SteelCentral AppInternals SaaS

SteelCentral AppInternals SaaS helps you build and deliver high-performing applications, infrastructure, and networks on and off the cloud. It continuously monitors them with minimal overhead to give you end-to-end visibility and insights around-the-clock.

SteelCentral AppInternals SaaS collects server-side application monitoring metrics, including but not limited to, CPU utilization, memory utilization and transaction response times (collectively, "**Customer Data**") from the customer and uses this data to provide application performance analytics, network and infrastructure diagnostics, and user experience and business insights. Detailed information about what personal data SteelCentral AppInternals SaaS collects along with its privacy and security practices is available here. A high-level overview of relevant topics is provided below.

Processing of Customer Data

The customer is responsible for choosing which software, system or application they would like to monitor by installing a SteelCentral agent therein. Once installed, the SteelCentral agent transmits Customer Data to SteelCentral AppInternals SaaS servers, where it is processed, and performance analytics are displayed back to the customer.

SteelCentral AppInternals SaaS is designed to monitor application performance, not individuals. Certain customers may choose to configure SteelCentral AppInternals SaaS to process certain types of data for their use that may include personal data. Configuration settings are completely within the customer's control and customers may change their settings to address data privacy and security concerns.

Storage and Transfer

SteelCentral AppInternals SaaS servers are located in the United States. To provide customers with the best possible service, Riverbed operates a follow-the-sun 24/7 global support delivery model. Riverbed transfers any personal data in compliance with applicable legislation, including ensuring that transfers of personal data outside of the EEA are subject to appropriate safeguards.

Security Measures

SteelCentral AppInternals SaaS provides industry standard data security mechanisms and controls that incorporate 'privacy by design and privacy by default' principles. Such measures include but are not limited to:

Encryption

- ***SteelCentral agents***: Communications between SteelCentral agents and Riverbed servers are encrypted in transit.
- ***Cloud management platform***: The SteelCentral AppInternals 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.
- ***Databases***: SteelCentral AppInternals SaaS servers reside in state-of-the-art data centers that comply with a variety of IT security standards, including SOC 1, SOC 2 and ISO 27001. Customer Data stored on SteelCentral AppInternals SaaS servers is encrypted at rest.

Access Controls

SteelCentral AppInternals SaaS provides customers with the ability to implement and configure detailed access controls in order to help regulate access to Customer Data and any personal data included therein. Customers can define specific user roles and groups to which pre-defined permissions are assigned.

Data Segregation and Infrastructure

SteelCentral AppInternals SaaS is built on a multitenant architecture with utmost care to ensure separation of data between multiple tenants on the cloud-hosted infrastructure.

Security Standards and Certifications

Riverbed's corporate security policies are aligned with the NIST 800-171 standard, 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. At this time, SteelCentral AppInternals SaaS has been issued a SOC 2 Type 1 audit report and will be undergoing annual SOC 2 Type II audits of its security practices and policies going forward.

Customer Data Backup, Retention and Deletion

Customer Data is backed-up hourly and such back-ups are retained for up to a two (2) week period.

Riverbed does not retain any personal data collected in connection with the provision of SteelCentral AppInternals SaaS on its long-term aggregation servers and typically deletes any personal data within a few weeks and in any event within ninety (90) days.

Upon closure of a customer SteelCentral AppInternals 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.