SteelCentral Aternity SaaS

SteelCentral Aternity SaaS monitors the performance of applications and devices from the end user perspective so that the customer can measure and improve the productivity of its workforce.

Riverbed collects performance measures and non-measureable descriptive attributes which provide additional context for performance measurements from applications, devices and end users (collectively, "**Customer Data**") to proactively identify and rapidly resolve end user issues and optimize workforce productivity. Detailed information about what personal data SteelCentral Aternity 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 application or device they would like to monitor by installing a SteelCentral agent therein. Once installed, the SteelCentral agent transmits Customer Data to Aternity servers, where it is processed, and end user analytics are displayed back to the customer.

SteelCentral Aternity SaaS is designed to monitor the end-user experience, not individuals. Certain customers may choose to configure SteelCentral Aternity 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. More information about such settings is available here.

Storage and Transfer

Customers may select the data center region in which SteelCentral Aternity SaaS will be hosted. Available SteelCentral Aternity SaaS data center regions include the United States and Germany. 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 Aternity 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. Customers may also request to configure SteelCentral agents for two-way TLS authentication.
- ***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.
- ***Databases***: SteelCentral Aternity 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 Aternity SaaS servers is encrypted at rest.

Access Controls

SteelCentral Aternity 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 Aternity 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. SteelCentral Aternity SaaS has been issued a SOC 2 Type 2 audit report and undergoes annual audits of its security practices and policies.

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 Aternity SaaS on its long-term aggregation servers and typically deletes any personal data within a few weeks and in any event within a maximum period of ninety (90) days.

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.