Frame.io Security Overview

Adobe

Adobe Security

At Adobe, we know the security of your digital experience is important. Security practices are deeply ingrained into our internal software development, operations processes, and tools. These practices are strictly followed by our cross-functional teams to help prevent, detect, and respond to incidents in an expedient manner. We keep up to date with the latest threats and vulnerabilities through our collaborative work with partners, leading researchers, security research institutions, and other industry organizations. We regularly incorporate advanced security techniques into the products and services we offer.

This paper describes the defense-in-depth approach and security procedures implemented by Adobe to secure Frame.io and its associated data.

About Frame.io

Frame.io is the leading collaboration and feedback platform for professional video creators. With the Frame.io cloud-based platform, video producers and editors can securely upload, review, and share media, enabling every team member to share files, comment directly on clips in real time, draw directly on video, and compare different versions or edits of a clip side by side.

Adobe Frame.io Solution Architecture

The Adobe Frame.io solution is comprised of the following four (4) components:

- Frame.io Clients – Enable users to upload, edit, and consume various types of media (e.g., MP4, JPEG, TXT, PDF). Upload clients include the Frame.io web app, the Frame.io iOS app, the Frame.io Transfer app, and supported NLEs (non-linear editors, e.g., Adobe Premiere Pro). Consumption clients include the Frame.io web app, the Frame.io iOS app, the Frame.io tvOS app, and supported NLEs.
- Frame.io API – Provides the interface for all uploads of media from any media source to the Frame.io solution.
- Frame.io Media Ingest Pipeline – Analyzes, generates metadata, and prepares uploaded media files using a transcoding service designed specifically for the type of media.
- Frame.io Streaming Service – Prepares media for delivery by applying content security and segmenting audio/video for the best viewer experience. Content is packaged into HLS (HTTP Live Streaming) format and delivered securely over HTTPS.

Original media files uploaded by content creators and transcoded media files generated by Frame.io are stored independently from each other in a leading cloud storage provider.

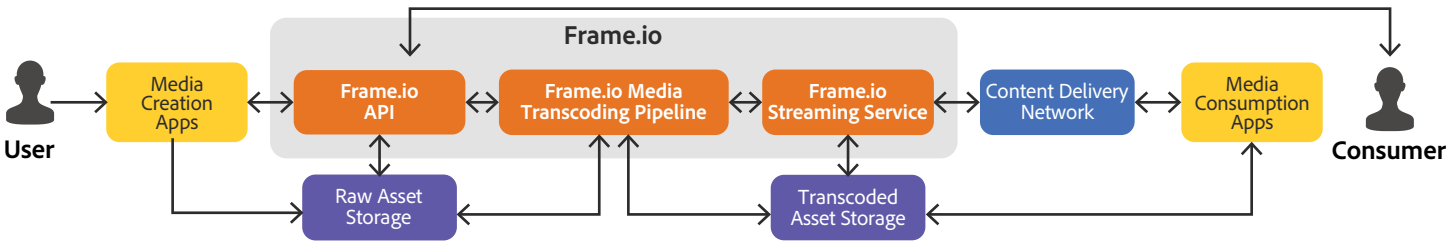

Figure 1: Frame.io Solution Architecture Diagram

Adobe Frame.io Security Architecture and Data Flow

The following steps illustrate how data flows through the Frame.io solution in a typical user interaction:

Media Uploading and Transcoding

1. The user opens their chosen Frame.io client and authenticates themselves using one of the supported authentication methods.
2. The client application executes a PUT request to the Frame.io API's upload endpoint with basic file information and receives a signed URL in response.
3. The client application then uses the signed URL to upload the content to secure cloud storage over HTTPS.
4. The Frame.io Media Ingest Pipeline then analyzes the uploaded file and creates "proxy" files (images and/or video at multiple resolutions).
5. Generated proxy files are stored in a separate cloud storage location.
6. The Media Ingest Pipeline notifies the Frame.io API upon completion of the proxy generation process.

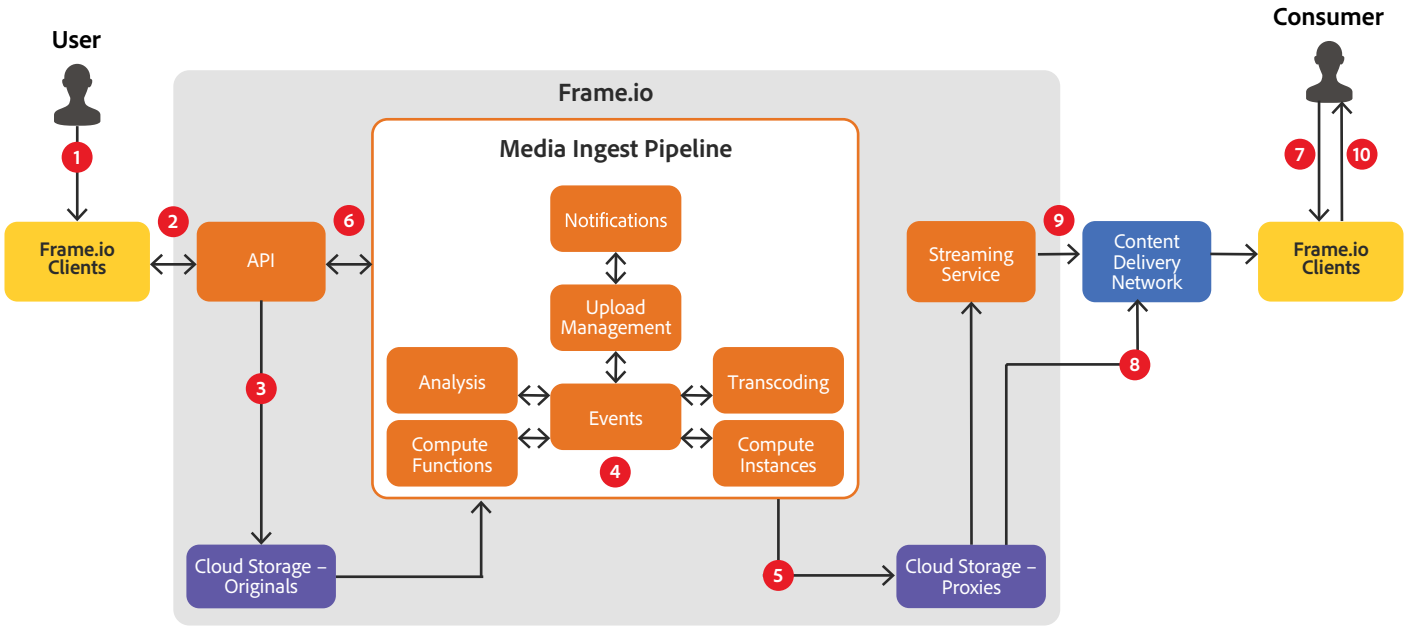

Figure 2: Frame.io Data Flow Diagram

Media Consumption

7. The user launches the Frame.io website or other Frame.io client.
8. The Frame.io API authenticates the user as needed and delivers appropriately signed URLs to content, which is delivered to the user via CDN.
9. If just-in-time content security, such as Watermark ID or DRM (Digital Rights Management), is required, the content will pass through the Frame.io Streaming Service before being sent to the CDN for delivery.
10. The user can now view, edit, comment, or update the content using their Frame.io client.

Data Encryption

All data in transit is encrypted using AES 128 GCM over TLS 1.2 and at rest using AES 256-bit key encryption.

Only communications over ports 80/443 are allowed within the Frame.io solution.

Security Features for Enterprise Customers

Digital Rights Management (DRM)

DRM, a media protection scheme that leverages built-in OS and browser-based technologies to manage a license and key exchange for enhanced security, is available to customers with a Frame.io enterprise license. Frame.io applies DRM encryption in the media consumption workflow (see Figure 2 above), after video proxies are generated and placed into cloud storage.

When the user enables DRM, the Frame.io Streaming Service applies unique, per-asset DRM encryption to the audio and video content before it packages the HLS manifests and segments for delivery through the CDN. Signed URLs with limited expiry times are supplied to Frame.io clients so that the video player can execute a license exchange and media decryption inside the browser or mobile device's content decryption module.

Watermarking/Content Security

Customers with a Frame.io enterprise license may use built-in text-based watermarking to create an established record of authenticity for media content shared in the solution. Administrators can enable this functionality to create their own custom watermark, set its opacity, and choose where in the frame they want it to appear. Once configured, the watermark is automatically burned into any uploaded video or image file before the media content is stored.

For additional content security, enterprise customers can purchase the Watermark ID (WMID) session-based watermarking add-on, which offers a dynamic option for video security playback. When enabled within a shared link and any viewer presses play, Frame.io completes a real-time, on-demand transcode of the video with a configurable set of information, such as the viewer's email address, date and time, and IP address in each frame. Session-based watermarking occurs within the Frame.io Streaming Service and is compatible with DRM.

Frame.io User Authentication

Frame.io supports all authentication solutions that conform to the Security Assertion Markup Language 2.0 (SAML 2.0) standard for single sign-on (SSO). Once enabled, any user in the customer's domain(s) can use SSO to access Frame.io, as well as any of its integrations (e.g., Adobe Premiere Pro, Adobe After Effects).

Frame.io encrypts and stores all passwords as a one-way hash with salt, logs all user activities, and enforces password changes on all accounts every 90 days. Frame.io also enforces password complexity requirements on all accounts, disallows the use of previous passwords, and suspends the account after a set number of unsuccessful logins.

Two-Factor Authentication (2FA)

For an added layer of security, individual users may enable two-factor authentication (2FA) for their specific account. Administrators can also enforce 2FA for all users on the organization's Frame.io license. If an admin enforces 2FA, all users of Frame.io in that organization who do not already have 2FA enabled will receive an email notification advising them to enable it immediately. Users who do not enable 2FA within 24 hours will be logged out and required to enable 2FA next time they log in. Currently, Frame.io supports Google Authenticator and SMS verification.

Roles and Permissions

Frame.io uses the principle of least privilege access and role-based permissions to achieve stringent access control. Administrators use the Frame.io Admin UI to grant granular role-based permissions to users.

Frame.io Data Governance and Compliance

Frame.io is fully compliant with Trusted Partner Network (TPN), a joint venture between the MPAA (Motion Picture Association of America) and CDSA (Content Delivery and Security Association). TPN is a global, industry-wide television content protection initiative that provides a set of requirements and best practices designed to prevent leaks, breaches, and hacks of pre-released, high-value media content. TPN assessments are intended to provide large studios and enterprises that store material worldwide confidence in the security of their media.

Frame.io Hosting Locations

The Frame.io service infrastructure resides in the data center of a leading cloud service provider in the US-East (Virginia) region.

Segregation of Customer Data

Using a virtual private cloud (VPC), customer data remains logically separated from other tenants in the cloud. Customer data is further segregated in the Frame.io database by marking each data field with a unique customer identifier. Media files stored in cloud storage are tagged with these customer-specific identifiers.

Data within the VPC is protected behind access controls, role-based permissions, and a Web Application Firewall (WAF). Access to the Frame.io database and cloud storage use an AES-256 security key managed by the cloud provider's key management service, which provides an additional layer of control and security.

Adobe Security Program Overview

The integrated security program at Adobe is composed of five (5) centers of excellence, each of which constantly iterates and advances the ways we detect and prevent risk by leveraging new and emerging technologies, such as automation, AI, and machine learning.

Figure 3: The Five Security Centers of Excellence

The centers of excellence in the Adobe security program include:

- Application Security – Focuses on the security of our product code, conducts threat research, and implements bug bounty.
- Operational Security – Helps monitor and secure our systems, networks, and production cloud systems.
- Enterprise Security – Concentrates on secure access to and authentication for the Adobe corporate environment.
- Compliance – Oversees our security governance model, audit and compliance programs, and risk analysis; and
- Incident Response – Includes our 24x7 security operations center and threat responders.

Illustrative of our commitment to the security of our products and services, the centers of excellence report to the office of the Chief Security Officer (CSO), who coordinates all current security efforts and develops the vision for the future evolution of security at Adobe.

The Adobe Security Organization

Based on a platform of transparent, accountable, and informed decision-making, the Adobe security organization brings together the full range of security services under a single governance model. At a senior level, the CSO closely collaborates with the Chief Information Officer (CIO) and Chief Privacy Officer (CPO) to help ensure alignment on security strategy and operations.

In addition to the centers of excellence described above, Adobe embeds team members from legal, privacy, marketing, and PR in the security organization to help drive transparency and accountability in all security-related decisions.

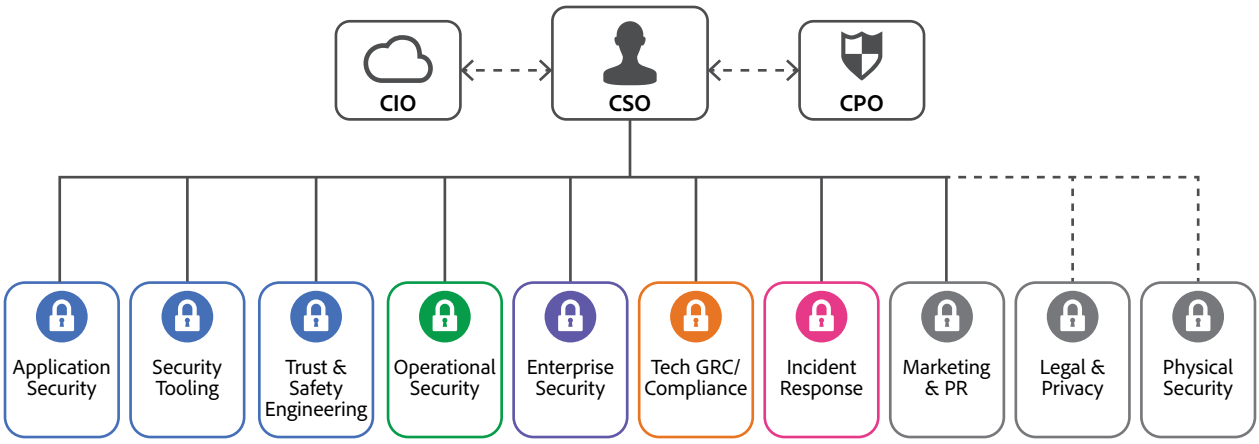

Figure 4: The Adobe Security Organization

As part of our company-wide culture of security, Adobe requires that every employee completes our security awareness and education training, which requires completion and re-certification on an annual basis, helping ensure that every employee contributes to protecting Adobe corporate assets as well as customer and employee data. On hire, our technical employees, including engineering and technical operations teams, are auto-enrolled in an in-depth 'martial arts'-styled training program, which is tailored to their specific roles. For more information on our culture of security and our training programs, please see the Adobe Security Culture white paper.

The Adobe Secure Product Lifecycle

Integrated into several stages of the product lifecycle—from design and development to quality assurance, testing, and deployment— the Adobe Secure Product Lifecycle (SPLC) is the foundation of all security at Adobe. A rigorous set of several hundred specific security activities spanning software development practices, processes, and tools, the Adobe SPLC defines clear, repeatable processes to help our development teams build security into our products and services and continuously evolves to incorporate the latest industry best practices.

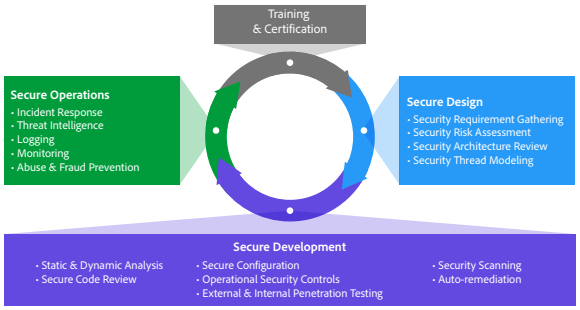

Figure 5: The Adobe Secure Product Lifecycle

Adobe maintains a published Secure Product Lifecycle Standard that is available for review upon request. More information about the components of the Adobe SPLC can be found in the Adobe Application Security Overview.

Adobe Application Security

At Adobe, building applications in a "secure by default" manner begins with the Adobe Application Security Stack. Combining clear, repeatable processes based on established research and experience with automation that helps ensure consistent application of security controls, the Adobe Application Security Stack helps improve developer efficiency and minimize the risk of security mistakes. Using tested and pre-approved secure coding blocks that eliminate the need to code commonly used patterns and blocks from scratch, developers can focus on their area of expertise while knowing their code is secure. Together with testing, specialized tooling, and monitoring, the Adobe Application Security Stack helps software developers to create secure code by default.

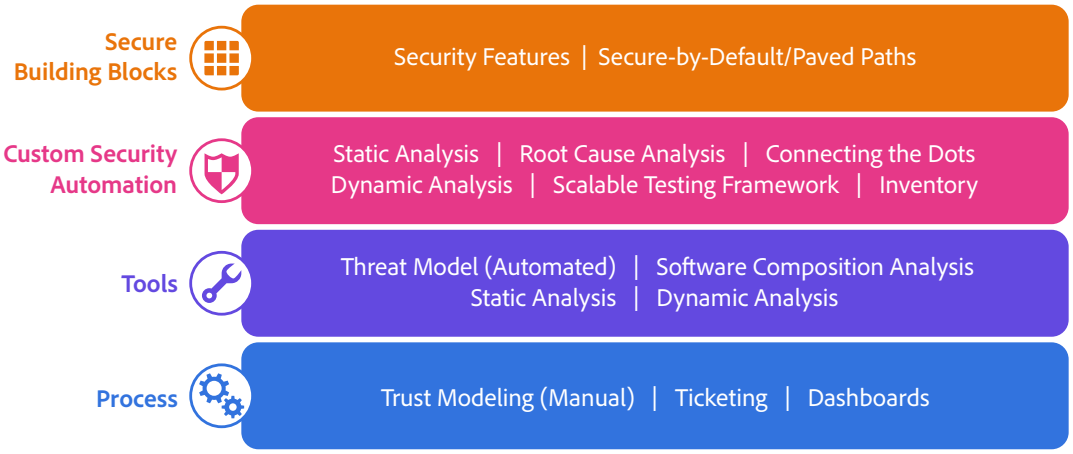

Figure 6: The Adobe Application Security Stack

Adobe also maintains several published standards covering application security, including those for work specific to our use of public cloud infrastructure. These standards are available for view upon request. For more information on Adobe application security, please see the Adobe Application Security Overview.

Adobe Operational Security

To help ensure that all Adobe products and services are designed from inception with security best practices in mind, the operational security team created the Adobe Operational Security Stack (OSS). The OSS is a consolidated set of tools that help product developers and engineers improve their security posture and reduce risk to both Adobe and our customers while also helping drive Adobe-wide adherence to compliance, privacy, and other governance frameworks.

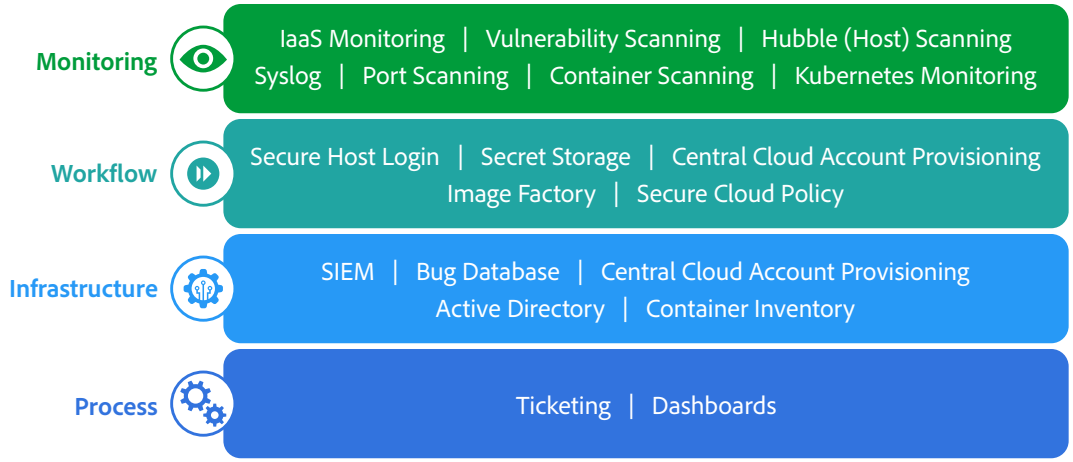

Figure 7: The Adobe Operational Security Stack

Adobe maintains several published standards covering our ongoing cloud operations that are available for view upon request. For a detailed description of the Adobe OSS and the specific tools used throughout Adobe, please see the Adobe Operational Security Overview.

Adobe Enterprise Security

In addition to securing our products and services as well as our cloud hosting operations, Adobe also employs a variety of internal security controls to help ensure the security of our internal networks and systems, physical corporate locations, employees, and our customers' data. For more information on our enterprise security controls and standards we have developed for these controls, please see the Adobe Enterprise Security Overview.

Adobe Compliance

Adobe products and services either meet applicable legal standards or can be used in a way that enables customers to help meet their legal obligations related to the use of service providers. Customers maintain control over their documents, data, and workflows. Adobe also maintains compliance training and related standards that are available for review upon request. For more information on the Adobe CCF and key certifications, please see the Adobe Compliance, Certifications, and Standards List.

Incident Response

Adobe strives to ensure that its risk and vulnerability management, incident response, mitigation, and resolution processes are nimble and accurate. We continuously monitor the threat landscape, share knowledge with security experts around the world, swiftly resolve incidents when they occur, and feed this information back to our development teams to help achieve the highest levels of security for all Adobe products and services.

We also maintain internal standards for incident response and vulnerability management that are available for view upon request. For more details about Adobe's incident response and notification process, please see the Adobe Incident Response Overview.

Business Continuity and Disaster Recovery

The Adobe Business Continuity and Disaster Recovery (BCDR) Program is composed of the Adobe Corporate Business Continuity Plan (BCP) and product-specific Disaster Recovery (DR) Plans, both of which help ensure the continued availability and delivery of Adobe products and services. Our ISO 22301-certified BCDR Program enhances our ability to respond to, mitigate, and recover from the impacts of unexpected disruptions. More information can be found in the Adobe Business Continuity and Disaster Recovery Overview.

Conclusion

The proactive approach to security and stringent procedures described in this paper help protect the security of Frame.io and your confidential data. At Adobe, we take the security of your digital experience data very seriously and we continuously monitor the evolving threat landscape to try to stay ahead of malicious activities and help ensure the security of our customers' data.

For more information about Adobe security, please go to the Adobe Trust Center.

Information in this document is subject to change without notice. For more information on Adobe solutions and controls, please contact your Adobe sales representative.