riverbed®

SAAS ACCELERATOR

SECURITY OVERVIEW

Table of Contents

OVERVIEW

This document provides a general overview of the technical and organizational security measures implemented by Riverbed's SaaS Accelerator cloud product offering.

Introduction

SaaS Accelerator is a subscription-based cloud-delivered solution offering end-to-end acceleration and performance measurement of leading third-party enterprise SaaS applications.

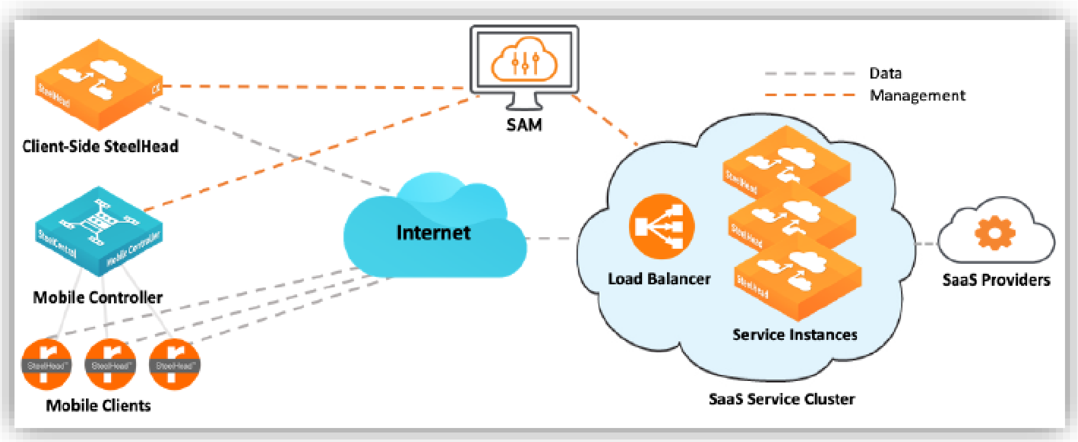
Upon subscription activation, SaaS Accelerator spins up acceleration infrastructure in a cloud-based service cluster. Any physical, virtual, or client-based SteelHead product pairs with the dedicated SaaS Accelerator service cluster to deliver increased third-party SaaS application performance. Users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

Definitions

- "**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.
- "**SaaS App**" means a specified application made available by a third-party SaaS provider for which performance is accelerated in connection with SaaS Accelerator.
- "**SAM**" means SaaS Accelerator Manager, a cloud-based control and management console used to configure and deploy the overall SaaS Accelerator solution and display metrics related to SaaS Accelerator components and usage.
- "**Service Cluster**" means the dedicated cloud-based acceleration infrastructure.

INFRASTRUCTURE

The overall SaaS Accelerator solutions consists of three key components: (1) SAM – running on Amazon Web Services ("AWS") infrastructure as a service (IaaS); (2) one or more Service Clusters – running on Microsoft Azure ("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).



Third party service providers

The following third party service providers are involved in the delivery of SaaS Accelerator as describe below:

Datadog, Inc.

SaaS Accelerator uses Datadog for cloud environment infrastructure monitoring; no personal data is collected in connection with such monitoring.

Kollective Technology, Inc.

SaaS App acceleration for Microsoft Teams and Microsoft Stream Certain uses enterprise content delivery networks ("eCDNs") to optimize content delivery. SaaS Accelerator reduces bandwidth constrains and accelerates video distribution by enabling Kollective Technology's eCDN.

PHYSICAL SECURITY

SaaS Accelerator runs on physical infrastructure built and maintained by AWS and Azure. This third-party infrastructure leverages data centers for which AWS and Azure are responsible for providing appropriate physical security measures. Further information about the physical security provided by: (i) AWS is available from the AWS website here, and (ii) Azure is available from the Azure website here.

MANAGEMENT LAYER SECURITY

Riverbed uses dedicated secure networks when accessing management software used to operate the SaaS Accelerator infrastructure. Only authorized personnel involved in SaaS Accelerator's operation and maintenance have access to this management network and must be authenticated using digital certificates with SSH protocol or HTTPS.

CODE SECURITY

Riverbed has established controls in place to protect application, program, or object source code, and restrict access to such code by authorized personnel only.

Application and interface security

SaaS Accelerator utilizes a Software Development Life Cycle (SDLC) process that has been approved by management and communicated to relevant Riverbed personnel. Code is subject to code security and quality reviews. Manual source code analysis is used to detect security defects in code as well as security vulnerabilities in applications prior to production. Critical vulnerabilities are addressed prior to deployment.

Change control and configuration management

SaaS Accelerator's operations team maintains an operational change management / change control process that has been approved by management and communicated to relevant Riverbed personnel. Changes to the production environment including systems, application updates and code changes are subject to the change control process.

Riverbed does not outsource SaaS Accelerator software development activities.

DATA SECURITY

Internal standard and policies

Riverbed has internal data handling standards and procedures to guide employees on appropriate data handling. Handling procedures include processing, storage, transmission and destruction of data. Controls such as separation of duties, role-based access control and least-privilege access for all personnel are implemented to mitigate and contain security risks.

Data classification and handling

Riverbed has controls in place to maintain the confidentiality of any customer data that the customer makes available to SaaS Accelerator. All Riverbed employees are bound by Riverbed's internal policies regarding maintaining confidentiality of customer data and contractually commit to these obligations.

Customers retain control and ownership of customer data, and it remains the responsibility of customers to implement a structured data-labeling standard to meet their own requirements if they so choose.

Product and non-production environments

SaaS Accelerator'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.

Architecture and data segregation

SaaS Accelerator 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.

Customer data access by Riverbed

Customers retain control and ownership of their customer data, and data stewardship of customer data remains the responsibility of the customer.

Access privileges to Riverbed systems used to deliver SaaS Accelerator are controlled based on the principle of least privilege – only the minimum level of access required is granted. Access is based on an individual's need-to-know as determined by job functions and requirements. Access privileges are authorized by the appropriate level of management and documented prior to being granted; access privileges are implemented and controlled through centralized tool and directories.

Access to customer environments where a customer's data is stored requires authorized Riverbed personnel to authenticate. All activity performed is logged. SaaS Accelerator's automated operations use log capture and security monitoring technologies tools to monitor Riverbed personnel accessing customer data and to monitor unauthorized access attempts.

Data storage and location

SaaS Accelerator stores the following data: (i) customer configurations; and (ii) metrics related to SaaS Accelerator components and usage. SaaS Accelerator 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.

Data protection

Data is encrypted at rest with AES-256 or higher and in-transit within Riverbed's domain with TLS1.2. 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.

Secure disposal

As described in the "INFRASTRUCTURE" section, SaaS Accelerator runs on infrastructure built and maintained by AWS and Azure, and as such AWS and Azure are responsible for securing such infrastructure, including secure disposal of physical assets. Further information for: (i) AWS can be found here; and (ii) Azure can be found here.

NETWORK SECURITY

SaaS Accelerator 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 SaaS Accelerator solution. SaaS Accelerator communication between the Service Cluster and Client SteelHeads uses TLS 1.2 using peering certificates for mutual authentication. SaaS Accelerator leverages Azure Key Vault (Hardware Secure Module) for TLS key storage and management.

IDENTITY AND ACCESS MANAGEMENT

Customer access

Customer access to SaaS Accelerator 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 SaaS Accelerator to automatically terminate a session if the session has been idle for a customer-designated period of time.

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

Riverbed users, groups and roles

The operation of SaaS Accelerator requires that some Riverbed personnel have access to the systems which store and process customer data. Strict access control, separation of duty and other policies define which Riverbed personnel have access to SaaS Accelerator's management systems. Riverbed personnel providing customer support may only access the customer's environment only after a customer has granted explicit permission via SAM's "Riverbed support access" setting.

All critical systems access is logged and monitored. Privileged access is logged, captured and monitored by SaaS Accelerator's automated systems.

Riverbed has established human resources (HR) policies for terminated employees. A semi-annual access review audit is performed to ensure access privileges are still appropriate. Controls are in place to ensure the timely removal of systems access no longer required for business purposes. HR systems, policies and procedures are in place to help guide management during termination or change of employment status. Access privileges to systems are removed when an employee leaves the company. An employee who changes roles within the organization will have access privileges modified according to their new position.

Customers are responsible for managing access to SAM and end-user access to customer resources including Client-Side SteelHeads.

Riverbed user access reviews and revocation

A semi-annual access review audit is performed to review entitlements for all Riverbed critical system users and administrators. All entitlement actions, along with remediation and certification actions for inappropriate entitlements, are recorded via Riverbed's internal systems used to grant/revoke access.

Timely de-provisioning (revocation or modification) of user access to the organization's systems, information assets, and data is implemented upon any change in status of employees, customers, business partners or involved third parties. Riverbed has HR systems, policies and procedures in place to help guide management during termination or change of employment status. Access privileges to systems are removed with a status change. Employees who change roles within the organization will have access privileges modified according to their new position. Any change in user access status is intended to include termination of employment, change of employment or transfer within the organization. A semi-annual access review audit is performed to ensure access is still appropriate, and regular internal audits are conducted to confirm access control changes have been implemented on critical systems.

VULNERABILITY AND PATCH 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.

As of this document’s publication date, SaaS Accelerator has not yet undergone any third-party independent evaluations; Riverbed will furnish copies of applicable third-party evaluations (including audit reports), subject to appropriate confidentiality obligations, as they become available.

OPERATIONS MANAGEMENT

Security, logging, monitoring and intrusion detection

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

Security incident management

Riverbed maintains an incident response plan that includes responsibilities, how information security events are assessed and classified as incidents, and response plans and procedures.

Incident reporting

Riverbed notifies SaaS Accelerator customers of (a) security incidents as required by applicable law; and (b) personal data breaches without undue delay. Notification(s) of such events 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 events.

HUMAN RESOURCES AND ORGANIZATIONAL SECURITY

Human resources security

Background screening

Pursuant to local laws, regulations, ethics and contractual constraints, employees are subject to background verification. Riverbed conducts criminal background checks, as permitted by applicable law, as part of pre-employment screening practices for employees commensurate with the employee’s position.

Employment agreements, training and termination

Riverbed maintains a set of human resource policies that have been approved by management, published, and communicated to all Riverbed personnel. A disciplinary process is in place for non-compliance. All Riverbed personnel are required to enter into employment agreements; Riverbed’s employment agreements include provisions relating to acceptable use, code of conduct/ethics, and confidentiality/non-disclosure agreement. All Riverbed personnel must undergo annual security training. Depending on job function, certain Riverbed personnel may receive additional role-based security training. An enterprise learning management system is used to facilitate the delivery of Riverbed training programs, including the annual security awareness training. The tools used to record the successful completion of required training, and completion reports are reviewed. Access privileges to systems are removed when an employee leaves Riverbed. An employee who changes roles within the organization will have access privileges modified according to their new position. Terminated employees are required to return assets.

Policy

Riverbed has a set of internal information security policies that have been approved by management, published, and communicated to Riverbed personnel.

Asset management

Riverbed maintains inventories of critical assets, including asset ownership, as well as an inventory of critical supplier relationships. Upon termination of workforce personnel, all organizationally owned assets are required to be returned within an established period.

Organizational security

Governance

Riverbed has designated an individual responsible for information security within its organization (the “CISO”) and has defined information security roles and responsibilities throughout the organization. Executive and senior leadership, in conjunction with Riverbed’s CISO, play important roles in establishing Riverbed’s overall information security management system program. Dedicated information technology security personnel are responsible for corporate information security processes. SaaS Accelerator product management oversees cloud product-specific security program and features.

Vendor risk management

Riverbed maintains a sourcing and vendor risk management process and program to select third-party vendors that meet Riverbed’s requirements. Vendor agreements are in place to ensure vendors comply with applicable laws, including security and privacy obligations. Riverbed assesses the privacy and security practices of any vendors engaged by Riverbed to assist with the processing of customer data. Vendors are required to enter into appropriate security, confidentiality and privacy contract terms with Riverbed based on the risks presented by the assessment, including data processing terms as required by applicable law.

BUSINESS CONTINUITY AND DISASTER RECOVERY

Business continuity

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.

Disaster recovery

SaaS Accelerator 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 SaaS Accelerator 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.