ from the global roles above.

Distributed Denial of Service (DDoS) Attacks

AWS network infrastructure leverages proprietary DDoS mitigation techniques developed as a result of running the world's largest online retailer and providing cloud infrastructure for many large enterprises and governments. Additionally, AWS's networks are multi-homed across a number of Internet service providers to achieve Internet access diversity. Insight cloud services scale horizontally behind load balancers to further mitigate DDoS attacks.

Man-in-the-Middle (MITM) Attacks

By default, all communication with Rapid7's cloud instances occur over authenticated channels.* HTTPS traffic is secured with TLS and authenticated using trusted Certificate Authorities to prevent MITM attacks.

*InsightOps libraries allow you to send data encrypted with TLS, but you can also send log data over unencrypted connections to support legacy connections.

IP Spoofing

Amazon EC2 VMs running the Rapid7 service cannot send spoofed network traffic. The AWS controlled, host-based firewall infrastructure does not permit an instance to send traffic with a source IP or MAC address other than its own.

Cloud Security Architecture and Governance

In addition to designing security into each layer of our products, Rapid7 also builds security into every aspect of our architecture that hosts the Insight cloud. Misconfiguration of cloud infrastructure continues to be a leading attack vector against SaaS companies. This section describes how Rapid7 implements, validates, and monitors the cloud security architecture to minimize this risk.

Least Privileged Design

The principle of least privilege and separation of duties is built into every layer of our cloud infrastructure:

AWS account separation and access: The Insight cloud uses a microservice architecture consisting of several small services working together. These services are logically separated into several different AWS accounts to minimize the blast radius of security incidents. Each AWS account contains a grouping of related services that provide a single product or product feature. Developer and operations employees are granted least privilege access to each AWS account individually as needed to perform their jobs. Employees access AWS consoles and APIs via Rapid7's corporate SSO system, which requires two-factor authentication. VPC networks are not peered across accounts. Cross-account communication is permitted where needed using least-privilege IAM roles or authenticated REST services. No direct database access is allowed between accounts.

Subnet separation: Several different network subnets exist within a single account. Services are provisioned to the appropriate subnet for their purpose. For example, databases are placed in a subnet with no route to the Internet to mitigate the risk of data exfiltration.

Host-level firewalls: Each set of identical Insight cloud services are assigned to a separate security group, which acts as an independent firewall for that service. Security groups deny network traffic by default, so all network traffic rules are whitelist-based and are defined to allow services to communicate with each other using only the specific ports and protocols necessary for them to function together. This mitigates the risk of lateral movement between instances comprising each Insight cloud service.

Service-level roles: When Insight cloud services need to access AWS services, (e.g. S3, KMS, SNS/SQS, etc.), their access is permitted via IAM roles attached to each group of identical services. Credentials for these roles are managed by AWS and regularly rotated. These roles allow least privileged access to cloud resources. Each service type has its own IAM role. For example, if a microservice needs access to read from S3, its IAM role would only permit reading from a specific S3 bucket. No write access would be permitted.

Scoped external access: IAM roles are used to access AWS resources where possible. When IAM keys must be used, different keys with least privilege access are issued for different tasks.

No direct access: Access to internal services is guarded by user authentication, IP address whitelisting, and two-factor authentication. Internal services such as jump hosts and back-office admin portals can only be accessed from the Rapid7 corporate LAN or VPN. Admin SSH access to backend services, databases, and other infrastructure must transit through a jump host.

Centralized logging: We store and retain logs centrally for security, compliance, and operational needs. These centralized logs cannot be altered after they have been submitted to our logging system.

Change Management

Software

Rapid7 applies a systematic approach to managing change so that changes to customer-impacting services are reviewed, tested, approved, and well communicated.

Change management processes are based on Rapid7 change management guidelines and tailored to the specifics of the Insight cloud.

The goal of Rapid7's change management process is to permit no unintended service disruptions and to maintain the integrity of services provided to customers. All code is version controlled for accountability on who did what, when, and where.

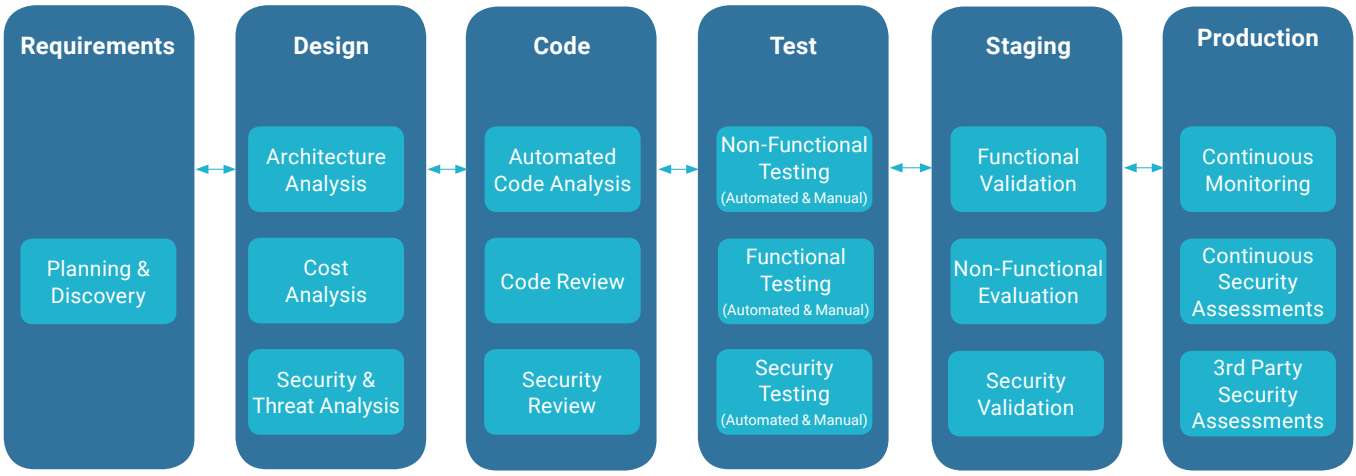
Prior to being deployed in production environments, new changes are:

- **Reviewed:** Peer reviews of the technical aspects of a change are performed to proactively catch and correct code errors;
- **Tested:** Changes are applied in testing environments to ensure they perform as expected and do not adversely impact performance; and
- **Approved:** Oversight is provided to ensure changes are prioritized and agreed upon.

Changes are typically moved into production in a phased automated deployment. Rollback procedures are available in order to revert to a previous version if any failures occur.

Emergency changes to production systems that require deviations from standard change management procedures are associated with an incident and are logged and approved as appropriate.

Rapid7's Engineering teams follow a formally documented Software Development Life Cycle process which is based on Agile and Scrum methodologies. This process includes peer code review, automated testing, and scenario testing to ensure quality and to identify security vulnerabilities prior to shipping.



Infrastructure

The Insight cloud relies on public cloud providers such as AWS to provide infrastructure services. The Cloud Operations team has configuration, deployment, and change responsibilities for the infrastructure of Insight cloud customers and the Insight platform Engineering team.

Rapid7's Cloud Operations team manages the operational development. The Cloud Operations team develops tools, which automate and validate that proper configurations and software are installed in a standard manner, based on host classes, and updated regularly.

Changes to cloud infrastructure are orchestrated in code and all changes are version controlled. When making an infrastructure configuration change, these tools provide a view of what will change and a mechanism to rollback if a problem occurs. Infrastructure is regularly monitored for manual changes made outside of these tools. In the event infrastructure is changed outside of code, it can quickly be brought back in compliance.

Changes deployed into production environments are:

- **Reviewed:** Peer reviews of the technical aspects of a change.
- **Tested:** To ensure that a change will behave as expected and not adversely impact performance. Rapid7 rolls out to its own systems first for quality assurance.
- **Approved:** Oversight is provided to ensure changes are prioritized and agreed upon.

Emergency, non-routine, and other configuration changes to existing Insight cloud infrastructure are authorized, logged, tested, approved, and documented in accordance with industry best practices for similar systems.

Updates to Rapid7's infrastructure are done in such a manner that in the vast majority of cases they will not impact the customer and their service use.

Rapid7 communicates with customers directly via email if service use may be adversely affected. Rapid7 also communicates operational status of the Insight cloud via status.rapid7.com.

Configuration Scanning

Rapid7 performs regular automated scans of our cloud infrastructure with a suite of tools to ensure our policies and best practices are in place. If a misconfiguration is found, operations engineers are alerted immediately so they can diagnose and fix the problem.

Rapid7 scans for several rules including appropriate controls from compliance benchmarks such as CIS AWS Foundations and AWS Well-Architected Framework. Some notable examples of checks scanned for are listed below:

- **Publicly accessible S3 buckets:** S3 buckets are scanned to ensure buckets aren't publicly accessible (readable or writable). Bucket Access Control Lists (ACLs) and bucket policies are evaluated. While some buckets (such as website assets, public downloads, etc.) are designed to be public, no other S3 buckets are ever permitted to be publicly readable or writable.
- **Publicly accessible resources:** Internal servers, databases, and other resources should never be accessible to the Internet. Security groups are scanned to ensure ingress from 0.0.0.0/0 is only allowed on appropriate resources and only for specific ports.
- **IAM keys:** IAM keys are scanned for age, recent access, and attached policies. Newly issued keys are reviewed. IAM policies associated with IAM keys used by third-party services are checked against approved policies. Old keys are removed when they are no longer needed.

Traceability

Rapid7 ensures cloud actions are logged and monitored. All AWS API actions are logged. Access to servers and services are logged to external systems to prevent tampering. Logs are analyzed by Rapid7's own products (InsightIDR and InsightOps) for notable events. Rapid7's Managed Detection & Response services team works with our internal Security Operations team to monitor these events 24/7 and investigate any alerts.

Compliance

Rapid7 SOC Reports

Rapid7 can provide a SOC 2 Type II report covering InsightIDR, InsightOps, InsightVM, InsightConnect, and InsightAppSec under NDA. This report is a representation of Rapid7's overall security posture and controls.

AWS SOC Reports

The Insight cloud is hosted by AWS. You can retrieve AWS compliance reports (SOC 2, SOC 3, FedRAMP Partner Package, ISO 27001:2013 SoA etc.) here: aws.amazon.com/artifact.

Third-Party Penetration Test

External penetration tests are conducted on an annual basis by a third party. Rapid7 can provide letters of attestation from the external firm summarizing the number and risk rating of findings. All findings are addressed in accordance with Rapid7's formally documented Vulnerability Handling and Disclosure Standard Operating Procedure. To avoid potential service disruptions, Rapid7 does not allow any customer, user, or individual to penetration test our products or services without written consent.

Vulnerability Handling and Disclosure

As a provider of security software, services, and research, Rapid7 is committed to addressing security issues that are found in our products and systems. Rapid7 has a defined standard operating procedure for responsible handling and disclosure of vulnerabilities that are reported. In the case that a vulnerability is reported to us, Rapid7 will work with the reporter to triage and fix the vulnerability in a timely fashion. Rapid7 will also provide public acknowledgement and attribution to any reporters who request it. Additional information about this process can be found here: www.rapid7.com/security/disclosure.

GDPR

The EU's General Data Protection Regulation (GDPR) has imposed obligations regarding the processing, storage, or transmission of personal data of individuals residing in the European Union (EU). Rapid7 has a Data Protection Officer, and has implemented controls across our organization so that we can better achieve and maintain compliance with this framework.

Rapid7 has a Data Processing Addendum which is incorporated into its standard contracts to comply with GDPR. You can find Rapid7's Data Processing Addendum at www.rapid7.com/legal/dpa. For more information about privacy at Rapid7 please visit: www.rapid7.com/privacy-policy.

Amazon Web Services (AWS) Security Competency

Rapid7 has achieved Amazon Web Services (AWS) Security Competency, which differentiates Rapid7 as an AWS Partner Network (APN) member that offers specialized software designed to help organizations adopt, develop and deploy complex security projects on AWS. To receive the designation, APN partners must possess deep AWS expertise and deliver solutions seamlessly on AWS.

More information about Rapid7 compliance and security frameworks can be found at https://www.rapid7.com/trust.

About Rapid7

Rapid7 (Nasdaq: RPD) is advancing security with visibility, analytics, and automation delivered through our Insight cloud. Our solutions simplify the complex, allowing security teams to work more effectively with IT and development to reduce vulnerabilities, monitor for malicious behavior, investigate and shut down attacks, and automate routine tasks. 7,800 customers rely on Rapid7 technology, services, and research to improve security outcomes and securely advance their organizations. For more information, visit our website, check out our blog, or follow us on Twitter.