riverbed

Riverbed Xirrus Cloud Processes and Data Privacy

June 19, 2018

riverbed

PURPOSE OF THIS DOCUMENT

This document outlines Xirrus Management System – Cloud ("**XMS-Cloud**") processes and data privacy practices. Riverbed takes rigorous steps to ensure the reliability, scalability, availability, security of XMS-Cloud services and data privacy of our users.

In this document, references to "XMS-Cloud" and "XMS-Cloud Services" encompass all Riverbed Xirrus services offered as a SaaS which includes XMS-Cloud management platform, EasyPass Access Services and CommandCenter.

Specific to data privacy, this document outlines how the XMS-Cloud Services can help customers meet their privacy-related compliance obligations.

DATA CENTER PROCESSES

XMS-Cloud Services are hosted in state of the art data centers located in the United States, which utilize innovative architectural and engineering approaches. These data centers implement a secure infrastructure with audit services. All XMS-Cloud Services are hosted in redundant data centers. These data centers are designed and managed in compliance with security best practices and a variety of IT security standards, which include but are not limited to:

- CSA, ISO 9001 /27001 /270017 / 270018
- PCI DSS Level1, SOC 1/ 2/ 3
- FISMA, FedRAMP, FIPs, FERPA, CJIS, NIST
- DoD SRG, ITAR, PDPA, Privacy Act, MTSC

Physical and Environmental Security

The data centers that host the XMS-Cloud Services are fully equipped with fire detection, fire suppression, 24x7 power backup in the event of critical power failure, state of the art climate and temperature controls and 24x7 monitoring of all critical environmental parameters.

Resiliency and Redundancy

The data center infrastructure has a high level of availability and provides customers the features to deploy a resilient IT architecture. The data center systems are designed to tolerate system or hardware failures with minimal customer impact. The data centers act as backup data centers for each other and provide redundant infrastructure.

Network Security

Network devices, including firewall and other boundary devices, are in place at the data centers to monitor and control communications at the external boundary of the network and at key internal boundaries within the network. These boundary devices employ rule sets, access control lists (ACL), and configurations to enforce the flow of information to specific information system services.

riverbed®

Network Monitoring

The data center infrastructure utilizes a wide variety of automated monitoring systems to provide a high level of service performance and availability. Monitoring tools in place at the data centers are designed to detect unusual or unauthorized activities and conditions at ingress and egress communication points. These tools monitor server and network usage, port scanning activities, application usage, and unauthorized intrusion attempts. Controls are in place to address various types of attacks including:

- Distributed Denial Of Service (DDOS)
- Man in the Middle (MITM)
- IP spoofing
- Port scanning and port sniffing

Access Controls and Audits

Access to the data centers is limited to employees and contractors who have a legitimate business need for such privileges. When a data center employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee. All physical access to data centers is logged and audited routinely.

XMS-CLOUD SERVICES

XMS-Cloud architecture is designed for high resiliency and availability. Additionally, XMS-Cloud Services are designed for extreme scalability with all the security controls and minimal reliance on the cloud infrastructure for Wi-Fi network operations.

The application infrastructure is managed by a 24x7 operational team to ensure high performance and availability of the XMS-Cloud Services.

Scalability

XMS-Cloud Services are highly scalable with the ability to add capacity on demand. XMS-Cloud application nodes can be instantly added to augment necessary application demands.

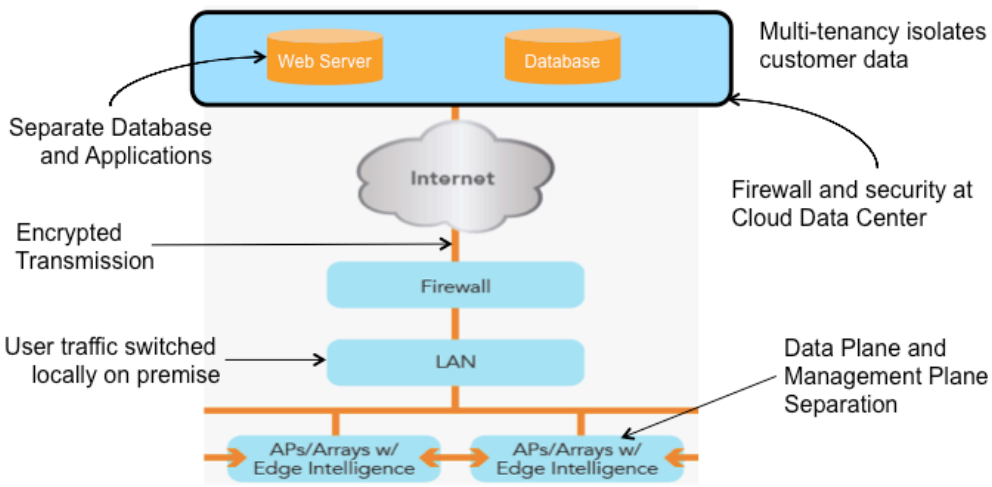
Reliability

Redundant cloud service provides high availability and client connectivity is not impacted even if internet connectivity between access points and the XMS-Cloud platform is lost. Access points continue to act autonomously even if a cloud connection is lost, meaning security and traffic are processed directly at the network edge in each access point.

Security

Management traffic between access points and the XMS-Cloud platform is encrypted using industry standard encryption (https over SSL/TLS). The application and network object databases are hosted on different servers to create another level of separation. All passwords are encrypted in transit and stored in encrypted format. Riverbed follows industry best security practices for application design, development and implementation.

XMS-Cloud Architecture



Administrative Access

XMS-Cloud Services provide granular role-based access to the XMS-Cloud console. Administrators can use any browser-enabled devices to access the XMS-Cloud console. Access to the XMS-Cloud console is password protected and the passwords are stored in a 1-way hash algorithm and the sessions are timed out after three (3) hours of inactivity. Sessions are encrypted using SSL/TLS. XMS-Cloud also supports SSO-based access using federated identity management (FIdM) systems such as Azure and Google. Communications between XMS-Cloud and these FIdM systems are encrypted using SSL/TLS.

DATA PRIVACY

XMS-Cloud Services are built on a multitenant architecture with the utmost care to ensure separation of data between multiple tenants on the cloud infrastructure. Each tenant's data is isolated from that of other tenants. The table below identifies the types of data collected and stored by XMS-Cloud Services in order to deliver an optimized experience for the end user.

Data Collected by XMS-Cloud

XMS-Cloud Services collect two types of data:

- Performance measurements to provide IT organizations visibility into the health of the network, like throughput, usage, or connection speeds.
- Non-measurable descriptive attributes, which add context to the performance measurements to help troubleshoot the problem, like MAC address, device name, user name, application name, etc.

XMS-Cloud collects performance measurements and attributes (collectively, "**Network Management Data**") in three areas: applications, devices and users.

Category	Collected Data
Applications	XMS-Cloud identifies applications used on the Wi-Fi network XMS-Cloud monitors: (a) the usage of these applications and (b) the top users of these applications
Devices	Device type and system information such as Windows, Mac, etc. Hostname, MAC address and IP address Signal strength, connection speeds, Wi-Fi bands, channels Errors metrics
Users	User name Location of user devices on the customer-uploaded floor map Guest user data as enabled by the customer (e.g. phone numbers, public social media demographics, email address) (collectively, "**EasyPass Guest Data**")

Location of Collected Data

All Network Management Data collected by XMS-Cloud Services resides on servers hosted in the United States.

Data Polling

Statistical data is polled from access points on a periodic basis that varies based on the nature of the data. Client statistics are polled as frequently as every 30 seconds. All polled statistical data is sent to XMS-Cloud over a secure tunnel that is encrypted with SSL/TLS.

Data Backup

Network Management Data is backed up daily and such back-ups may contain historical data dating back to initial deployment. Statistical data is backed up five (5) times per week.

Secure Data Transmission

Network Management Data and statistical data collected from access points is transmitted to XMS-Cloud using encrypted industry standard protocols (https over SSL/TLS).

The XMS-Cloud Services separate Network Management Data from user data (i.e. web browsing, internal applications, etc.) providing a level of traffic segregation while keeping user data secure on the LAN. User data does not flow through XMS-Cloud but instead flows directly to its destination on the LAN or across the WAN.

riverbed®

Duration of Data Retention in XMS-Cloud

Network Management Data and statistical data is retained in raw form for thirty (30) days after which only aggregated data is stored along with associated device information for auditing, reporting and compliance purposes for up to a year. Such data may also be used for disaster recovery and service restoration.

Customers have the option to delete EasyPass Guest Data within the XMS-Cloud management console.

Restricted Access to Data

XMS-Cloud assigns privileges to users according to the principle of least privilege. We give users the minimum access required for them to perform their tasks according to that role. For details, refer to Administrative Access section in this document. Customers can send REST API queries to directly extract and analyze XMS-Cloud data without accessing XMS-Cloud dashboards. Customers can combine the data with other data sources if needed, or transform it as required, then view it in Microsoft Excel, Power BI, or other customer-owned data applications.

Controlled Data Sharing with Third Party

Riverbed uses the Network Management Data to deliver superior performance to end users. Under no circumstances does Riverbed shares this data with third parties unless a customer has authorized that certain data be shared through application programming interfaces (APIs) or other means. Customers have the ability to mask certain information such as hashed MAC addresses when sharing data with third parties. We implement standards based JSON APIs which use SSL/TLS to encrypt data in transit.

CONTACT

If you have a specific privacy-related question, please contact rvbd-privacy@riverbed.com

RESOURCES

Additional resources are available at www.riverbed.com/privacy.