RIVERBED APM

SECURITY MEASURES

These Security Measures describe the technical and organizational security measures implemented by Riverbed APM.

TABLE OF CONTENTS

riverbed

1. OVERVIEW

Riverbed APM is offered by Riverbed as both a SaaS and on-premise observability product to companies ("**Customer**") who acquire it for internal business use. Riverbed APM is designed to help organizations collect, process, and analyze application performance data. It provides insights into application behavior, user interactions, and system health to optimize performance and detect anomalies.

Simplified high-definition monitoring that is scalable, easy to use and deploy.

The Product includes the following capabilities:

- Analysis Server: The central APM component that stores and processes performance data generated by monitored web pages and agent systems. The analysis server also provides the web interface for users to analyze data it collects. It can be included as part of the APM virtual appliance, installed on a dedicated Linux system, or hosted in the cloud (SaaS).
- Agent: APM agent software is installed on monitored systems. It collects application data and environmental data.
- Riverbed K8s Operator: Provides a simple, cloud-native mechanism to deploy Riverbed APM instrumentation into a Kubernetes-managed cluster.

1.1. RIVERBED PLATFORM

Riverbed APM is a product that is built on the Riverbed Platform, which is based on the underlying infrastructure for Riverbed's Aternity EUEM SaaS product ("**Riverbed Platform**"). Except as otherwise noted in this document, all existing Riverbed Platform data processing requirements, including those related to security, privacy, and compliance, fully apply to data processed and stored within Riverbed APM. For more details about the Riverbed Platform, please refer to the security measures documentation for Aternity EUEM.

2. DEFINITIONS

The definitions below contain a series of terms that are used throughout this document. When encountering one of these capitalized terms, please refer to the definition below.

- "**Customer Data**" means all information and data provided by or on behalf of a Customer to Riverbed as part of Riverbed APM.
- "**Personal Data**" means any information related to an identified or identifiable natural person that is contained within the Customer Data.
- "**Personal Data Breach**" means a subtype of Security Incident involving Personal Data.
- "**REST API**" means the Riverbed APM API.
- "**Security Incident**" means a breach of Riverbed APM's security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Data on systems managed or otherwise controlled by Riverbed. "Security Incidents" will not include unsuccessful attempts or activities that do not compromise the security of Personal Data, including unsuccessful log-in attempts, pings, port scans, denial of service attacks, and other network attacks on firewalls or networked systems.
- "**Trust Center**" means the security and privacy related documentation applicable to Riverbed APM, as updated from time to time, and accessible via the Trust Center at https://www.riverbed.com/trust-center/ (or a successor website designated by Riverbed).

3. SECURITY ORGANIZATION & PROGRAM

Riverbed has a dedicated Information Security team that manages Riverbed's security program. The Information Security team is headed by Riverbed's Chief Information Security Officer ("**CISO**"). Riverbed's CISO meets with executive management regularly to discuss security-related matters and coordinate company-wide security initiatives. Riverbed's security program has a set of information security policies that have been approved by management, published, and communicated to relevant Riverbed personnel.

4. HUMAN RESOURCE SECURITY

4.1. Personnel Background Checks

Riverbed performs background checks on all new employees at the time of hire in accordance with applicable local laws. Riverbed currently verifies a new employee's education and previous employment and performs reference checks. Where permitted by applicable law, the scope may also include criminal, credit, immigration, and security checks depending on the nature and scope of a new employee's role.

4.2. Personnel Agreements

All Riverbed personnel are required to enter into employment agreements including provisions relating to acceptable use, code of conduct/ethics, and confidentiality.

4.3. Personnel Training

All Riverbed personnel must undergo annual security, data handling, and privacy training. Personnel in select roles are required to undergo additional role-specific security training.

5. SECURITY CERTIFICATIONS & ATTESTATIONS

The Riverbed Platform holds the following security-related certifications and attestations. Copies of such may be viewed or requested by visiting the Trust Center.

- ISO/IEC 27001
- SOC 2 Type II

6. CLOUD ARCHITECTURE & DATA SEGREGATION

6.1. Hosting Architecture

The Riverbed Platform leverages Amazon Web Service ("**AWS**")'s Infrastructure-as-a-Service ("**IaaS**") cloud service and Riverbed provides Riverbed APM to Customers using Virtual Private Cloud (VPC) and storage services provided by AWS ("**Cloud Environment**"). The Cloud Environment (including all hardware, virtualization, networking, and other supporting infrastructure) is owned, managed, and protected by the security and environmental controls of AWS. More information regarding such AWS controls is available at https://aws.amazon.com/compliance/.

6.2. Customer Data Storage

The Riverbed Platform manages the Customer Data storage for Riverbed APM.

6.3. Data Segregation

The Riverbed Platform manages the Customer Data segregation for Riverbed APM.

7. ENCRYPTION

7.1. Customer Data Encryption

The Riverbed Platform manages the Customer Data encryption for Riverbed APM.

7.2. Encryption Key Management

The Riverbed Platform manages and maintains encryption keys in accordance with key management industry standards using AWS Key Management Service, a platform-managed key service. Customer Data stored within the Cloud Environment is encrypted at all times.

8. ACCESS CONTROL

8.1. Access Provisioning

The Riverbed Platform defines and manages access provisioning for Customer Data for Riverbed APM, ensuring that access is restricted to authorized users and follows strict security protocols.

8.2. Password Controls

For Riverbed personnel, password requirements include a minimum password length of at least 12 characters, complexity (a combination of upper-case letters, lower-case letters, numbers and special characters), restrictions on password re-use, and passwords are rotated in accordance with NIST SP800-63-3 guidelines. Initial and temporary passwords must be random and complex and changed upon next

login. Riverbed personnel are trained and required to change passwords if there is any indication of a possible compromise of the password system. Passwords are encrypted in transit and encrypted and/or hashed when stored.

8.3. Multi-Factor Authentication

The Riverbed Platform defines and manages multi-factor authentication (MFA) for Riverbed APM, adding an extra layer of security by requiring users to provide multiple forms of verification to access Customer Data.

9. PHYSICAL & ENVIRONMENTAL SECURITY

9.1. Cloud Environment Data Centers

Riverbed regularly reviews the physical and environment controls for its data centers hosting the Cloud Environment as audited under the Cloud Environment provider's third-party audit and certifications. Riverbed requires that any third-party IaaS cloud service provider engaged by Riverbed to have a SOC 2 Type II annual audit and ISO 27001 certification, or equivalent industry-recognized accreditations and/or frameworks.

9.2. Riverbed Corporate Offices

While Customer Data is not hosted at Riverbed's corporate offices, the controls applicable to Riverbed's corporate offices include, but are not limited to, the following:

- Physical access to the corporate office is controlled;
- Badge access is required for all Riverbed personnel;
- Visitor sign-in is required;
- Use of CCTV at building ingress and egress points;
- Fire detection and sprinkler systems; and
- Climate control systems.

10. SYSTEM AND NETWORK SECURITY

10.1. Endpoint Controls

For access to the Cloud Environment, Riverbed personnel use Riverbed-issued laptops which utilize security controls that include, but are not limited to, (i) disk encryption, (ii) malware and antivirus monitoring and alerting, and (iii) vulnerability management. Endpoints are not used to store or process Customer Data and Riverbed APM does not send or receive Customer Data via physical media.

10.2. Asset Management

Riverbed maintains and periodically reviews an asset management program approved by management that is communicated to relevant Riverbed personnel; the asset management program includes an asset inventory list. A process is in place to verify the return of Riverbed personnel assets (e.g., laptops, access cards, tokens, etc.) upon termination. Riverbed personnel must return assets as soon as possible and access is revoked promptly upon termination.

10.3. Separation of Environments

Development, test and staging environments are separated from the production environment by either separate VPC, Availability Zone (data centers) or physical location. The Cloud Environment is both logically and physically separate from Riverbed's corporate offices and networks.

10.4. Monitoring & Logging

Infrastructure Logs. The Riverbed Platform defines and manages infrastructure logs, ensuring comprehensive logging of system activities and events via diagnostic and audit logs, which provides visibility into access, changes, and potential security incidents to enhance monitoring, auditing, and the overall security of Customer Data for this service.

User Logs. As further described in the documentation, the Riverbed Platform also captures logs of certain activities and changes within a Customer's account and makes those logs available to Customer.

10.5. Network Management

The Riverbed Platform defines and manages network management, utilizing the Cloud Environment's capabilities to ensure secure, controlled, and isolated communication channels for the protection and integrity of Customer Data for Riverbed APM.

11. APPLICATION DEVELOPMENT & CHANGE MANAGEMENT

11.1. Application Development

The Riverbed Platform and Riverbed APM utilize a formal Software Development Life Cycle ("**SDLC**") process that has been approved by management and communicated to appropriate Riverbed personnel. The Riverbed software engineering department is responsible for maintaining and reviewing the SDLC policy. The Riverbed Platform and Riverbed APM are evaluated from a security perspective prior to promotion to production, including: (i) security requirements gathering, (ii) security architecture review, (iii) security signoffs, (iv) secure code reviews, and (v) vulnerability scans.

11.2. Change Management

The Riverbed Platform and Riverbed APM maintain a documented change management / change control process that includes: (i) change control procedures required for all changes to the production environment, (ii) testing prior to deployment, (iii) stakeholder communication and/or approvals, (iv) documentation for all system changes, (v) version control for all software, (vi) logging of all change requests, (vii) backout procedures are required for production changes, and (viii) access to make changes to source code is restricted to select Riverbed personnel.

Riverbed uses reasonable efforts to notify Customers two (2) weeks' prior to scheduled maintenance; as of this document's publication date, scheduled maintenance is performed on a monthly basis on a weekend night between Saturday and Sunday (EST).

12. VULNERABILITY DETECTION & MANAGEMENT

12.1. Antivirus & Vulnerability Detection

The Cloud Environment leverages advanced threat detection tools, which are used to monitor and alert for suspicious activities, potential malware, viruses and/or malicious computer code. New anti-malware signature updates are deployed no later than twenty-four (24) hours after release. Vulnerability scans are performed on a daily basis.

12.2. Penetration Testing

On an annual basis, an independent consulting firm executes an application penetration test, a REST API penetration test and an external network penetration test against the in-scope Riverbed Platform and Riverbed APM assets. An executive summary of the Riverbed Platform and Riverbed APM penetration test may be requested via the Trust Center.

12.3. Vulnerability Management

Identified vulnerabilities are generally mitigated or remediated in accordance with the following timelines based on applicable risk: critical (45 days), high (60 days), and medium (120 days) after discovery and identification. Vulnerabilities classified as low priority are added to the product release roadmap.

13. SECURITY INCIDENT MANAGEMENT

13.1. Policies & Procedures

Riverbed APM has an established incident management program that has been approved by management and communicated to relevant Riverbed personnel. The incident management program leverages centralized incident management processes and Riverbed APM maintains a formal incident response plan, including guidance for: (i) feedback and lessons learned; (ii) applicable data breach notification requirements (including notification timing), (iii) escalation procedure, (iv) communication timelines and process, (v) procedures to collect and maintain a chain of custody for evidence during incident investigation, and (vi) actions to be taken in the event of a Security Incident. Testing of the Riverbed Platform and Riverbed APM incident response plan occurs at least annually and includes end-to-end testing, associated BCP / DR plans, and review of the test results by product management leadership and remediation if needed.

13.2. Security Incident Notification & Communication

Riverbed notifies Riverbed APM Customers of (a) Security Incidents as required by applicable law; and (b) Personal Data Breaches without undue delay. Notification(s) of any Security Incident(s) or Personal Data Breach(es) (as applicable) will be delivered to one or

more of the Customer's business, technical or administrative contacts by any means Riverbed selects, including via email. Riverbed will provide all such timely information and cooperation as a Customer may reasonably require in order for the Customer to fulfill its data breach reporting obligations under applicable data protection laws. Riverbed will take such measures and actions as it considers necessary to remedy or mitigate the effects of a Security Incident or Personal Data Breach and will keep respective Customers informed in connection with such Security Incident or Personal Data Breach.

14. VENDOR RISK MANAGEMENT

When engaging third-party providers of products and services ("**Vendors**") Riverbed requires non-disclosure agreements be in place with any potential Vendor before engaging in discussions regarding a potential business arrangement. Riverbed's procurement and legal teams review proposed Vendor engagements. For those Vendors that will have access to Riverbed's internal networks and/or will store, process, or transmit data, Riverbed assesses the security and privacy practices of such Vendors to ensure they provide a level of security and privacy appropriate to the data and scope of services they are engaged to deliver. Vendors are required to enter into appropriate security, confidentiality and privacy contract terms with Riverbed based on the risks presented by the Vendor assessment.

15. RESILIENCE & SERVICE CONTINUITY

15.1. Resilience

The Cloud Environment leveraged by the Riverbed Platform and Riverbed APM is designed to provide robust availability based on extensive redundancy achieved with virtualization technology and a globally distributed data center infrastructure.

15.2. BCP/DR

Riverbed APM has a business continuity plan ("**BCP**") and disaster recovery ("**DR**") plan. Riverbed APM conducts testing on a monthly basis to validate the ability to failover a production instance from the primary data center to the secondary data center utilizing Riverbed APM DR procedures. The BCP plan is validated on an annual basis.

15.3. Customer Data Backups

Customer Data is automatically replicated on a near real-time basis to a secondary database server ("**Cloned Database Server**") and backed-up to localized data stores. The Cloned Database Server is backed-up on a daily basis; back-ups are retained for a 1-week period.

The Riverbed Platform has the following recovery time objective ("**RTO**") and recovery point objective ("**RPO**"):

- RTO: The maximum RTO is twenty-four (24) hours; however, in most disaster scenarios, the Riverbed Platform is designed to meet an RTO of less than one (1) hour.
- RPO: The maximum targeted period for which Customer Data might be irrecoverably lost is twenty-four (24) hours.

16. APPLICATION SECURITY TOOLS FOR CUSTOMERS

16.1. Configurable Security Policies

Customers can configure organization-wide security policies for Riverbed APM user accounts to better protect access to Riverbed APM; configuration options include:

- Single sign on (SSO) / SAML integration including the ability to enforce multi-factor authentication;
- Role-based administration;
- Idle timeout;
- Granular access control ability (based on IP address filtering);
- Provisioning/deprovisioning process for the Customer's Riverbed APM user accounts;
- API management;
- Customized password policies, including forced periodic password change, minimum password length and complexity, user lockouts after repeated failed login attempts, and disallowed password reuse;
- For native authentication (when SAML 2.0-based Single Sign-On is not utilized), the Riverbed Platform and Riverbed APM encrypt passwords in transit and in storage; and
- Encrypted communications are required for all remote connections.

16.2. Audit Logs

The following user log audit data is accessible to Customers via the REST API: (i) Riverbed APM user account log-ins, (ii) configuration changes, (iii) dashboard views, and (iv) API access.

16.3. Session IDs

Riverbed APM generates session IDs automatically/randomly; session IDs are in-memory only and are not stored. Session IDs are sent only over encrypted connections and rotated after successful login. Riverbed APM disconnects the sessions when the user terminates the session. Riverbed APM automatically terminates a Customer session and logs out if the Customer session has been idle for more than 30 minutes.

Customers may visit the Trust Center to obtain additional information regarding privacy, compliance and reliability in connection with APM.