Riverbed Xirrus Management System (XMS) Cloud

XMS-Cloud is a cloud-based network-management platform for deploying and managing Wi-Fi networks. It provides complete control and visibility for network administrators bringing improved affordability and efficiency.

XMS-Cloud collects network management data that is user-related (i.e. MAC address, IP address, device information) and performance-related (i.e. applications, application usage, connection speeds, throughput) from the customer's Wi-Fi network (collectively, "**Customer Data**"). A high-level overview of relevant topics is provided below.

Processing of Customer Data

Using Riverbed Xirrus access points along with XMS-Cloud, customers can design and deploy Wi-Fi networks from which their enterprise and guests can access online resources and the internet. Customer Data is transmitted to XMS-Cloud servers via the Xirrus access points for the purpose of displaying network configuration information, analytics and insights back to the customer. XMS-Cloud architecture is designed to separate Customer Data from end user traffic data (i.e. web browsing, internal applications, etc.) such that only Customer Data flows to XMS Cloud servers, while end-user traffic data remains on the customer's LAN and flows directly to its destination.

Ultimately, XMS-Cloud is designed to manage and monitor networks, not individuals. Certain customers may choose to configure XMS-Cloud 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. For example, customers may choose to hash MAC addresses when publishing location data to a third-party service through APIs. More information about such settings is available here.

Storage and Transfer

XMS-Cloud 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

XMS-Cloud 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

- ***Xirrus access points***: Customer Data is transmitted from a customer's edge device to Xirrus access points with which the edge device connects, and the access points transmit Customer Data by means of an encrypted connection to XMS-Cloud servers for display via XMS-Cloud.

- ***Cloud management platform***: The XMS-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**: XMS Cloud 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 XMS Cloud servers is encrypted at rest.

Access Controls

XMS-Cloud 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

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

Security Standards

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.

Customer Data Backup, Retention and Deletion

Customer Data is backed-up daily and statistical data is backed-up five (5) times per week. Data is retained in raw form for thirty (30) days after which only aggregated data is stored along with associated device information for a period of up to twelve (12) months.

Upon closure of a customer XMS-Cloud account, Riverbed will delete all Customer Data at the customer's request. Requests for return of Customer Data or other deletion requests are handled on a case-by-case basis.