RAPID7

WHITEPAPER

Information Security

| Q4 2020

TABLE OF CONTENTS

Overview

Rapid7 is on a mission to help organizations reduce risk across their entire connected environment through the visibility, analytics, and automation offered through the Insight cloud. Rapid7 has policies and procedures in place to keep our data and products secure so that we can continue providing solutions that keep our customers secure.

Compliance

Rapid7 SOC Reports

Rapid7 undergoes SOC 2 Type II audits annually to ensure the effectiveness of controls relevant to security. We can provide a SOC 2 Type II report covering the Insight cloud upon request. This report is a representation of Rapid7's overall security posture and controls.

AWS SOC Reports

The Insight cloud is hosted by Amazon Web Services (AWS). All AWS compliance and audit reports—including SOC 2, SOC 3, FedRAMP Partner Package, ISO 27001:2013 Statement of Applicability, and more—are easily accessible from the AWS Artifact portal. To retrieve these documents, perform the following steps:

1. Navigate to aws.amazon.com/artifact.
2. Sign in or create an AWS account.
3. Select Get this Artifact. You may be required to review the AWS Artifact NDA prior to downloading, based on the sensitivity of the report.

Third-Party Penetration Tests

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 handled 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. However, as a provider of security software, services, and research, we are committed to addressing security issues that are found in our products and systems. Such issues can be reported to us through Rapid7's coordinated vulnerability disclosure process outlined here: 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 rapid7.com/legal/dpa. For more information about privacy at Rapid7 please visit: rapid7.com/privacy-policy.

Organizational

Information Security Team Structure

The Information Security department consists of three teams: Trust & Security Governance, Security Operations & Engineering, and Product & Platform Security. The Trust & Security Governance team is responsible for governance, risk, compliance, and trust activities; security training; and overall security program management. The Security Operations & Engineering team is responsible for vulnerability management, incident detection and response, and dynamic application security testing, among other security operations responsibilities. The Product & Platform Security team ensures security is built into our products by providing security requirements, code analysis, and infrastructure configuration monitoring throughout multiple stages of our software development lifecycle.

Privacy

Ensuring your data is used only in a manner consistent with your expectations is a responsibility we take very seriously. We back our privacy guidelines with layers of security to safeguard your data. Please visit rapid7.com/privacy-policy to view our privacy policy.

Security Policies

The Information Security team distributes relevant policies internally upon hire, including Rapid7's Acceptable Use Policy, which addresses the following standards: Asset Usage, Data Protection, Secure Access, Software Usage, Monitoring, Loss and Theft, and Physical and Computer Security. The Information Security and Information Technology groups are responsible for monitoring compliance with data security policies and procedures. Users found in violation of information security policies may be subject to disciplinary action, up to and including termination of employment and legal action. When required, Information Security will work with Legal and People Strategy to address any instance of noncompliance.

Security Awareness Training

Security awareness training is completed by all employees at least annually. The training is offered as an interactive video course developed in-house to train employees on Rapid7 security principles and policies, as well as industry best practices and common pitfalls. The Information Security team also performs real-time training (e.g. phishing drills) across the entire company on a regular basis, and distributes company-wide security alerts on an as-needed basis as new risks and threats arise.

Background Checks

All employees undergo a background check prior to being hired. This includes reference checks, education verification, and a criminal background check against addresses, names, and Social Security Numbers. Finance hires also undergo a credit check.

We have a Code of Business Conduct and Ethics, or a Code of Conduct, that is acknowledged by all Rapid7 employees. The Audit Committee of our Board of Directors is responsible for overseeing the Code of Conduct, and any waivers of the Code of Conduct must be approved by our Board of Directors.

Infrastructure & Endpoint Security

Cloud Security

Rapid7 monitors our AWS accounts for cloud infrastructure security risks, such as public S3 buckets, IAM keys, and insecure Security Groups. The Insight Agent is installed across our production cloud environment, allowing Rapid7 to monitor for anomalous platform events and respond accordingly. Information Security works closely with Cloud Delivery and Information Technology to remediate or mitigate any cloud infrastructure configuration risks that are found in our AWS environments.

Encryption

All Rapid7-issued laptops have full-drive encryption enabled on them and are continuously monitored to ensure full compliance.

Rapid7 uses a secure file transfer server, which we host in our own data centers. Customers and employees can use this server for transmitting sensitive data. All data sent through our secure file transfer server is encrypted in transit and at rest.

Passwords

Rapid7 passwords must be at least 12 characters and contain a number, a symbol, an uppercase character, and a lowercase character. Passwords cannot contain the user's name, "Rapid7," "Password," be a reused password, or have more than two repeating characters.

Password-protected screen savers are required and set to engage after, at most, fifteen minutes of inactivity, or whenever a user leaves a computer unattended. After five failed login attempts, user accounts are locked out for 30 minutes or until released by an admin.

As a matter of policy, employees are not permitted to share their user account passwords with anyone. Regular phishing drills provide employees with learning opportunities for upholding this policy.

A secure password management solution is provided to all employees to securely store credentials. Service account credentials and other types of shared credentials are also stored in a secure password management tool.

Network Security

All Rapid7 wireless networks are secured with WPA2. All wireless networks are segmented from corporate wired networks and production networks. Peer-to-peer blocking is enabled to protect wireless network clients.

Network and host-based firewalls are in place across production environments. On production networks, firewalls deny access to all connections which are not explicitly allowed. For on-premise networks, different internal environments are logically segmented from each other with firewall rules. For cloud virtual private networks (VPCs), different environments are logically segmented from each other using a combination of separate AWS accounts, separate VPCs, and cloud firewall rules (e.g. Security Group rules).

Intrusion Detection and Prevention

Rapid7 deploys host- and network-based IPS/IDS tooling in parallel with audit trails, log monitoring, and metrics to identify and detect malicious activity or intrusions across systems and environments. We follow formal processes to track modifications to our systems, such as firewall configuration, and regularly perform internal and external network scans to monitor for unauthorized changes.

Data Loss Prevention

Data loss prevention controls are in place across the organization to ensure the safety of customer data. All production assets on the Insight cloud are monitored for data loss events and anomalous network activity. The use of USB devices is prohibited by policy and read-only access is technically enforced.

Antivirus and Anti-malware

A next-generation anti-malware solution is in place to address the most relevant malicious software threats to Rapid7. Anti-malware agents installed on Windows and Mac Rapid7 workstations are configured to check for and install updates on a daily basis. Security Operations Analysts are alerted when anti-malware agents detect and take action on malware. Anti-malware agents are centrally managed, and their policies are regularly tuned by Information Security.

Identity and Access Management

Rapid7 provisions all network and application access using the principle of least privilege. Key administrative access is limited to appropriate personnel only. Service accounts are used sparingly and only for defined business needs.

Access reviews for SOX applications are completed quarterly. Rapid7's Cloud Operations team conducts a quarterly review of Insight cloud production access to ensure the level of access is commensurate with least-privilege required to perform job responsibilities. For all other application, system, and physical access reviews are completed at varying intervals based on risk.

For all terminations, access is removed on employee's last day.

Authentication

Two-factor authentication (2FA) is used throughout our environments. Rapid7's Insight cloud and corporate IT production environments require 2FA to access production infrastructure systems. We allow YubiKeys, app-generated passcodes, and push-notifications as authentication factors. SMS and phone call-based 2FA are explicitly disallowed.

VPN or direct corporate LAN access is required to connect to production systems.

Rapid7 uses Okta as our single sign-on provider for all business applications that support SAML. This allows us to enforce Rapid7's password policy for all of our business applications and 2FA when logging into Okta and Okta-managed applications.

Physical Security

Rapid7 Offices

There are various risk-mitigating physical and logical security controls in place at all Rapid7 offices, 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 when they enter Rapid7 facilities and must be escorted when entering sensitive areas.

Physical access to restricted spaces at Rapid7, such as our Managed Detection and Response Security Operations Centers (SOCs), requires additional authentication. Electronic badge and PIN code must be provided to gain access.

AWS

Physical access to all AWS data centers, colocations, and facilities housing IT infrastructure components is restricted to authorized data center employees, vendors, and contractors who require access in order to execute their jobs. AWS utilizes multi-factor authentication mechanisms for data center access, as well as additional security mechanisms to ensure that only authorized individuals enter an AWS data center. A more detailed description of AWS data center controls can be found here: aws.amazon.com/compliance/data-center/data-centers

Security Operations

Vulnerability Management

Information Security continuously monitors Rapid7's corporate IT and Insight cloud environments for system vulnerabilities in accordance with formally documented vulnerability management processes and procedures. Information Security conducts network and agent-based vulnerability scans of these environments on a continuous basis using InsightVM, with new vulnerability results coming in daily or weekly. Information Security partners with Rapid7's Managed Vulnerability Management team to augment our vulnerability management processes.

Rapid7 also utilizes InsightAppSec and Information Security partners with Rapid7's Managed AppSec team to monitor the Insight platform and Rapid7 web properties for web application vulnerabilities.

Scanning & Patching

Information Security actively monitors patching compliance using InsightVM. Security patches are deployed on a regular basis by Information Technology for corporate IT systems, and by Cloud Operations for Insight cloud infrastructure. Out-of-band patching is performed for all vulnerabilities, including critical vulnerabilities, in accordance with our Vulnerability Handling & Disclosure Standard Operating Procedure.

Vulnerability Handling & Disclosure

When a vulnerability is identified and reported to the Information Security team, either by an internal or external party, we follow our Vulnerability Handling and Disclosure Standard Operating Procedure to remediate issues in a timely fashion. Details about Rapid7's vulnerability disclosure program can be found here: rapid7.com/security/disclosure.

Penetration Testing

External penetration tests are conducted on an annual basis by a third party, and Rapid7 can provide letters of attestation under NDA. Internal penetration tests are conducted as needed or following a material change to a Rapid7 product in partnership with Rapid7's Penetration Testing Services team.

Change Management & Change Control

Rapid7 applies a systematic approach to managing change so that changes to services impacting Rapid7 and our customers are reviewed, tested, approved, and well communicated. Separate change management processes are in place for corporate IT systems and Insight cloud systems to ensure changes are tailored to the specifics of each environment. The goal of Rapid7's change management processes is to prevent unintended service and business disruptions and to maintain the integrity of services provided to customers. All changes deployed to production undergo a review, testing, and approval process.

Software Development Life Cycle (SDLC) Process

All Engineering teams follow a formally documented SDLC process that is based on Agile and Scrum methodologies. This process is in place to ensure quality and identify security vulnerabilities prior to releasing code into production environments. The Rapid7 SDLC includes mandatory code review, automated testing, and scenario testing. Types of test coverage may include functionality, compatibility, UI consistency, performance, security, integration, internationalization, and regression tests.

Segregation of Duties

Conflicting duties and areas of responsibilities are segregated to reduce opportunities for unauthorized or unintentional modification or misuse of Rapid7 assets.

Asset Management

We use a combination of InsightVM scans, agent data, and API integrations to inventory our servers, workstations, printers, network devices, cloud services, and other technology assets.

Incident Management

Incident Detection & Response

Rapid7 uses InsightIDR to monitor on-premises and cloud environments for security incidents. Information Security partners with the MDR and Incident Response services teams to augment Rapid7's incident response program. InsightIDR alerts are regularly reviewed by analysts and escalated via a paging system when indications of potentially malicious activity are detected.

Rapid7 maintains a formal Incident Response Policy and procedures in accordance with industry best practices and to meet numerous compliance requirements. This policy and supporting procedures document the process for analysis, containment, eradication, recovery, and follow up in the event of a security incident. Annual testing and refinement of this policy and procedures is required to help prepare for adverse security incidents and to manage and minimize risk.

Rapid7 will notify customers of any breaches affecting their data within 72 hours. For any other breaches, Rapid7 will follow internal policy and all applicable federal, state, and local laws.

Business Continuity

Rapid7 maintains a Business Continuity and Disaster Recovery Plan for the Insight cloud. The primary goal of this plan is to ensure organizational stability, as well as coordinate recovery of critical business functions, in the event of disruption or disaster. Thus, the plan accomplishes the following:

- Ensures critical functions can continue during and after a disaster with minimal interruption;
- Identifies and decreases potential threats and exposures; and
- Promotes awareness of critical interdependencies.

We can share a high-level overview of our Business Continuity and Disaster Recovery Plan and Test Overview for the Insight cloud upon request.

Rapid7 Risk Management

Risk Management Program

Rapid7 maintains an Information Security Risk Management (ISRM) program in order to identify information security risks, assess these risks, and take steps to reduce risk to an acceptable level. Formal risk assessments are conducted annually. Risk owners are assigned for all risks. These risk owners are responsible for reviewing, approving, and coordinating risk treatment plans.

Vendor Security Assessments

All third-party vendors undergo a formal vendor security assessment by Rapid7's Information Security team. Rapid7 takes a risk-based approach to vendor security assessments to ensure all vendors meet our security, quality, and privacy standards.

For more information, please visit 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.