CYBERSECURITY

A CRITICAL REQUIREMENT FOR ENTERPRISE AR

We built this whitepaper to help security teams understand Librestream's approach to security throughout the entire partnership.
For further support, please contact info@librestream.com

LIBRESTREAM

CYBERSECUITY,
THE STATUS QUO
IS LONGER
ACCEPTABLE.

Contents

01

Introduction

The global average cost of a data breach in 2020 is **$3.86 million**.

Cybersecurity is an ongoing, evolving threat that impacts every industry causing loss of time, money and reputation. The global average cost of a data breach in 2020 is $3.86 million, according to Cost of a Data Breach Report 2020, from IBM. It takes an average of 280 days to identify and mitigate a breach, time during which your business is constrained and putting out fires. Keeping data as safe as possible and auditing safety protocol frequently and proactively are essential strategies to prevent such attacks.

Security touches every aspect of software — its development, infrastructure, use, and maintenance. Integrating security into the software development lifecycle (SDLC) means understanding who uses the software and how; understanding and regulating what kinds of data is stored where; and how data makes its way through networks. The alphabet soup of regulations that software-as-a-service (SaaS) companies must demonstrate compliance with, necessitates security as part of the software DNA, instead of a mere afterthought.

01

For example, with software like Onsight from Librestream, data needs to be protected no matter where it is being captured, used or stored: whether in the cloud; passing through the network, on premise or as part of the application on a device. This translates to oversight of:

+ Access points and people
+ Network security
+ Data processing and storage
+ Software development
+ Data governance and privacy

Industry standards and best practices dictate what security looks like in and across each of these compartments. Enterprises need to adopt a holistic approach to meet their security requirements.

Librestream addresses security in each of these compartments — and beyond.

02

Oversight of Access Points and People

By 2022, more than 75% of smartphones used in the enterprise will be because of a BYOD policy.

Librestream's signature Onsight software can be accessed through mobile and wearable devices, which means related cybersecurity is a must. The Bring-Your-Own-Device (BYOD) to work market is growing at a rapid clip. By 2022, more than 75% of smartphones used in the enterprise will be because of a BYOD policy. The increasing number of mobile devices to access software apps and transfer (and access) data make them vulnerable endpoints. Librestream provides a platform for robust IT-supervised mobile device management (MDM) procedures.

Restricting access to data through identity and access management (IAM) also enables software companies to keep a strict eye on security. IAM confers one digital identity per individual which then allows for tracking through a user's access lifecycle. IAM enables compliance with company and government cybersecurity protocols by delivering a transparent breadcrumb pattern of usage.

02

Librestream's IAM policies include restrictions to information security management systems and managing and storing the identity of all personnel who have access to the IT infrastructure. Librestream users can implement single sign-on (SSO) controls — the user works with one set of name and password for multiple applications — which conforms to SAMLv2.0. SAML (security assertion markup language) is an open standard that helps verify user credentials.

Librestream enables customers to set additional access controls to manage users easily. IT administration can also centrally control password complexity and other details for sign-in access. Finally, Librestream also uses a comprehensive encryption key management solution as part of data security strategies.

"Librestream has taken security seriously and they encrypt everything that is transmitted and something we took into account [When deciding on technology partner]"

– **DIRECTOR OF INNOVATION AND KNOWLEDGE TRANSFER** (LEADING ENERGY COMPANY)

ACCESS CONTROLS

PASSWORD CONTROLS

ENCRYPTION KEY MANAGEMENT

03

Oversight of Data Networks

No matter what type of information you transport (voice, video, data), network security is paramount.

Transport Layer Security (TLS) plays a key role in security of data in transit by encrypting network traffic. Voice over IP (VoIP), Session Initiation Protocol (SIP) and media are all encrypted using TLS. Librestream complies with TLS 1.2 to maintain security of data packets over networks. In addition, Librestream provides encryption algorithms such as AES so customers can protect data as it moves through the Internet.

Additional supported network security measures from Librestream include:

+ Cloud connectivity supports access via HTTPS with SHA-2 Certificates, to protect against eavesdropping, tampering, and message forgery;
+ SIP-TLS AES signaling encryption to secure call setup between endpoints;
+ Media encryption (AES) to provide end to end security for Onsight video, audio and data streams; and
+ Privacy mode to restrict the ability to take pictures or record sessions through client policies, which work in conjunction with mobile device privacy settings.

04

Oversight of Data Processing and Storage

With the Onsight platform, customers can choose to use software on-premise and in the cloud. For example, defense agencies and contractors often choose Librestream's on-premise deployment to meet their strict requirements.

Using an app or software program invariably means using application programming interfaces (APIs). Coders rely on these to make their lives easier and companies use them to transfer data. Secure APIs, i.e. application and interface security, are key to data safety as it is routed and processed by third-party applications. Assigning quotas to how often APIs can be called and detecting when these calls are overused is a good way of detecting spambots. API gateways determine which software gets access, analyze patterns of use, and enforce traffic rules. Librestream software conforms to industry standards like Build Security in Maturity Model (BISMM) benchmarks, ACS, and NIST to continuously discover and correct security vulnerabilities in API calls.

04

Librestream uses dynamic load balancing and monitored alarms to detect and respond to network-based attacks in addition to using host-based intrusion prevention systems and antimalware and antivirus programs. In addition, Librestream logs and alerts of any changes made to virtual machine images. Only authorized personnel can access audit logs.

Librestream's hosted services run on AWS and Azure cloud services which manage data use and capacity. Industry standards like ISO 27001 regulate data security protocols in such instances. Security vulnerability assessment tools, such as the third-party Veracode, accommodate virtualization techniques and understand how to scan for weaknesses.

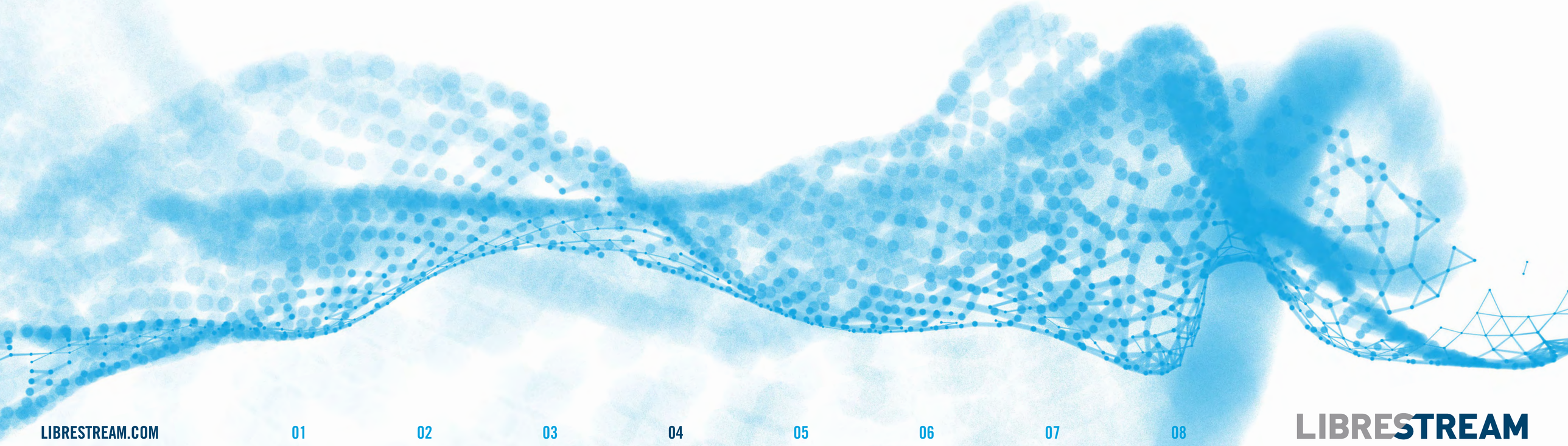
Data centers and supply chains must be secure both physically and electronically. Supply chain challenges sometimes surface during modifications to software and hardware, which expose vulnerabilities in key links.

Librestream works with supply chain partners to correct data quality errors and minimize associated risk. Personnel throughout the supply chain only access data based on assigned duties.

04

The security of data while in storage also comes into play. Librestream provides multiple approaches and options to customers for storage of pictures, data or videos captured using Onsight. Customers can securely store content on Librestream's Workspace knowledge management tool within a Librestream hosted solution or as an On Premise deployment. They can also use Librestream's Content API to store content directly in an existing content system. Customers can access a comprehensive privacy notice about how Librestream Onsight works with their data.

Librestream also enables effective e-discovery and cloud forensics techniques that allow for effective gathering of usable data in case of a security breach.



05

Oversight of Software Development

Librestream conducts thorough reviews for software vulnerabilities before launching.

Today's competitive, fast-paced and often agile software development lifecycles might inadvertently sideline security concerns especially if developers view security standards as constraints to deadlines and creativity. Security needs to be baked into the SDLC to eliminate this outcome. Librestream enforces application and interface security processes by incorporating industry standards for software development: Build Security in Maturity Model (BSIMM) benchmarks; Open Group ACS Trusted Technology Provider Framework, and NIST. Librestream's data security architecture conforms to industry standards.

To ensure that software meets cybersecurity standards, Librestream conducts application static binary analysis scans, which evaluate code thoroughly for vulnerabilities before release. In addition to conducting manual source-code analysis, an automated source code analysis tool detects code security defects prior to release. Penetration testing are intentional attacks designed to expose security vulnerabilities, if any, in software.

05

The tests check for weaknesses in the software as well as APIs that the software interacts with. Librestream conducts third-party manual penetration testing and weekly vulnerability scans to ensure compliance. Librestream also verifies that all software suppliers abide by industry standards for SDLC security.

In addition to the compartments discussed above, cybersecurity involves company-wide strategies for data governance and a threat and vulnerability management strategy.

06

Overall Data Governance

80% of organizations worldwide will face modern privacy and data protection requirements.

Gartner predicts that through 2022, privacy-driven spending on compliance tooling will increase to more than $8 billion worldwide, and by 2024, more than 80% of organizations worldwide will face modern privacy and data protection requirements.

Industry standards and government mandates (GDPR, NIST and more) provide directions for gathering and secure handling of data. Cybersecurity is expected to become even more challenging as data streams in from field equipment (operational technology, OT) in addition to standard IT avenues. Industry-specific standards (such as MISRA for safety-critical industries such as automotive) further complicate the picture.

Overall data governance starts with a comprehensive threat and vulnerability management strategy, which continuously identifies and assesses weaknesses in endpoints and overall software coding and execution. Since no solution can be 100% cybersecure, evaluating a company's appetite for risk and understanding how to manage it, is also part of the cybersecurity plan.

06

Data governance must meet compliance standards and affects not just coding but all other departments like HR, customer service, supply chains and more.

By no means a comprehensive list, a few of these compliance standards incorporated by Librestream include:

+ ISO 27001, which protects data from unintentional distribution and access.
+ ISO/IEC 27018 which specifically applies to data handling and storage in the cloud, especially of personally identifiable information (PII).
+ The General Data Protection Regulation (GDPR) places strict guidelines for obtaining customer content for data gathering and processing and breach notification among other stipulations.
+ National Institute of Standards and Technology (NIST). The U.S. based cybersecurity framework is being embraced by global companies as it lays out specific procedures for identifying and addressing cybersecurity risks and incidents.

Third-party independent audits have certified Librestream as ISO 27001 and ISO 27018-compliant. Librestream is GDPR compliant through centralized privacy and content controls. For example, Librestream's custom messaging feature delivers the ability to enable a custom message that must be accepted by the user as part of the login process. The customer controls the text and how it relates to privacy in the message. Librestream also share results of data protection impact assessments.

07

Business Continuity and Operational Resilience

Business continuity and disaster recovery plans account for disruptions in service caused by variety of circumstances that range from flooding and hurricanes to power outages.

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. Internal disaster recovery plans include policies and procedures for technology disaster recovery, as well as process-level plans for retrieving critical technology platforms and infrastructure. In the event of a potential disaster/emergency situation, the disaster recovery team decides on the appropriate actions to be taken, as outlined in the internal Disaster Recovery document.

07

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.

Librestream backs up all data up to tape at each data center, on a rotating schedule of incremental and full backups in multiple regions.

08

Ongoing Oversight

SaaS providers such as Librestream must balance advanced, open features with significant and important cybersecurity concerns. A comprehensive threat detection and remediation strategy rooted in gathering, working with and storing of data is key. Security-first software development and disaster resilience also help keep cybersecurity needs as proactive concerns rather than reactive ones. Periodic reviews of cybersecurity plans are important as the nature of threats and corresponding solutions keeps changing over time.

Librestream understands that the costs of a data breach are severe; you can't afford to not stay ahead.

BACK TO TOP ↑

For more information on the Onsight platform visit **LIBRESTREAM.COM**

LIBRESTREAM