riverbed

# Technical and Organizational Measures for SteelCentral Aternity SaaS

riverbed

This document describes the Technical and Organizational Measures (the "**TOMs**") implemented by Riverbed to protect the data customers entrust to Riverbed as part of SteelCentral Aternity SaaS.

As used in this document, the following definitions apply:

- "**Customer**" means any subscriber to Riverbed SteelCentral Aternity SaaS.
- "**SteelCentral Aternity SaaS**" means the Software-as-a-Service provided by Riverbed to its Customers.
- "**Customer Data**" means any information provided or submitted by the Customer that is processed by SteelCentral Aternity SaaS.
- "**Personal Data**" means information relating to an identified or identifiable natural person.

In addition to measures described in this document, more information is available at https://help.aternity.com/privacy.

riverbed

# 1. Infrastructure – Customer Data Storage

SteelCentral Aternity SaaS is hosted on the infrastructure of a third-party hosting provider, Amazon Web Services, Inc. ("**AWS**"); Riverbed stores Customer Data in data centers operated by AWS. Further information about security provided by AWS is available here, including AWS's data center controls.

In general, Customer Data is stored in data centers in the region from which a Customer subscribes to SteelCentral Aternity SaaS; however, Customers may request to be hosted in a specific region (either US- or EU-based region).

# 2. Architecture and Data Segregation

SteelCentral Aternity SaaS architecture provides logical data separation for different Customers and allows the use of Customer and user role-based access privileges. Additional data segregation is ensured by providing separate environments for different functions, especially for testing and production.

| Measures | Remark |
|---|---|
| Servers | All AWS instances are connected to AWS VPC. Each component has its own subnet.<br><br>Routing tables, NACLs and Security Groups are defined to allow communication only between relevant servers.<br><br>All AWS instances have only internal IP address.<br><br>All instances are protected using antivirus and intrusion prevention system solutions.<br><br>Servers are hardened pursuant to group policies. |

# 3. System Access

SteelCentral Aternity SaaS has a comprehensive access controls to ensure SteelCentral Aternity SaaS systems are accessed only by approved, authenticated users.

| Measures | Remark |
|---|---|
| Role-Based Access | SteelCentral Aternity SaaS assigns privileges to users according to the principle of least privilege. We give users the minimum access required for them to perform their tasks according to that role.<br><br>No one person may be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves sensitive information. |

| Measures | Remark |
|---|---|
| Principle of Least Privilege | Access privileges for any user should be limited to only what is necessary to complete their assigned duties or functions, and nothing more. |
| Change Log | Changes to the operating system and/or SteelCentral Aternity SaaS system configuration are logged. |
| Passwords | Riverbed has an established password policy that prohibits that sharing of passwords and requires passwords to be changed on a regular basis and conform to defined minimum complexity requirements. |
| Remote Access | The production environment is separated from Riverbed's office network.<br><br>Access to the SaaS environment requires VPN with multi factor authentication (MFA); Google Virtual Authenticator is used as the MFA mechanism.<br><br>Servers can be accessed only from Jump Box on AWS. |

## 4. Data Access

SteelCentral Aternity SaaS implements measures to prevent unauthorized access to Customer Data.

| Measures | Remark |
|---|---|
| Data Access Limitation | In the routine course of business, Riverbed personnel do not access Customer Data. |
| "Need-to-know" | Access to Customer Data is granted solely where an employee's job responsibilities necessitate access to such data on a strict, need-to-know basis. |
| Logging | Access is logged and monitored. |
| Personal Data | SteelCentral Aternity SaaS gathers the following categories of Personal Data in order to facilitate identifying and troubleshooting end user issues: Active IP Address, AD Title, Client Device Name, Email Address, Hostname, IP Address User Full Name, Username. SteelCentral Aternity SaaS does not store the contents of any applications, documents, emails, or text messages. |
| Training | Personnel training covers guidelines on the definition, use and protection of Personal Data. |
| Configuration Options | Customers have the option to configure the SteelCentral Agent for Windows (which monitors end user devices) to encrypt user-specific Personal Data when it reports to SteelCentral Aternity SaaS by enabling "Privacy Mode." The Privacy Mode setting encrypts the Personal Data from Windows devices permitting the Customer to associate several performance problems with the same hostname or user, but not the real-world name of the user who has those problems. |

riverbed

## 5. Data Transmission/Storage/Deletion

| Measures | Remark |
|---|---|
| Data Transmission | All data in transit (between the SteelCentral Agents and the SteelCentral Aternity SaaS servers) is encrypted. All traffic / communication is initiated from the SteelCentral Agent (not from server). |
| Cloud Management Platform | The SteelCentral Aternity SaaS cloud management platform is SSL-secured and password-protected; communications between a user's browser and the management portal can be encrypted leveraging a TLS-enabled connection. |
| Encrypted Database | Database volumes are encrypted. |
| Data Retention | SteelCentral Aternity SaaS stores Personal Data for a maximum of three months only. Performance measurements (which excludes Personal Data) are retained between one month and one year. |
| Data Deletion | Upon closure of a Customer SteelCentral Aternity SaaS account, all Customer Data (with the exception of Personal Data subject to the above retention schedule) will be deleted from Riverbed systems as soon as reasonably practicable and within a maximum period of twelve (12) months. Requests for return or other deletion requests are handled on a case-by-case basis. |

## 6. Confidentiality and Integrity

| Measures | Remark |
|---|---|
| Background Checks | Riverbed has a formal background check process and carries out background checks prior to employment commencing. |
| Confidentiality Obligation | Riverbed personnel are subject to a contractual or other appropriate statutory obligation of confidentiality, where necessary. |
| SDLC | Riverbed employs a robust and secure Software Development Life Cycle. |
| Change Management | SteelCentral Aternity SaaS Ops team tracks historical activities through SaaS change management records. The purpose of these records is to provide a historical audit trail for changes applied to the Customer environment that may be initiated by Customer request, system maintenance activity, incident management, upgrade activity, or proactive support. |
| Control Management Records | SaaS change management control records are created by the Hosting Operations or Support team representatives. They may be related to Support case activity, in which case, they will be identified in the records under "Case" field. Examples of related case activity are: critical system outage, Customer change request for runtime settings, hotfix or patches, or system environment upgrades. If the activity is not related to cases, records created would be proactive or preventative actions in nature and implemented by the Aternity Ops team in the course of normal system maintenance. |

riverbed

# 7. Monitoring

Riverbed monitors the SteelCentral Aternity SaaS systems including, but not limited, to the following types of servers: database servers, web and application servers, domain controllers, FTP and file exchange servers, and DNS servers.

| Measures | Remark |
|---|---|
| Uptime | 24x7 application availability monitoring. The SteelCentral Aternity SaaS Ops team receives alerts by phone, SMS, and email. |
| Host Resources | Monitoring the CPU, memory, network, disk space, disk I/O, and latency. |
| Performance | Monitoring application performance to ensure best use of the system. KPI metrics are collected and sent to the central monitoring system for evaluation and trend analysis. |
| Logs | Logs are collected to centralized locations for analysis. The SteelCentral Aternity SaaS Ops team proactively performs health checks on the functionality of the system on a regular basis |
| Event Reporting | Any outages that occur are tracked as Support case events for review and resolution. Once the system is up and verified functional, the case may be escalated to R&D for review, summarized and closed accordingly. |
| Customer Notification | Customers are notified via Salesforce regarding any change that affects accessibility to the system and/or negatively affects the functionality of the system. |

# 8. Incident Management

Riverbed maintains an up-to-date incident response plan that includes responsibilities, how information security events are assessed and classified as incidents and response plans and procedures. Riverbed regularly tests its incident response plan and incorporates the results of such tests in plan improvements. In the event of a security breach, Riverbed will notify Customers without undue delay after becoming aware of the security breach in accordance with applicable law.

riverbed

# 9. Reliability and Backup

SteelCentral Aternity SaaS is designed to ensure reliability through redundancy.

| Measures | Remark |
|---|---|
| Customer Data Backup | Customer Data is backed-up hourly and such back-ups are retained for up to a two (2) week period. |
| Oracle Database Backup | The Oracle database is backed up using the following methods:<br>• Clone database that is updated near real time and is located in a different AWS Availability Zone.<br>• Daily Recovery Manager Backup that is saved as an Amazon snapshot on AWS S3<br><br>Backups are retained for seven (7) days. |

# 10. Disaster Recovery

Through the use of Availability Zones and data replication, Riverbed aims to achieve short recovery time and recovery point objectives.

| Measures | Remark |
|---|---|
| Monitoring | The SteelCentral Aternity SaaS Product Operations team utilise alerts sent from the Amazon CloudWatch and other external monitoring systems to confirm outage events. |
| Standby System | The SteelCentral Aternity SaaS Disaster Recovery solution is based on a standby system that is located on a separate AWS Availability Zone.<br><br>Recovery Time Objective (RTO): In a worst case scenario in which the close database is damaged, the SteelCentral Aternity SaaS Ops team expects to recover from a disaster within 24 hours. If the clone database is not damaged, the team expects to recover within less than 1 hour.<br><br>Recovery Point Objective: The SteelCentral Aternity SaaS Ops team expects that the maximum targeted period in which data might be lost is 24 hours. |

riverbed

# 11. Audits and Certifications

The following security and privacy-related audits and certifications are applicable to Riverbed SteelCentral Aternity SaaS.

| Measures | Remark |
|---|---|
| Service Organization Control (SOC) report | SteelCentral Aternity SaaS undergoes an independent evaluation in the form of a SOC 2 Type 2 audit. The most recent SOC 2 report is available upon request and subject to written confidentiality obligations. |
| HIPAA | An independent auditor has also certified that SteelCentral Aternity SaaS's control environment satisfies the requirements of the HIPAA Security Rules (Health Information Insurance Portability and Accountability Act). |
| NIST 800-171 | Riverbed's corporate information security management systems are aligned to NIST 800-171 (which includes the following key control requirements: access control, awareness and training, audit and accountability, configuration management, identification and authentication, incident response, maintenance, media protection, personnel security, physical protection, risk assessment, security assessment, system and communications protection, and system and information integrity). |

Additionally, SteelCentral Aternity SaaS undergoes security assessments by internal personnel and third parties, which include infrastructure vulnerability assessments and application security assessments, on at least an annual basis.