RAPID7 INFORMATION SECURITY

An Overview of Rapid7's Internal Security Practices and Procedures

060418

TABLE OF CONTENTS

OVERVIEW

Rapid7 is on a mission to drive the SecOps movement into the future, and we take that to heart with our holistic approach to security. Rapid7 has policies and procedures in place to keep our data and products secure, so that we can continue creating tools and services that keep our customers secure.

COMPLIANCE

Rapid7 SOC Reports

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

AWS SOC Reports

The Insight platform is hosted by AWS. All AWS compliance and audit reports, including SOC 2, SOC 3, FedRAMP Partner Package, ISO 27001:2013 SoA etc. are easily accessible. To retrieve these documents, you may complete the following steps:

1. Navigate to https://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 unless explicit written consent has been granted. 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: https://rapid7.com/security/disclosure/.

PCI

Rapid7 is SAQ (Self Assessment Questionnaire) compliant in alignment with our bank's PCI guidelines, and we can provide a PCI certificate.

GDPR

The EU's General Data Protection Regulation ("GDPR") went into effect on May 25, 2018. GDPR has imposed new 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 implemented controls across our organization so that we can better achieve and maintain compliance with this new framework.

Rapid7 has drafted a Data Processing Addendum to update customer contracts to comply with GDPR, and has incorporated this Addendum into its standard contracts. You can find Rapid7's Data Processing Addendum at https://www.rapid7.com/legal/dpa/.

For more information please visit https://rapid7.com/privacy.

ORGANIZATIONAL

Information Security Team Structure

Rapid7's Information Security department consists of three functions/teams: Trust & Security Governance, Security Operations, and Platform Security. The Trust & Security Governance function is responsible for governance, risk, compliance, and trust activities; security training; and overall security program management. The Security Operations function is responsible for vulnerability management, incident detection and response, and dynamic application security testing, among other security operational roles and responsibilities. The 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 https://www.rapid7.com/privacy-policy/ to view our privacy policy.

Security Policies

The Information Security team distributes relevant policies internally upon hire, including the Rapid7 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

Online security awareness training is completed by all employees at least annually. The training is an interactive video course developed in-house to communicate 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 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 SSNs. Finance hires also undergo a credit check.

Rapid7 has 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. Information Security works closely with the Platform Delivery and Information Technology teams 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, which are continuously monitored and enforced 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.

Where applicable, Rapid7 employs 3DES, AES, and/or FIPS 140-2 as acceptable encryption algorithms.

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 must be used and set to engage after, at most, fifteen minutes of inactivity, or whenever a user leaves a computer unattended. User IDs are locked out for 30 minutes or until released by admin after five failed login attempts. As a matter of policy, employees are not permitted to share passwords with anyone. Regular phishing drills provide employees with learning opportunities for upholding this policy.

A secure password vault solution is used for managing service account credentials and other types of shared credentials.

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-premises networks, different internal environments are logically segmented from each other with firewall rules. For virtual private cloud 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.

Antivirus and Antimalware

Rapid7 uses a next-generation anti-malware solution to address the most relevant malicious software threats.

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.

Access Control

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.

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

Access reviews for SOX applications are completed quarterly. For all other application, system, and physical access, reviews are completed at varying intervals, based on risk.

Authentication

Two-factor authentication (2FA) is used throughout our environments. Rapid7's Insight platform 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 is explicitly disallowed.

VPN or direct corporate LAN access is required to connect to production systems. Only Rapid7-issued workstations are permitted to access the VPN: this is enforced with device certificates.

Rapid7 uses Okta as our single sign-on provider for many of our business applications (whenever an application supports SAML). This allows us to enforce Rapid7's password policy for all of our business apps and 2FA when logging into Okta and Okta-managed applications.

2FA is also required for physical access to restricted spaces at Rapid7, such as our Managed Detection & Response Security Operations Centers, which require badge access and PIN codes.

PHYSICAL SECURITY

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, automatic screen locking, and full-drive encryption on laptops. All visitors must check in when they enter Rapid7 facilities and must be escorted when entering sensitive areas.

AWS

Physical access to all AWS data centers, collocations, 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.

SECURITY OPERATIONS

Scanning/Patching

Information Security actively monitors patching compliance using InsightVM. Security patches are deployed to workstations on a regular basis by Information Technology for corporate IT systems and by Platform Delivery for Insight platform infrastructure. Out-of-band patching is performed for critical vulnerabilities in accordance with our Critical Vulnerability Response Standard Operating Procedure.

Vulnerability Management

The Information Security team continuously monitors Rapid7's corporate IT and Insight platform 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 Insight platform and Rapid7 web properties for web application vulnerabilities.

Vulnerability Handling & Disclosure

When a vulnerability is identified and reported to the Information Security team, either by an external security researcher or an internal employee, Rapid7 follows 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: https://www.rapid7.com/disclosure.jsp.

Penetration Testing

External penetration tests are conducted on an annual basis by a third party. Internal penetration tests are conducted as needed and 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 platform systems to ensure changes are tailored to the specifics of each environment. The goal of Rapid7's change management process is to prevent unintended service 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 which is based on Agile and Scrum methodologies. This process is in place to ensure quality and identify security vulnerabilities prior to putting code into production environments. The Rapid7 SDLC includes code review, automated testing, scenario testing, and penetration testing. Our test coverage includes 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 the misuse of our assets.

Asset Management

Rapid7 uses a combination of InsightVM scans, agent data, and API integrations to inventory our servers, workstations, printers, 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 process for analysis, containment, eradication, recovery, and follow up in the event of a security incident. Rapid7 will notify customers of any breaches affecting their data within 48 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 Plan for the Insight platform. The primary goal of this plan is to ensure organizational stability, as well as coordinate recovery of critical business functions in managing and supporting business recovery 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 Plan for the Insight platform upon request.

THIRD PARTY RISK MANAGEMENT

Vendor Security Assessments

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

ABOUT RAPID7

Rapid7 powers the practice of SecOps by delivering shared visibility, analytics, and automation that unites security, IT, and DevOps teams. The Rapid7 Insight platform empowers these teams to jointly manage and reduce risk, detect and contain attackers, and analyze and optimize operations. Rapid7 technology, services, and research drive vulnerability management, application security, incident detection and response (SIEM), orchestration and automation, and log management for organizations around the globe. To learn more about Rapid7 or join our threat research, visit www.rapid7.com.

Learn more about Rapid7's approach to data security:

www.rapid7.com/trust