Overview of Security Capabilities

Last Modified on 08/19/2024 4:54 pm IDT

About

Kaltura's online video platform offers advanced video publishing, management, syndication and monetization solutions suitable for many verticals, including education, enterprise, government, media and entertainment, advertising, and many others. Kaltura's flexible platform and APIs allow publishers and organizations to rapidly, and cost-effectively, build video applications, widgets and plug-ins, as well as add core video services to their existing offerings.

Whether you publish video on the web or use it only for internal audiences, it is important for you to address the security aspects of your online video strategy. Kaltura offers various effective ways to implement the right level of security for your needs and has built in physical, architectural and applicative security measures that provide end-to-end protection for your assets and information.

Whether you choose a Software as a Service (SaaS) implementation using our scalable infrastructure and trusted CDN partner, or opt for a self-hosted and self-operated platform on your own premises (Kaltura On-Prem™), Kaltura will help you implement the security measures you need to have in place, while assuring an intuitive and smooth experience for your end users.

This guide provides an overview of the security capabilities that Kaltura offers and includes a high level description of the Kaltura security capabilities for video based content – including ingestion, storage and delivery. The methods that Kaltura uses to protect user information are described, in addition to Kaltura's business continuity and disaster recovery policies, Kaltura's secure platform architecture, and the physical security Kaltura maintains in its hosting facilities. If you require a more in depth description of Kaltura's security capabilities, please contact a Kaltura representative.

The options can be used as standalone capabilities – or used together to provide a full security package.

Protecting Content in Transit

Some organizations are concerned about the security of their media as it is being streamed. Content can be hijacked using man-in-the-middle attacks or other stream capture methods, and then the content can be stored locally or published illegally.

To protect your content in transit, you can use a secured streaming protocol. You can configure the CDN to stream over an encrypted protocol (HTTPS/RTPME) to prevent

exposure of the content in transit. The Kaltura platform allows you to easily implement secured streaming.

AES Encryption

To support content protection on delivery, Kaltura supports AES standard encryption of content delivery for HLS delivery. Content is encrypted on the fly utilizing the Kaltura on the fly packager, and the Kaltura player can access the decryption key on the Kaltura servers to decrypt content as it is being played back.

Encryption at Rest

To support secure storage of content on the Kaltura servers, Kaltura employs encryption at rest of content. Encryption is on a per rendition level, with the encryption done as part of the transcoding process. Content is securely transitioned and stored thought the whole ingest/transcoding process.

Encryption at rest is especially beneficial for customers utilizing the Kaltura uDRM module. Since Kaltura utilizes on the fly packaging and encryption for DRM content, customers can enjoy the benefits of storing only the original content renditions – without the need of storing pre encrypted DRM flavors, and still make sure content is stored securely utilizing encryption at rest.

See Digital Rights Management for more information.

HTML Purifier

HTML Purifier is a standards-compliant HTML filter library that removes malicious code (like XSS) and ensures the output is clean, safe, and valid HTML. It is commonly used in web applications to sanitize user-generated content, stripping out potentially harmful elements while preserving well-formed HTML. This helps to prevent security vulnerabilities and maintain the integrity of web content. HTML Purifier can be configured to allow specific tags and attributes, making it flexible for different use cases.

Kaltura accounts can be configured on the backend with HTML purifier to use only basic list for purification or to purify image content with block behavior (recommended). For more information, please contact your Kaltura representive.