riverbed

STEELHEAD SAAS CLOUD SERVICE

SECURITY MEASURES

These Security Measures describe the technical and organizational security measures implemented by the SteelHead SaaS Cloud Service (f/k/a SaaS Accelerator).

TABLE OF CONTENTS

1. OVERVIEW

The SteelHead SaaS Cloud Service ("**SteelHead SaaS**") is a subscription-based cloud-delivered solution offering end-to-end acceleration and performance measurement of leading third-party enterprise SaaS applications.

Upon subscription activation, SteelHead SaaS spins up acceleration infrastructure in a cloud-based service cluster. Any physical, virtual, or client-based SteelHead product pairs with the dedicated SteelHead SaaS service cluster to deliver increased third-party SaaS application performance. Users can access (i) configurations and (ii) metrics related to SteelHead SaaS components and usage via SteelHead SaaS's cloud-based control and management console.

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.

- "**AWS**" means Amazon Web Services' infrastructure as a service.
- "**Azure**" means Microsoft Corporation's infrastructure as a service.
- "**Client-Side SteelHead**" means the customer's physical, virtual, or client-based Riverbed SteelHead/optimization product.
- "**Customer Data**" means all information and data submitted by or on behalf of a customer to SteelHead SaaS.
- "**Personal Data**" means any information related to an identified or identifiable natural person.
- "**Personal Data Breach**" means a subtype of Security Incident involving Personal Data.
- "**SaaS App**" means a specified application made available by a third-party SaaS provider for which performance is accelerated in connection with SteelHead SaaS.
- "**SAM**" means SteelHead SaaS Manager, a cloud-based control and management console used to configure and deploy the overall SteelHead SaaS solution and display metrics related to SteelHead SaaS components and usage.
- "**Service Cluster**" means the dedicated cloud-based acceleration infrastructure.
- "**Security Incident**" means a breach of SteelHead 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 Customer 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 SteelHead SaaS, 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.

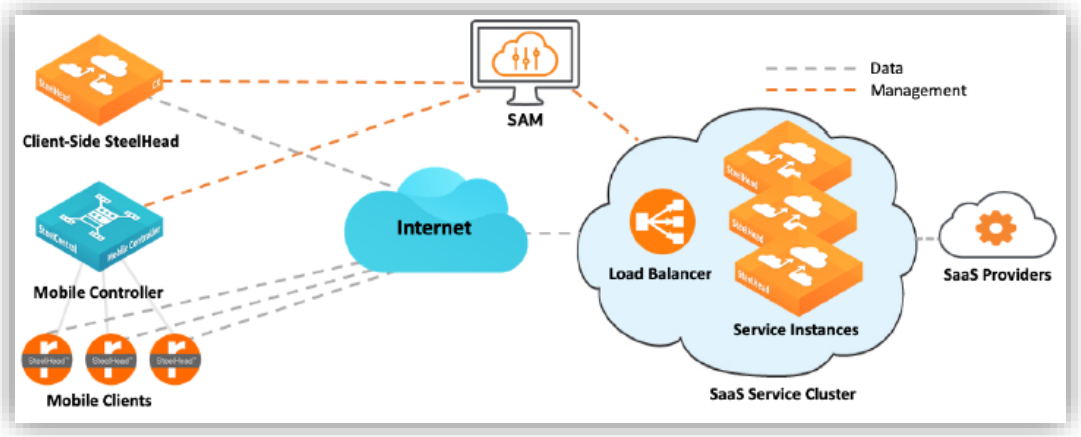
4.3 Personnel Training

All Riverbed personnel must undergo annual security, data handling and privacy training. Select roles are required to undergo additional security training.

5. CLOUD ARCHITECTURE & DATA SEGREGATION

5.1 Hosting Architecture

The overall SteelHead SaaS solutions consists of three key components: (1) SAM – running on AWS infrastructure as a service ("**IaaS**"); (2) one or more Service Clusters – running on Azure IaaS; and (3) Client-Side SteelHeads – consisting of on-premise appliances and/or software managed by the customer and installed in the customer's data centers, branch offices or on the customer's devices (i.e., laptops or desktops).



5.2 Customer Data Storage

SteelHead SaaS stores the following data: (i) customer configurations; and (ii) metrics related to SteelHead SaaS components and usage. SteelHead SaaS stores this data in SAM; at the time of purchase, customers may select the AWS Region from which SAM is provided. As of this document's publication date, the following AWS Regions are available: United States, EU (Frankfurt), Asia Pacific (Singapore), and Asia Pacific (Sydney).

Service Clusters are deployed in the Azure Region selected by customer. For optimal performance, most customers select the Azure Region nearest to where the customer's SaaS App server instance is located. As of this document's publication date, customers may select from the following Azure Regions: APAC (Singapore), Australia, Brazil, Canada, EMEA (Amsterdam), India, Japan, South Korea, United Arab Emirates, United Kingdom, and the United States. Traffic between Client-Side SteelHeads and the Service Cluster is stored solely for network optimization purposes and such traffic is encrypted at rest.

5.3 Data Segregation

SteelHead SaaS is designed to segregate and restrict access to customer data; customer data is segregated using logical separation. SAM's architecture leverages separate containers; each Service Cluster is deployed in a dedicated Azure Resource Group specific to each customer with unique credentials.

6. ENCRYPTION

Data is encrypted at rest with AES-256 or higher and in-transit within Riverbed's domain with TLS 1.2. Scalable Data Referencing (SDR) provides data scrambling at rest for end-user traffic. SDR takes all candidate traffic and segments it using a rolling data-driven computation.

7. ACCESS CONTROL

7.1 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. Access rights are reviewed at least semi-annually. An employee's access is promptly removed upon termination of their employment. All critical systems access is logged and monitored. Privileged access is logged, captured and monitored by SteelHead SaaS's automated systems.

7.2 Password Controls

For Riverbed personnel, password requirements include a minimum password length, complexity (a combination of upper-case letters, lower-case letters, numbers and special characters), limitations on password re-use, and automatic password expiration. Riverbed personnel are trained and required to change passwords if there is any indication of a possible compromise of the password system.

7.3 Customer Access

Customer access to SteelHead SaaS requires authentication via the following mechanism: user ID/password. Customers can elect to configure MFA via SAM. Following successful authentication, a random session ID is generated and stored in the user's browser to preserve and track session state. Session IDs are only sent over encrypted connections and rotated after successful login. A customer session is terminated when the user logs out; customers can configure SteelHead SaaS to automatically terminate a session if the session has been idle for a customer-designated period of time.

For account recovery, the SteelHead SaaS password reset interface will email a one-time URL to the customer email address on record.

8. PHYSICAL & ENVIRONMENTAL SECURITY

8.1 Cloud Environment Data Centers

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

8.2 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 points;
- Fire detection and sprinkler systems; and
- Climate control systems.

9. SYSTEM AND NETWORK SECURITY

9.1 Endpoint Controls

For access to the Cloud Environment, Riverbed personnel use Riverbed-issues 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 SteelHead SaaS does not send or receive Customer Data via physical media.

9.2 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.

9.3 Separation of Environments

SteelHead SaaS's infrastructure is partitioned into production and non-production environments. Development is performed in non-production environments with documented procedures for testing and validation of updates prior to production release. Production and non-production environments are logically segregated. Development, quality assurance (QA) and production use separate environments. Production data is not replicated or used in non-production environments. The SteelHead SaaS cloud environment is both logically and physically separate from Riverbed's corporate offices and networks.

9.4 Monitoring & Logging

SteelHead SaaS continuously collects and monitors environment logs. Access to audit logs is restricted to authorized Riverbed personnel. Audit logs are stored and retained whenever required.

9.5 Network Management

SteelHead SaaS relies on layers of network security and builds on top of the base network security, including firewall protection, provided by AWS and Azure for each respective component of the overall SteelHead SaaS solution. SteelHead SaaS communication between the Service Cluster and Client SteelHeads uses TLS 1.2 using peering certificates for mutual authentication. SteelHead SaaS leverages Azure Key Vault (Hardware Secure Module) for TLS key storage and management.

10. APPLICATION DEVELOPMENT & CHANGE MANAGEMENT

SteelHead SaaS maintains a Software Development Life Cycle ("**SDLC**") process that has been approved by management and communicated to appropriate Riverbed personnel. The Riverbed product management team is responsible for maintaining and reviewing the SDLC policy. SteelHead SaaS maintains a documented change management / change control process.

11. VULNERABILITY DETECTION & MANAGEMENT

If made aware of a vulnerability, Riverbed performs a triage process to determine the severity of the vulnerability; this includes a National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS)-style re-assessment to rate vulnerabilities into high, medium, or low severity levels. The severity level is used to determine the appropriate remediation response and schedule. Remediation efforts are prioritized and applied against critical and high-risk issues. Critical patches are installed in a timely manner. Non-critical patches are included in the pre-defined patch schedule and applied within commercially reasonable timeframes.

12. SECURITY INCIDENT MANAGEMENT

12.1 Policies & Procedures

SteelHead SaaS has an established incident management program that has been approved by management and communicated to relevant Riverbed personnel. The incident management program leverages a centralized incident management tool and SteelHead 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.

12.2 Security Incident Notification & Communication

Riverbed notifies SteelHead 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.

13. 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.

14. RESILIENCE & SERVICE CONTINUITY

14.1 Resilience

SteelHead SaaS leverages the underlying IaaS of AWS and Azure both of which are designed to mitigate the risk of single points of failure and provide a resilient environment to support continuity and performance. In the event SAM fails or is offline, Service Clusters remain unaffected and optimization between the applicable Service Cluster(s) and Client-Side SteelHead(s) continues without interruption. Service Clusters running on Azure's IaaS use premium Azure managed disks providing secure and scalable resource backup. Customer configurations in SAM are backed up and can be used to provision SteelHead SaaS in a different geographic region if necessary. In the event of a Service Cluster failure, SaaS App traffic is no longer accelerated, however, end-user access to the SaaS App is not disrupted.

14.2 BCP/DR

Riverbed's risk management program includes business continuity and disaster recovery strategies for data and hardware redundancy, network configuration redundancy and backups, and regular testing exercises. As part of its bustiness continuity program, Riverbed implements and maintains appropriate controls to protect its employees and assets against natural or man-made disasters.

14.3 Backups

Service Clusters running on Azure's IaaS use premium Azure managed disks providing secure and scalable resource backup. Customer configurations in SAM are backed up and can be used to provision SteelHead SaaS in a different geographic region if necessary.