riverbed

STEELCENTRAL APPINTERNALS CLOUD SERVICE

PRIVACY AND SECURITY DOCUMENTATION

Published: May 17, 2019

STEELCENTRAL APPINTERNALS CLOUD SERVICE OVERVIEW

The SteelCentral AppInternals Cloud Service monitors the performance of an enteprise's web pages, applications and systems. The SteelCentral AppInternals Cloud Service provides complete insight, with full diagnostic detail for every transaction, at any scale by capturing all transactions, and their associated end user, trace, log, network metadata down to deep levels of app code, along with fine-grained infrastructure metrics to deliver a unified monitoring solution

Customers are responsible for choosing which application or server they would like to monitor by installing a SteelCentral Agent thereon. Once installed, the SteelCentral Agent transmits Customer Data (as defined below) to SteelCentral AppInternals servers, where it is processed and end user analytics are displayed back to the customer.

DEFINITIONS

- "**AWS**" means Amazon Web Services.
- "**Customer Data**" means (a) performance measurements, like wait times, response times, or resource consumption ("Performance Data"); and (b) non-measurable descriptive attributes, which add context to the performance measurements to help troubleshoot the problem, e.g., system name, user name, location name and application details like names, classes and methods ("Descriptive Data").
- "**End User Devices**" means Riverbed-managed desktops, laptops, tablets and smartphones.
- "**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.
- "**REST API**" means the SteelCentral AppInternals Cloud Service cloud API.
- "**Security Incident**" means a breach of Riverbed'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.
- "**SteelCentral Agent**" means a piece of software that a customer installs on an application or server that transmits Customer Data to Riverbed.
- "**SteelCentral AppInternals Cloud Service**" means Riverbed's cloud-hosted and/or SaaS offering of SteelCentral AppInternals.

1. SECURITY POLICY

1.1. The SteelCentral AppInternals Cloud Service has a set of information security policies that have been approved by management, published, and communicated to relevant Riverbed personnel.

1.1.1. The SteelCentral AppInternals Cloud Service undergoes an independent evaluation in the form of an annual SOC 2 Type 2 audit report; please refer to Section 17 for instructions on how to request a copy of this report.

2. CLOUD ARCHITECTURE AND SECURITY

2.1. The SteelCentral AppInternals Cloud Service leverages AWS's public cloud infrastructure meaning the underlying physical infrastructure on which a customer's Customer Data is stored is AWS's public cloud and the SteelCentral AppInternals Cloud Service runs on top of the AWS public cloud.

2.1.1. All hardware, software, and other supporting infrastructure is owned and managed by AWS; AWS data center controls are available at: https://aws.amazon.com/compliance/data-center/controls/.

2.2. The SteelCentral AppInternals Cloud Service is operated in a multi-tenant architecture that is designed to segregate and restrict access to Customer Data.

2.2.1. Customer Data is segregated using application logical segmentation: each customer is assigned a customer-specific unique account key and data is tagged as belonging to that customer; these account keys also facilitate the use of customer and user role-based access privileges.

2.3. The SteelCentral AppInternals Cloud Service stores Customer Data in an AWS data center located in the following AWS Region: US East (N. Virginia).

2.4. SteelCentral AppInternals Cloud Service's cloud environment has a logging, monitoring and alerting process in place.

2.5. SteelCentral AppInternals Cloud Service's cloud environment has the following controls in place:

2.5.1. Firewalls

2.5.2. IDS/IPS

2.5.3. Antivirus / antimalware

2.5.4. Access login

2.5.5. Security incident response

2.6. The SteelCentral AppInternals Cloud Service is architected to prevent man in the middle attacks: only SteelCentral Agents are permitted to initiate connection to the SteelCentral AppInternals server and require a valid Riverbed Certificate Authority (CA); all other connection attempts are logged and rejected.

2.7. SteelCentral AppInternals Cloud Service customers have the ability to manage the following types of security configurations:

2.7.1. Access and authentication controls;

2.7.2. API management;

2.7.3. SAML/SSO; and

2.7.4. Password policy.

3. ACCESS CONTROL

3.1. The SteelCentral AppInternals Cloud Service has an access control program that has been approved by management and communicated to relevant Riverbed personnel. The SteelCentral AppInternals Cloud Service product management is responsible for ownership and regular review of the SteelCentral AppInternals Cloud Service access control program.

3.1.1. Access control on all SteelCentral AppInternals Cloud Service systems is configured according to the principle of least privilege.

3.1.2. The SteelCentral AppInternals Cloud Service uses a central identity and access management system.

3.2. Individual IDs are required for user authentication to SteelCentral AppInternals Cloud Service systems.

3.2.1. Segregation of duties is taken into account for approving and implementing access requests.

3.2.2. User access rights are reviewed at least quarterly.

3.2.3. Access rights are reviewed when a Riverbed employee changes roles.

3.2.4. Privileged user access rights are reviewed at least quarterly.

3.2.4.1. All privileged account activities are logged and monitored.

3.2.5. Multi-factor authentication is deployed for both remote access (VPN) and privileged accounts (admin).

3.2.6. Shared user account credentials are securely stored and access is controlled, audited and monitored.

3.3. Remote sessions timeout after a thirty (30) minute period.

3.4. The SteelCentral AppInternals Cloud Service requires that administrator passwords include:

3.4.1. A minimum password length of at least eight characters.

3.4.2. A requirement of complexity (a combination of upper case letters, lower case letters, numbers and special characters).

3.4.3. Password history at least 12 before reuse.

3.4.4. A requirement for initial and temporary passwords to be changed upon next login.

3.4.5. A requirement that initial and temporary passwords be random and complex.

3.4.6. A requirement to change passwords when there is an indication of possible system of password compromise.

3.4.7. A requirement that passwords expire within ninety (90) days or less.

3.4.8. A requirement to terminate or secure active sessions when finished.

3.4.9. A requirement to logoff terminals, PC or servers when the session is finished.

3.4.10. A requirement to not include unencrypted passwords in automated logon processes.

3.5. Passwords are encrypted in transit.

3.6. Passwords are encrypted or hashed in storage.

3.7. Encrypted communications are required for all remote connections.

4. APPLICATION SECURITY

4.1. No outside development resources are utilized in the development of the SteelCentral AppInternals Cloud Service.

4.2. The SteelCentral AppInternals Cloud Service is configured to follow best practices or security guidelines, e.g., OWASP.

4.3. Development, test and staging environments are separated from the production environment by either separate VPC or physical location.

4.4. The SteelCentral AppInternals Cloud Service utilizes a formal Software Development Life Cycle (SDLC) process that has been approved by management and communicated to appropriate Riverbed personnel. The SteelCentral AppInternals product management team is responsible for maintaining and reviewing the SDLC policy.

4.5. The SteelCentral AppInternals Cloud Service maintains a documented change management / change control process that includes:

4.5.1. Change control procedures required for all changes to the production environment.

4.5.2. Testing prior to deployment.

4.5.3. Stakeholder communication and/or approvals.

4.5.4. Documentation for all system changes.

4.5.5. Version control for all software.

4.5.6. Logging of all change requests.

4.5.7. Backout procedures are required for production changes.

4.5.8. Access to make changes to source code is restricted to select Riverbed personnel.

4.6. The SteelCentral AppInternals Cloud Service is evaluated from a security perspective prior to promotion to production.

4.6.1. For every release, the following security testing procedures are performed:

4.6.1.1. Security requirements gathering.

4.6.1.2. Security architecture review.

4.6.1.3. Security signoffs.

4.6.1.4. Secure code reviews.

4.6.1.5. Vulnerability scans.

4.6.2. The SteelCentral AppInternals Cloud Service is subject to third party penetration testing at least annually.

4.6.3. The SteelCentral AppInternals Cloud Service conducts regular vulnerability analysis.

4.6.4. Sessions IDs: the SteelCentral AppInternals Cloud Service generates session IDs automatically/randomly; session IDs are in-memory only and are not stored.

4.6.4.1. Session IDs are sent only over encrypted connections.

4.6.4.2. Session IDs are rotated after successful login.

4.6.4.3. The SteelCentral AppInternals Cloud Service disconnects the sessions when the user terminates the session.

4.6.4.4. The SteelCentral AppInternals Cloud Service automatically terminates a customer session and logs out if the customer session has been idle for more than 3.5 hours.

5. ASSET AND INFORMATION MANAGEMENT

5.1. The SteelCentral AppInternals Cloud Service 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.

5.2. A process is in place to verify the return of Riverbed personnel assets (e.g. computers, cell phones, access cards, tokens, smart cards, keys, etc.) upon termination.

5.2.1. Riverbed personnel must return assets as soon as possible and access to SteelCentral AppInternals Cloud Service systems is revoked immediately upon termination.

5.2.2. Riverbed personnel assets are not used to store or process Customer Data.

5.3. The SteelCentral AppInternals Cloud Service does not send or receive Customer Data via physical media.

5.4. For Customer Data sent or received electronically, the SteelCentral AppInternals Cloud Service:

5.4.1. Encrypts Customer Data in transit while outside the network.

5.4.2. Encrypts Customer Data in transit within the network.

5.4.3. Deploys the following encryption protocols and algorithms for Customer Data transmission:

5.4.3.1. SteelCentral Agent files are digitally signed to protect against tampering in transit and incorporate several anti-hacking measures, including ASLR, DEP, and SHE.

5.4.3.2. When transmitting data, SteelCentral Agents report securely to the management console via HTTPS; SteelCentral Agents use TLS 1.1 or TLS 1.2 on devices with .NET 4.5 or later.

5.4.3.3. Customers may also request to configure SteelCentral Agents for two-way TLS authentication.

5.4.4. Validates Customer Data integrity following transmission using the measures outlined in Section 5.4.3.1 above.

5.5. For Customer Data stored electronically, the SteelCentral AppInternals Cloud Service:

5.5.1. Encrypts Customer Data at rest using AWS Key Management System (KMS) and AES 256-bit encryption.

5.5.2. Enables full-disk encryption.

5.5.3. Encrypts backup tapes and disks during storage.

5.6. The SteelCentral AppInternals Cloud Service manages and maintains encryption keys in accordance with key management industry standards and using a centralized key management system.

5.7. Riverbed personnel may only view a Customer's unencrypted Customer Data only in the context of providing support services in relation to the SteelCentral AppInternals Cloud Service and only to the extent that Customer has provided Riverbed with access to such unencrypted Customer Data.

6. INFORMATION HANDLING

6.1. The SteelCentral AppInternals Cloud Service classifies Customer Data according to legal or regulatory requirements and sensitivity to unauthorized disclosure and/or modification.

6.2. The SteelCentral AppInternals Cloud Service does not leverage public cloud storage, email, web and file transfer services, or removable media to deliver the product.

6.3. The SteelCentral AppInternals Cloud Service is hosted on AWS infrastructure; AWS data center controls, including its controls related to media disposal and decommissioning of assets are available at: https://aws.amazon.com/compliance/data-center/controls/.

7. OPERATIONS MANAGEMENT

7.1. The SteelCentral AppInternals Cloud Service maintains and periodically reviews a documented operational change management / change control program that has been approved by management and communicated to relevant Riverbed personnel.

7.1.1. Changes to the production environment including systems, application updates and code changes are subject to the change control process.

8. END USER DEVICE SECURITY

8.1. The SteelCentral AppInternals Cloud Service does not use End User Devices for transmitting, processing or storing Customer Data. Customer Data is transmitted from the SteelCentral Agent to SteelCentral AppInternals servers for processing and storage; these servers are hosted on AWS infrastructure.

9. NETWORK SECURITY

9.1. The SteelCentral AppInternals Cloud Service is hosted on AWS infrastructure and as such AWS is responsible for all network management.

10. HUMAN RESOURCE SECURITY

10.1. 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.

10.2. All Riverbed personnel are required to undergo background screening, which includes a criminal background check, prior to commencing employment with Riverbed.

10.3. All Riverbed personnel are required to enter into employment agreements; Riverbed's employment agreements include provisions relating to:

10.3.1. Acceptable Use

10.3.2. Code of Conduct / Ethics

10.3.3. Confidentiality / Non-Disclosure Agreement

10.4. All Riverbed personnel must undergo annual security training. Select roles are required to undergo additional security training.

10.5. Access to SteelCentral AppInternals Cloud Service systems containing Customer Data is revoked immediately upon termination.

11. ORGANIZATIONAL SECURITY

11.1. Riverbed has designated an individual responsible for information security within its organization (the "**Information Security Officer**") and has defined information security roles and responsibilities throughout the organization. Internal information security personnel are responsible for corporate information security processes.

11.2. The following roles share responsibility for managing the information security program within Riverbed:

11.2.1. The Information Security Officer described in Section 11.1; and

11.2.2. The Chief Information Officer.

11.3. All Riverbed personnel are required to undergo annual security training in addition to Riverbed's ongoing security awareness program.

11.4. SteelCentral AppInternals Cloud Service product management oversees the product-specific security program and features.

12. PHYSICAL AND ENVIRONMENTAL SECURITY

12.1. The SteelCentral AppInternals Cloud Service is hosted on AWS infrastructure; AWS data center controls are available at: https://aws.amazon.com/compliance/data-center/controls/.

12.2. As part of Riverbed's corporate organizational alignment to the NIST 800-171 standard, Riverbed maintains physical security and environmental controls for its office buildings which include:

12.2.1. Physical access control mechanisms (e.g., electronic access control, locks) to ensure only authorized individuals can obtain physical access to Riverbed facilities;

12.2.2. Riverbed conducts periodic inspections of facility perimeters and all access control mechanisms to provide ensure controls cannot be easily manipulated or bypassed to gain unauthorized access;

12.2.3. All Riverbed facility access/egress points are monitored by security staff and/or recorded with security cameras twenty-four (24) hours a day, seven (7) days a week;

12.2.4. Riverbed ensures that its personnel within Riverbed's facilities (e.g., employees, visitors, resident contractors) are able to be immediately identified (e.g., using identification badges);

12.2.5. Riverbed escorts visitors at all times. Riverbed data centers shall have a unique registry for all visitors and maintain access control logs.

13. THREAT MANAGEMENT

13.1. The SteelCentral AppInternals Cloud Service maintains and periodically reviews its anti-malware program; the anti-malware program has been approved by management and communicated to relevant Riverbed personnel.

13.1.1. New anti-malware signature updates are deployed no later than twenty-four (24) hours after release.

13.2. The SteelCentral AppInternals Cloud Service maintains and periodically reviews its vulnerability management program; the vulnerability management program has been approved by management and communicated to relevant Riverbed personnel.

13.2.1. Software vulnerability scans of SteelCentral AppInternals are performed periodically in accordance with the SDLC; software vulnerability scans are conducted prior to moving from QA to production.

13.2.2. 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 SteelCentral AppInternals Cloud Service assets.

13.3. Any vulnerabilities identified during this process are remediated in accordance with the following timelines:

13.3.1. Vulnerabilities classified as critical, high or medium priority are remediated as soon as possible, and in any event no later than 30 days after identification.

13.3.2. Vulnerabilities classified as low priority are added to the development roadmap and generally remediated within the next release cycle.

14. INCIDENT EVENT AND COMMUNICATIONS MANAGEMENT

14.1. The SteelCentral AppInternals Cloud Service has an established incident management program that has been approved by management and communicated to relevant Riverbed personnel.

14.1.1. The SteelCentral AppInternals Cloud Service incident management program leverages a centralized incident management tool.

14.2. The SteelCentral AppInternals Cloud Service maintains a formal incident response plan; it includes guidance for:

14.2.1. Feedback and lessons learned.

14.2.2. Applicable data breach notification requirements (including notification timing).

14.2.3. Escalation procedure.

14.2.4. Communication timelines and process.

14.2.5. Procedures to collect and maintain a chain of custody for evidence during incident investigation.

14.2.6. Actions to be taken in the event of a Security Incident.

14.3. Testing of the SteelCentral AppInternals Cloud Service incident response plan occurs at least annually and includes:

14.3.1. End-to-end testing.

14.3.2. Security incident response and data breach response.

14.3.3. Associated BCP / DR plans.

14.3.4. Review of the test result by product management leadership and remediation if needed.

Riverbed notifies SteelCentral AppInternals Cloud Service 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.

15. PRIVACY

15.1. Riverbed's Privacy Policy, available at www.riverbed.com/privacypolicy describes its practices and policies regarding the Personal Data it collects from individuals who visit Riverbed's website and interact with Riverbed online, and from Riverbed products and related services offered by Riverbed.

15.1.1. More information about Riverbed's privacy practices is available at www.riverbed.com/privacy.

15.1.2. Riverbed's corporate GDPR statement is available at www.riverbed.com/gdpr.

15.1.3. Riverbed's data processing addendum ("**DPA**") is available at www.riverbed.com/data-processing-addendum.

15.2. Riverbed provides data privacy and data protection training and awareness for its personnel.

15.3. The SteelCentral AppInternals Cloud Service collects two types of Customer Data: (a) performance measurements, like wait times, response times, or resource consumption ("**Performance Data**"); and (b) non-measurable descriptive attributes, which add context to the performance measurements to help troubleshoot the problem, e.g., system name, user name, location name and application details like names, classes and methods ("**Descriptive Data**").

15.3.1. More information about SteelCentral AppInternals Cloud Service's data collection and privacy features is available at:

https://doc.steelcentral.net/help/wwhelp/wwhimpl/js/html/wwhelp.htm#href=Notices/appinternals_privacy.html.

15.3.1.1. The SteelCentral AppInternals Cloud Service does not collect or store the content of any customer applications, documents, emails or text messages.

15.3.2. The Descriptive Data processed by the SteelCentral AppInternals Cloud Service may contain Personal Data; as of this document's publication date, the SteelCentral AppInternals Cloud Service collects the following categories of Personal Data:

15.3.2.1. User IP address; and

15.3.2.2. Username.

More information regarding the categories of Personal Data collected by the SteelCentral AppInternals Cloud Service is available at:

https://doc.steelcentral.net/help/wwhelp/wwhimpl/js/html/wwhelp.htm#href=Notices/appinternals_privacy.html

15.4. The SteelCentral AppInternals Cloud Service stores Customer Data in an AWS data center located in the following AWS Regions: US East (N. Virginia) for data storage.

15.4.1. Riverbed complies with applicable data protection laws governing the transfer of Personal Data outside of the European Economic Area ("EEA") as further described in Riverbed's DPA available at www.riverbed.com/data-processing-addendum.

15.5. Retention of Customer Data processed by the SteelCentral AppInternals Cloud Service is dependent on the volume of such Customer Data elected to be processed by customer in conjunction with the amount of storage available in such customer's tenant.

15.6. Within thirty (30) days post contract termination, SteelCentral AppInternals Cloud Service customers may request and Riverbed will for a period of no longer than sixty (60) days make Customer Data available to such customer for export or download as provided in the SteelCentral AppInternals Cloud Service documentation.

15.7. Riverbed assesses the privacy and security practices of any subprocessor engaged by Riverbed to assist with the processing of Customer Data. Subprocessors 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.

15.7.1. As of this document's publication date, the SteelCentral AppInternals Cloud Service engages the following third-party subprocessors:

15.7.1.1. Amazon Web Services – cloud hosting infrastructure for the SteelCentral AppInternals cloud environment;

15.7.1.2. Answer 1, LLC – Tier 1 24x7 telephone customer support services; and

15.7.1.3. salesforce.com, inc. – customer account administration and support case incident management.

16. BUSINESS CONTINUITY, DATA BACKUP AND DISASTER RECOVERY

16.1. The SteelCentral AppInternals Cloud Service is designed for redundancy and resiliency.

16.1.1. Customer Data is backed-up on an hourly basis; back-ups are retained for a rolling one (1) week period.

16.2. The AWS production data centers leveraged by the SteelCentral AppInternals Cloud Service are designed to mitigate the risk of single points of failure and provide a resilient environment to support continuity and performance. AWS utilizes independent Availability Zones with high availability and the SteelCentral AppInternals Cloud Service is architected to automatically fail-over between Availability Zones without interruption.

16.3. The SteelCentral AppInternals Cloud Service reviews its business continuity and disaster recovery ("**BCP / DR**") plan twice a year; such review involves conducting table-top exercises and auditing any identified dependencies.

16.4. The SteelCentral AppInternals Cloud Service does not have a defined recovery time objective ("RTO") or recovery point objective ("RPO"). Recovery times are dependent on the volume of Customer Data elected to be processed by customer in conjunction with the amount of storage available in such customer's tenant.

17. SUPPLEMENTAL DOCUMENTATION

17.1. SteelCentral AppInternals Cloud Service customers may request copies of the following report(s) and additional policies and/or programs ("Supplemental Documentation") subject to appropriate written confidentiality obligations. Please email compliance@riverbed.com for Supplemental Documentation requests with the words "SteelCentral AppInternals Supplemental Documentation Request" in the subject line and specify what copies of the Supplemental Documentation listed below that you would like to receive:

17.1.1. SOC 2 Type 1 report (SOC 2 Type 2 forthcoming);

17.1.2. SteelCentral AppInternals SaaS Architecture;

17.1.3. SteelCentral AppInternals System Development Life Cycle;

17.1.4. SteelCentral AppInternals SaaS Change Management;

17.1.5. SteelCentral AppInternals SaaS Risk Assessment Policy;

17.1.6. SteelCentral AppInternals APM User Access Control Policy;

17.1.7. SteelCentral AppInternals Incident Response Guidelines;

17.1.8. SteelCentral AppInternals SaaS Disaster Recovery Procedure;