Adobe

SECURITY OVERVIEW

Adobe Frame.io

April 2026

About Adobe Frame.io Enterprise

Adobe Frame.io Enterprise provides a flexible, quick and intuitive platform that empowers creative teams and their stakeholders to organize, review and manage work-in-progress assets, and orchestrate the people and processes supporting them.

No matter the workflow—whether simple or complex—Adobe Frame.io Enterprise allows you to build it with ease and deliver it faster. Anchored in an all-new, powerful metadata framework, teams of any size can now use Adobe Frame.io Enterprise to customize any creative workflow centered on media assets and manage the people and processes supporting them.

Adobe Frame.io Enterprise components

Adobe Frame.io Enterprise is comprised of the following key components:

- **Frame.io Clients** – Enable users to upload, edit, and consume various types of media (for example: MP4, JPEG, TXT, PDF).
    - **Upload clients** – Include the Frame.io web app, the Frame.io iOS app, the Frame.io Transfer app, Camera 2 Cloud (C2C) devices, supported non-linear editors (NLEs) such as Adobe Premiere Pro, and any Frame.io integration.
    - **Consumption clients** – Include the Frame.io web app, the Frame.io iOS app, the Frame.io tvOS app, and supported NLEs.
- **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. Content is packaged into HTTP Live Streaming (HLS) format and delivered securely over HTTPS.
- **Frame.io Application Programming Interface (API)** – Allows customers to extend their workflows into the rest of their toolchain or into a custom application using REST APIs.

User authentication

Access requests to Frame.io Enterprise are authenticated using Adobe Identity Management Services (IMS). For all supported authentication methods, see the Frame.io V4 API documentation.

Frame.io Enterprise provides a role-based access control model that enforces the principle of least privilege across accounts, workspaces, projects, and folders. Administrators can assign granular permissions defining who can view, comment on, edit, download, or share content at multiple levels of the hierarchy. Permissions can be managed programmatically via the Frame.io APIs.

Single Sign-On (SSO) and Multi-Factor Authentication (MFA)

Frame.io Enterprise supports Single Sign-On (SSO) based on SAML 2.0, enabling organizations to integrate with their identity providers and enforce centralized authentication policies. Frame.io Enterprise also supports mandatory Multi-Factor Authentication (MFA), requiring users to verify their identity with an additional factor beyond a password. Individual users may enable 2FA on their account; administrators can enforce 2FA across the organization's Frame.io license. Frame.io Enterprise supports Google Authenticator and SMS verification.

Adobe-managed authentication

Frame.io Enterprise integrates with Adobe's enterprise identity infrastructure, enabling centralized user lifecycle management and authorization through the Adobe Admin Console. Organizations can manage Frame.io user entitlements alongside other Adobe products, enforce SSO, and align access policies with corporate identity providers and directory services.

Data encryption

- **In Transit** – All data is encrypted in transit over HTTPS using TLS 1.2 or greater.
- **At Rest** – All data stored within the Frame.io platform—including media assets, metadata, application data, and account information—is encrypted at rest using AES 256-bit encryption.

For customers leveraging Storage Connect (Bring Your Own Storage), original media assets remain within the customer-designated cloud storage environment, where encryption at-rest and key management are governed by the customer's own infrastructure policies. Frame.io connects to customer-designated storage over encrypted transport channels to facilitate proxy generation, playback, and collaboration workflows.

Adobe Frame.io security architecture and data flow narrative

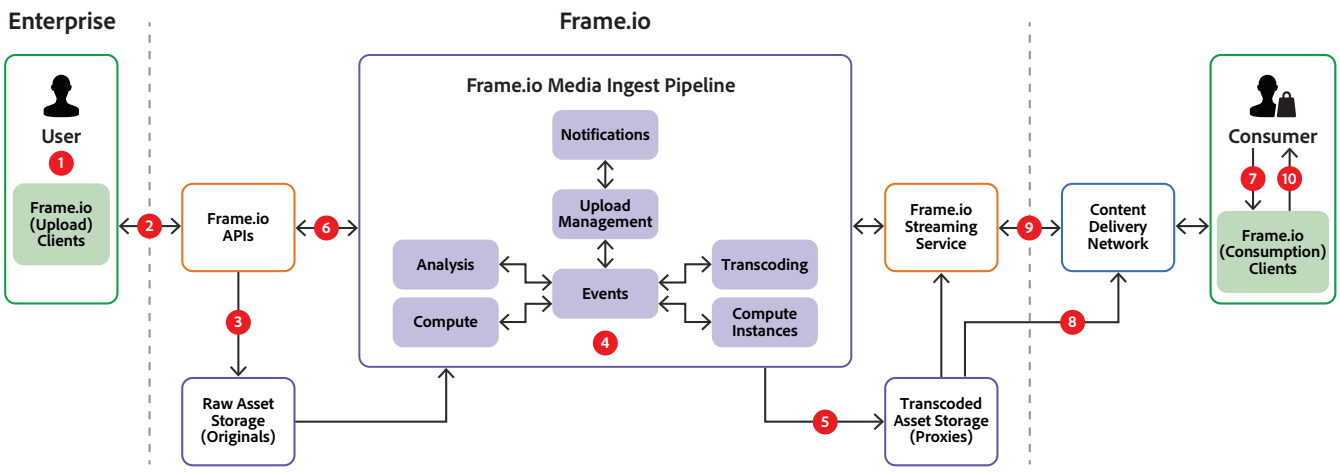

Figure 1: Frame.io Security Architecture and data flow diagram

Media uploading and transcoding data flow narrative

Step 1: The user opens their chosen Frame.io client and authenticates themselves using one of the supported authentication methods.

Step 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.

Step 3: The client application uses the signed URL to upload the content to secure cloud storage (AWS S3) over HTTPS.

Step 4: The Frame.io Media Ingest Pipeline analyzes the uploaded file and creates proxy files (images and/or video at multiple resolutions).

Step 5: The generated proxy files are stored in a separate AWS S3 bucket.

Step 6: The Media Ingest Pipeline notifies the Frame.io API upon completion of the proxy generation process.

Media consumption data flow narrative

Step 7: The user launches the Frame.io website or other Frame.io client.

Step 8: The Frame.io API authenticates the user as needed and delivers appropriately signed URLs to content, which is delivered to the user through the Content Delivery Network (CDN).

Step 9: If just-in-time content security, such as Session-based Watermarking, Forensic Watermarking, or Digital Rights Management (DRM), is required, the content will pass through the Frame.io Streaming Service before being sent to the CDN for delivery.

Step 10: The user views, edits, comments, or updates the content in their Frame.io client.

Other enterprise security controls

Restricted projects and restricted folders

To support compartmentalized collaboration and protect sensitive intellectual property, Frame.io Enterprise enables restricted projects and restricted folders that isolate content from broader visibility. Restricted projects are accessible only to explicitly invited members, creating a private area for highly confidential workflows. Within projects, restricted folders allow further segmentation of assets so that only selected users can see or interact with specific materials. These controls help enterprises manage content visibility by client, team, or confidentiality level without exposing sensitive material to unintended audiences, while still providing centralized administrative oversight.

Secure sharing

Frame.io Enterprise enhances external collaboration with secure sharing controls that extend governance beyond the entitled user base. Content owners can enable secure sharing which requires authentication before access, allows for restricting link availability to designated email addresses or approved domains, and manage or revoke shared links at any time. These protections help ensure that previews and review workflows remain confined to intended recipients, supporting enterprise policies around external collaboration without disrupting the creativity and agility teams rely on for iterative feedback.

Watermarking: Static, session-based, and forensic

Frame.io Enterprise provides multiple watermarking techniques to deter unauthorized distribution and support accountability across review workflows. Static watermarking applies burned in text visual identifiers—such as project names, account names, or legal notices—embedded directly into media frames. Session-based watermarking dynamically overlays viewer-specific data, such as email address, timestamp, or IP address, during playback, and reinforcing traceability for each session. For heightened protection, forensic watermarking embeds imperceptible identifiers at the pixel level that persist through recordings, downloads, or transcoding, enabling content owners to trace unauthorized redistribution back to the original viewer. These layered watermarking options provide proactive deterrence against leaks while preserving high-quality playback. For more information, see watermarking.

Digital Rights Management (DRM)

Frame.io Enterprise supports Digital Rights Management (DRM) to protect media during delivery and playback. When activated, DRM encrypts media streams and restricts decryption and playback to authorized viewers in supported environments, helping prevent unauthorized copying, capture, or redistribution outside approved workflows. By combining DRM with granular permissions, secure sharing, and watermarking, Frame.io Enterprise delivers a comprehensive framework for safeguarding sensitive pre-release media throughout its lifecycle.

Audit trail API

Frame.io Enterprise provides visibility into administrative actions and content activity to support enterprise governance, compliance, and operational oversight. Through its API and administrative interfaces, organizations can programmatically manage users, roles, and permissions, while integrating activity data with broader monitoring, reporting, or SIEM systems. This capability enables detailed audit trails of access control changes, user actions, and content interactions, supporting security investigations and internal accountability processes.

Hosting locations and data storage

The Frame.io Enterprise service and corresponding data and file storage are hosted in Amazon Web Services (AWS) data centers in the US-East-1 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. Data within the VPC is protected with access controls, role-based permissions, and a Web Application Firewall (WAF).

Adobe Frame.io Storage Connect

Frame.io Storage Connect[1] is an optional add-on feature that allows enterprise customers to use their own AWS-hosted storage for Frame.io. Using AWS IAM access models and policy-based roles and permissions, customers' Adobe Admins have greater oversight of the governance and security of their owned assets.

With Storage Connect, Frame.io remains the graphical management interface, but:

- **Original** assets uploaded to Frame.io are redirected to the enterprise customer's connected storage instead of Frame.io-owned storage.
- **Proxies** and derivative assets will continue to be stored in Frame.io-owned storage to help support performance and business continuity.

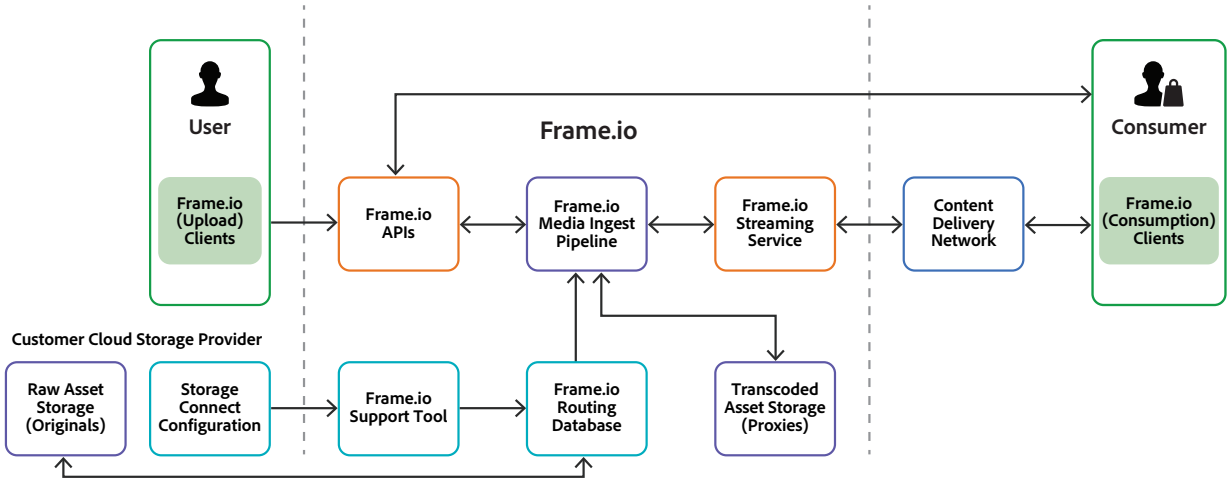

Figure 2: Frame.io Storage Connect diagram

Questions?

If you have any additional questions about the security posture and capabilities of Adobe Frame.io Enterprise, please contact your Adobe account manager. For all other questions about Adobe's security programs and processes and compliance certifications, please see the Adobe Trust Center.

[1] *With the Storage Connect option, originals of uploaded content are stored in the customer's US-East-1 storage location. Proxies and derivatives are stored in the Frame.io's US-East-1 storage location.*