ON SIGHT

WHITE PAPER

Librestream Security Overview

July 2016

LIBRESTREAM

Table of Contents

Document Revision
Librestream
Security Overview
Doc #: 400277-01
July 2016

Security Overview

The confidentiality, integrity, and availability of customer information are vital to Librestream's business operations and success. The Onsight mobile video collaboration system includes a range of security provisions to safeguard and control content.
Librestream also takes a multi-layered approach to protect customer information through constant monitoring, review and updates to the applications, hosted systems, and processes to meet the growing demands and challenges of security. This approach includes the following components.

Use of Secure data centers

The hosted service is collocated in dedicated spaces at the high availability Amazon Web Services (AWS) and Rackspace data centers. This infrastructure is designed and managed according to security best practices as well as a variety of security compliance standards. With both data centers, customers can be assured that Librestream has built the web architecture on top of some of the most secure computing infrastructure in the world.
These facilities provide carrier-level support, including:

- Physical security and access control
- Environmental controls
- Fire detection and suppression
- Power Redundancy
- Secure Network Architecture
- Transmission Protection
- Automated Backup

Security Monitoring, Internal Testing and Assessments

The Information Security group constantly monitors notification from various sources and alerts from internal systems to identify and manage threats.
Librestream tests all code for security vulnerabilities before release and regularly scans the network and systems for the following:

- Application vulnerability threat assessments
- Network vulnerability threat assessments
- Selected penetration testing and code review
- Security control framework review and testing

Penetration Testing Procedures

The Onsight servers are subjected to network penetration testing procedures on a regular monthly basis using the Nessus Vulnerability Scan software. Every Server Instance type is mirrored and then used as the target for security scanning.
A designated Engineer is responsible for ensuring that the scans are performed as per documented work instructions as well as verifying that that the scan process itself is sufficiently complete and effective.

Scan Results and Risk Mitigation

Scan results are reviewed by the Engineer once the scan is complete. If the scan results identify a new or unknown risk, the results are logged in the internal issue tracking system and reviewed by the Software Engineering security panel. The Software Engineering group is responsible for addressing identified issues.
If patches are required to mitigate risks, they shall be scheduled according to risk severity and in a manner as to minimize service outages.

Solutions shall be implemented if vulnerabilities are discovered with a rating of 'Medium' or higher, as defined in the Nessus Report.

Secure transmission and sessions

All components, including Librestream's Onsight video endpoints, can be centrally configured and controlled to enforce security policies over transmission media. The supported security measures include:

- Cloud connectivity supports access via HTTPS using Secure Sockets Layer (SSL), a cryptographic protocol that is designed to protect against eavesdropping, tampering, and message forgery.
- SIP-TLS signaling encryption to secure call setup between endpoints
- AES128 bit media encryption to provide end to end security over the Onsight content.
- Privacy mode to restrict the ability to take pictures or record sessions
- Wireless security protocols for WLAN network and 802.1x authentication such as WPA2-PSK and PEAP-GTC with certificate support
- Central management tools to configure and enforce these security policies

Disaster Recovery

There are many potential disruptive threats which could occur at any time and affect the normal business process. Librestream has considered a wide range of potential threats with the focus being on the level of business disruption which could arise from each type of disaster. The internal disaster recovery plans include policies and procedures for technology disaster recovery, as well as process-level plans for recovering critical technology platforms and infrastructure.

In the event of a potential disaster/emergency situation, the Disaster Recovery Team shall decide on the appropriate actions to be taken, as guided by the full internal Disaster Recovery document.
The Disaster Recovery Team is responsible for:

- Responding immediately to a potential disaster/emergency situation and calling emergency services (fire, ambulance, police) if appropriate
- Assessing the extent of the disaster and its impact on business activities, facilities, services, etc.
- Deciding which elements of this procedure are required for the situation
- Ensuring necessary personnel are notified and updating a recorded message to relay information to employees as it is available
- Managing the resources necessary and allocating responsibilities and activities as required to restore/maintain vital services
- Documenting actions taken and ensuring that records are maintained

Periodic disaster recovery tests verify the projected recovery times and the integrity of the customer data. A full verification of disaster recovery processes is conducted annually at a minimum.

Backup and Recovery

In the event of a disaster/emergency situation where Librestream business systems and/or data are affected, Librestream shall:

- Establish an emergency level of service
- Restore critical services
- Recover to normal operation

At the secure data centers, the back-up and recovery process includes:

- All data are backed up to tape at each data center, on a rotating schedule of incremental and full backups
- The backups are cloned over secure links to a secure tape archive
- Tapes are not transported offsite and are securely destroyed when retired

For More Information

Please contact Librestream at information@librestream.com.