BRIGHTCOVE

Data & Application SECURITY

Brightcove's unmatched reliability enables secure video workflows that easily scale to fit organizational strategies, and is backed by an award-winning, around-the-clock support team. Brightcove brings together security options that serve your strategic needs. Unlike other solutions on the market, is highly scalable, quick to deploy, and supports secure access to video content with the controls listed below.

	WHAT IS IT?
ENCRYPTED STREAMING (DRM and AES-128)	Encryption is the process of encoding information, such that only authorized users can view it. We offer two levels of stream encryption - AES-128 (HLSe) and DRM. HTTP Live Streaming Encryption (HLSe) lets you send encrypted video over HTTP for playback on desktop and mobile devices. DRM is studio-grade, hardware enforced encryption that adds an extra layer of copy protection described below.
DIGITAL RIGHTS MANAGEMENT (DRM)	DRM prevents your videos from being played back except in clients that are granted permission to do so. Implementations of DRM vary, but the typical use is to encrypt the video and decrypt it only if the client has a key to authorize playback. DRM is not included by default and can be purchased as an add-on. **Learn more here.**
TOKEN AUTHENTICATION / TIME-TO-LIVE (TTL)	Video Cloud adds a TTL token to URLs for renditions to prevent your content being viewed after a set expiry date. By default, these tokens have a very short life.
GEO-RESTRICTION & GEO-FILTERING	Ability to block playback in a specific country. Geo-filtering can be used for content protection by applying geographic restrictions using IP location.
IP ADDRESS RESTRICTION	In order to limit video playback to internal viewers only, Video Cloud Enterprise publishers can use IP address restriction. This approach prevents all the players in an account from loading unless the browser loading the player uses one of a specified list (whitelist) of allowed IP addresses. This provides a level of security that goes beyond domain restriction or geo-restriction.
DOMAIN RESTRICTION	Domain restrictions can be set on players to limit the domains where players can be used. If the player publishing code is copied and used on another site, domain restrictions would prevent the player from loading any videos.
SINGLE SIGN ON (SSO)	When creating an access control profile that uses SSO, site visitors will be prompted to login with valid credentials before they can access the site. Gallery supports the Security Assertion Markup Language 2.0 (SAML 2.0) standard for exchanging authentication and authorization data between security domains.

281 Summer Street, Boston, MA 02210 | Tel 617 674 6500 | Fax 617 261 4830 | brightcove.com |

BRIGHTCOVE

WHAT IS IT?

PROXY RESTRICTIONS (DRM and AES-128)

These restrictions block playback from the following identified scenarios:

- **ANONYMOUS** – IP address of the client is not available. Includes services that change location to beat DRM, TOR points, temporary proxies, and other masking services.
- **PUBLIC** – Multiple users proxied from a location allowing public internet access.
- **CORPORATE** – Generally considered harmless, but location can be a concern. Identify if multiple users are proxied through a central location or locations and can share a single network-apparent IP address.
- **TRANSPARENT** – IP address of the client is available via HTTP headers, though the value is not necessarily reliable (e.g., it can be spoofed).
- **HOSTING** – IP address belongs to a hosting facility and is likely to be a proxy since end users are not typically located in a hosting facility.

MID-STREAM RIGHTS CHECK

After the initial rights check is run at the start of video playback, another validation of the viewer's credentials is run mid-stream. If the mid-stream check fails, the player will stop video playback. A great example of this is for a paid sporting event: if the team has a limit on stream concurrency and a paid viewer shares their login, a mid-stream check would determine the user no longer meets the conditions of the restrictions (i.e, more than one person has signed in with those credentials) and playback would stop.

STREAM CONCURRENCY LIMITS

Limiting concurrent streams per user discourages viewers from sharing their credentials with friends who don't have accounts. With concurrent stream limits, you define the number of video streams that a specific user can watch at any given time.

DEVICE REGISTRATION

Device registration occurs when a DRM license request is made. A unique ID is assigned to each device, and with each license request, the device limit is checked and enforced. An example of this is when a content provider grants a publisher permission to stream their content for a period of time and their contractual agreement limits the number of devices associated with a single viewer to two. Once that limit is reached, if a user tries to view the content on a third device – say, a connected TV – the playback will be denied. This enables content owners to achieve monetization objectives and minimize unauthorized access.

To learn more about Brightcove and our solutions:

Visit Brightcove

BRIGHTCOVE