riverbed

ATERNITY MOBILE CLOUD SERVICE
SECURITY MEASURES

These Security Measures describe the technical and organizational security measures implemented by the Aternity Mobile cloud service.

Table of Contents

1. OVERVIEW

The Aternity Mobile cloud service is a cloud-based enterprise-grade Software-as-a-Service ("**SaaS**") digital experience management platform providing a comprehensive view of mobile app and device performance across employee mobile devices by capturing and storing technical telemetry data at scale (hereinafter referred to as "**Aternity Mobile SaaS**") made available by Riverbed to companies ("**Customer**") who acquire it for internal business use.

1.1. Aternity Mobile SaaS Platform Capabilities

- Empower the digital experience and drive enterprise performance for all device types and provide Unified Observability that transforms data into actionable insights across the entire digital ecosystem for a seamless digital experience.
- Provide visibility and take actions on mobile devices issues in a similar way to laptops and desktop from a single unified platform.
- Proactively detect and solve incidents, engage with employees on their mobile, and create executive level dashboards for mobile IT service.

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.

- "**Aternity Mobile Agent"** which is a piece of software that a Customer installs on an application or device that transmits Customer Data to the Aternity Mobile SaaS platform.
- "**Cloud Service Provider**" means the third party cloud service provider(s) providing infrastructure as a service for the Aternity Mobile SaaS platform as identified in Riverbed's subprocessor list.
- "**Customer Data**" means all information and data provided by or on behalf of a customer to Riverbed as part of Aternity Mobile SaaS.
- "**End User Devices**" means Customer-managed desktops, laptops, tablets, and smartphones that have an Aternity Mobile module and the Aternity Mobile Agent installed on them.
- "**Personal Data Breach**" means a subtype of Security Incident involving Personal Data.
- "**Personal Data**" means any information related to an identified or identifiable natural person that is contained within Customer Data.
- "**REST API**" means the Aternity Mobile SaaS cloud API.
- "**Security Incident**" means a breach of Aternity Mobile SaaS'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 Aternity Mobile SaaS, as updated from time to time, and accessible via the Trust Center at 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 also required to undergo additional role-specific training.

5. SECURITY CERTIFICATIONS & ATTESTATIONS

Aternity Mobile SaaS holds the following security-related certifications and attestations. Copies of such may be requested by visiting the Trust Center.

- ISO/IEC 27001
- SOC 2 Type II

Riverbed also holds an ISO/IEC 27701 certification. For additional details regarding Riverbed and Aternity Mobile SaaS certifications, please visit the Trust Center.

6. CLOUD ARCHITECTURE & DATA SEGREGATION

6.1. Hosting Architecture

Aternity Mobile SaaS leverages the public platform(s) of its Cloud Service Provider(s) ("**Cloud Environment**"). The Cloud Environment (including all hardware, software, and other supporting infrastructure) is owned, managed, and protected by the security and environmental controls of the applicable Cloud Service Provider.

6.2. Customer Data Storage

The hosting location of Customer Data is the production Cloud Environment in the Region offered by Riverbed and selected by Customer. "**Region**" means the physical location of a Cloud Service Provider's data center cluster; Region selection dictates where Cloud Environment resources are provisioned for Customer Data storage and processing. The current list of supported Regions is available in the subprocessor list.

6.3. Data Segregation

Aternity Mobile SaaS is operated in a multi-tenant architecture that is designed to segregate and restrict access to Customer Data. Customer Data is segregated using application logical segmentation: each Customer is assigned a Customer-specific unique account identifier and all Customer Data elements are tagged using this identifier.

7. ENCRYPTION

7.1. Customer Data Encryption

For Customer Data sent or received electronically, Riverbed encrypts Customer Data in transit both outside the Cloud Environment and within the network. When transmitting data, the Aternity Mobile Agent reports securely to Aternity Mobile SaaS via HTTPS; the Aternity Mobile Agent uses: (1) TLS 1.3 in transition for both Android and iOS; and (2) certificate pinning to avoid man in the middle eavesdropping of the TLS traffic; and it relies on OS containerization and secured storage (secure enclave and keystore) to guarantee no sensitive data can be accessed in device memory. Riverbed also encrypts Customer Data at rest in the Cloud Environment using AES 256-bit encryption.

7.2. Encryption Key Management

Aternity Mobile SaaS manages and maintains encryption keys in accordance with key management industry standards and leverages the applicable Cloud Service Provider's cloud-based key management services (e.g., AWS KMS). Customer Data stored within the Cloud Environment is encrypted at all times.

8. ACCESS CONTROL

8.1. Access Provisioning

Riverbed has an access control program that has been approved by management and communicated to relevant Riverbed personnel. Riverbed uses a central identity and access management system to provision access by Riverbed personnel in accordance with the principle of least privilege. Riverbed personnel are authorized to access Customer Data based on their job function, role, and responsibilities, and such access requires approval. All Riverbed personnel access to the Cloud Environment is via a unique user ID and password meeting the password controls outlined below; in addition, multi-factor authentication is required for remote access and access via privileged accounts. Access rights are reviewed at least quarterly. An employee's access is promptly removed upon termination of their employment.

Only a select predefined group of users are granted privileged system administration accounts: operations staff and SaaS admin users; each action taken by system administrators is audited.

8.2. Multi-Factor Authentication

Multi-factor authentication is enabled for all Riverbed personnel access to the Cloud Environment and Customer Data.

9. PHYSICAL & ENVIRONMENTAL SECURITY

9.1. Cloud Environment Data Centers

Riverbed regularly reviews each Cloud Service Provider's physical and environment controls for its data centers hosting the Cloud Environment as audited under the Cloud Service Provider's third-party audit and certifications. Riverbed requires that each Cloud Service Provider engaged by Riverbed must 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;
- 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 Aternity Mobile SaaS 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, and other pre-production 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. Aternity Mobile SaaS monitors and logs the following activities within the Cloud Environment; logs are stored for 1 year.

- Production issues are logged on a daily basis.
- The following activities are logged immediately: (i) failed logon attempts, (ii) application user locks, (iii) successful application log-ons by admin users, (iv) application data changes by Riverbed personnel, (v) application errors based on application KPIs, (vi) access denied to resources, and (vii) changes to user accounts by admin users.
- As governed by the ISO/IEC 27001:2013 Information Security Standard, Riverbed employs automated monitoring solutions that proactively alert upon production issues and security events, including: (i) verification of security updates on all servers, (ii) security events detected by A/V and IPS/IDS, and (iii) A/V scanning.

User Logs. As further described in the Documentation, Aternity Mobile SaaS also captures logs of certain activities and changes within a Customer's account and makes those logs available to Customer.

10.5. Network Management

Given that Aternity Mobile SaaS utilizes Cloud Service Provider public platforms, the respective Cloud Service Provider manages all physical-level network management, including (but not limited to) physical access controls, redundancy, capacity, and routing. Additionally, Aternity Mobile SaaS leverages the respective Cloud Service Provider's native network management components.

Aternity Mobile SaaS is architected to prevent man in the middle attacks: only Aternity Mobile Agent is permitted to initiate connection to the Aternity Mobile SaaS platform and connection requires a valid certificate issued by Aternity Mobile Certificate Authority (CA); all other connection attempts are logged and rejected.

11. APPLICATION DEVELOPMENT & CHANGE MANAGEMENT

11.1. Application Development

Aternity Mobile SaaS utilizes 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 process. Aternity Mobile SaaS is 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

Aternity Mobile SaaS maintains 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 Aternity Mobile SaaS assets. An executive summary of the Aternity Mobile SaaS 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 (30 days), high (45 days), and medium (120 days) after discovery and identification. Vulnerabilities classified as low priority that impact Aternity Mobile SaaS are added to the product release roadmap.

13. SECURITY INCIDENT MANAGEMENT

13.1. Policies & Procedures

Riverbed 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 Aternity Mobile SaaS 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 Aternity Mobile SaaS incident response plan occurs at least annually and include end-to-end testing, and review of the test result by product management leadership and remediation if needed.

13.2. Security Incident Notification & Communication

Riverbed notifies Aternity Mobile SaaS 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

All Aternity Mobile SaaS networking, systems, and application components are configured in a redundant configuration. The Cloud Environment leveraged by Riverbed is designed to mitigate the risk of single points of failure and provide a resilient environment to support continuity and performance achieved with virtualization technology and cloud-native technology from our Cloud Service Providers. Where available, Aternity Mobile SaaS utilizes independent availability zones offered by its Cloud Service Providers and is architected to fail-over between availability zones.

15.2. BCP/DR

Aternity Mobile SaaS has a business continuity plan ("**BCP**") and disaster recovery ("**DR**") plan. Aternity Mobile SaaS tests its DR plan on a monthly basis to validate the ability to failover a production instance from the primary data center to the secondary data center utilizing Aternity Mobile SaaS's 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.

Aternity Mobile SaaS 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, Aternity Mobile SaaS 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 Aternity Mobile SaaS user accounts to better protect access to Aternity Mobile SaaS; configuration options include:

- Single sign-on (SSO) / SAML 2.0-based integration (including the ability to enforce multi-factor authentication at Customer's identity provider);
- If not utilizing SSO: customized password policies, minimum password length and complexity, user lockouts after repeated failed login attempts, and disallowed password reuse; password encryption in transit as well as at rest;
- Role-based access control (RBAC);
- Idle timeout;
- Provisioning/deprovisioning process for the Customer's Aternity Mobile SaaS user accounts;
- API management (via OAuth); 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) Aternity Mobile SaaS user account log-ins, (ii) configuration changes, (iii) dashboard views, and (iv) API access.

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