LiveLitigation

This document outlines the LiveLitigation infrastructure design from a security standpoint and references the relevant parts of application security that interface with it.

Application / User Data

LiveLitigation is a web application accessed via the user's web browser over HTTPS – TLS 1.3/1.2/1.1 supported.

LiveLitigation customers have username/password authentication to access their online account. Passwords are stored as cryptographic hash.

LiveLitigation customers have optional 2-factor authentication via Twilio SMS service that can be enabled in their account.

LiveLitigation customers control access to LiveLitigation events/sessions. Customers create events and add individual attendees to each event. Each attendee is provided a unique 12-digit key that controls their access to the event, which can be revoked at any time by the customer.

LiveLitigation stores a very limited amount of personal data from customers, including Name, Email, and Phone Number. Customers can change, remove, or request deletion of their data at any time. LiveLitigation does not sell customer data under any circumstance (see Privacy Policy).

Streaming

LiveLitigation video and audio streaming utilizes WebRTC. Some notes about WebRTC security:

1. Encryption: Encryption is built in to WebRTC and is mandatory for all components including signaling. Transmission is encrypted using standards supported by compatible web browsers.
2. Encryption is handled using Data Transport Layer Security (DTLS) which is based on the TLS standard and is designed to prevent eavesdropping, tampering, and message forgery.
3. Additional encryption is handled by Secure Real-Time Protocol (SRTP) which protects real-time streaming data (such as video and audio) and is intended to provide encryption, message authentication and integrity, and replay attack protection.
4. WebRTC provides secure signaling channels for voice and data communication over web sockets.
5. Access to camera and microphone devices is handled directly by the user's web browser and explicit permission must be granted by the user before camera or microphone data can be accessed by the web browser. The user remains in control of camera and

microphone access at all times, and can disable access to camera and microphone devices using the controls provided by their web browser.

Exhibits

LiveLitigation exhibits are uploaded/downloaded over HTTPS and stored in encrypted storage volumes in Amazon S3. Access to exhibit files is limited to the end users who upload the files. Each end user sets a username and password before accessing their exhibits.

Each end user must authenticate to access exhibits. When connecting to a LiveLitigation event, each end user must supply their unique event key, followed by their personal username and password if they wish to access their previously uploaded exhibits. Deletion of exhibit files is handled by the end user.

Servers/Infrastructure

LiveLitigation is hosted on Amazon Web Services (AWS) in region us-west-2 (primary) with disaster recovery located in region us-east-1.
LiveLitigation utilizes the following AWS services:

1. EC2: Hosting of the LiveLitigation web application and media servers.
2. VPC: Virtual Private Cloud for secure exchange between services.
3. EBS: Encrypted filesystem and file storage for application data and user data.
4. KMS: Key management for cryptographic keys.
5. SES: Email invitations sent by customers to end users.
6. S3: Encrypted data storage.

LiveLitigation also uses various AWS servers for internal monitoring and access control including:

1. IAM: role based access to services.
2. CloudWatch: detailed monitoring of infrastructure performance and stability.
3. Inspector: regular vulnerability and security scans to compliment regular maintenance.

AWS services meet various security compliance standards such as FIPS 140-2 and FedRAMP: https://aws.amazon.com/compliance/fedramp/

HIPAA Compliance

LiveLitigation uses HIPAA-eligible services for all hosting, data transmission and data storage. Within the HIPAA-eligible services, LiveLitigation uses modern TLS/SSL connections exclusively for all data in transit, and all data objects (data at rest) is stored on encrypted volumes.

Example HIPAA-eligible services (More Info):

- Amazon EC2
- Amazon Elastic Block Store
- Amazon S3
- AWS WAF – Web Application Firewall
- Amazon Inspector
- AWS Lambda
- Amazon ElastiCache for Redis
- Amazon CloudWatch