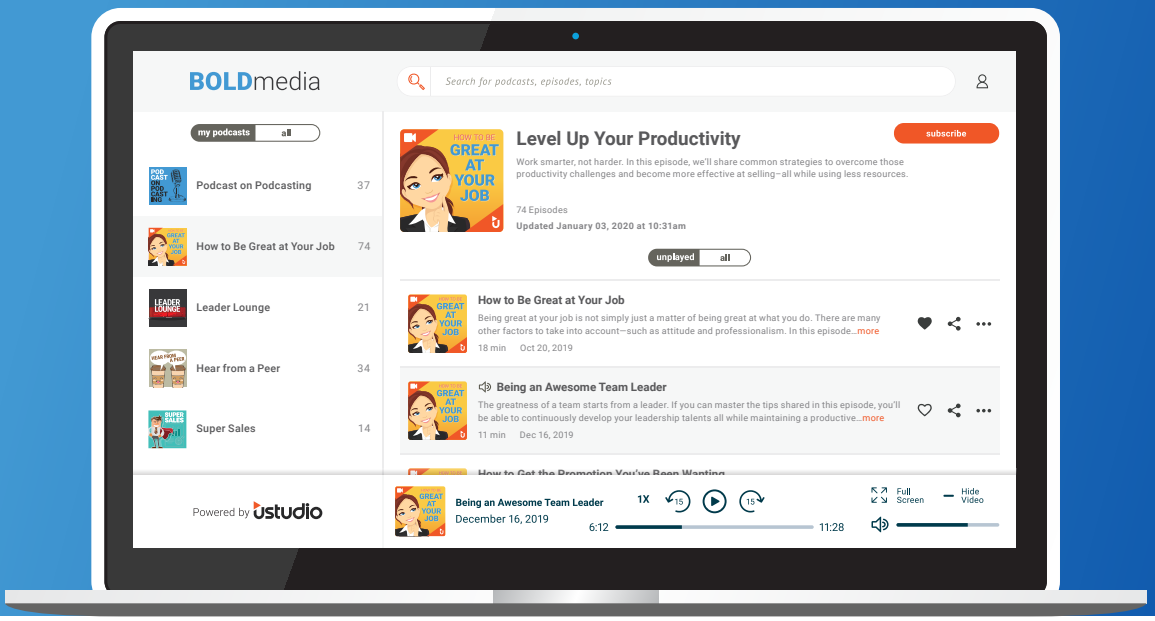
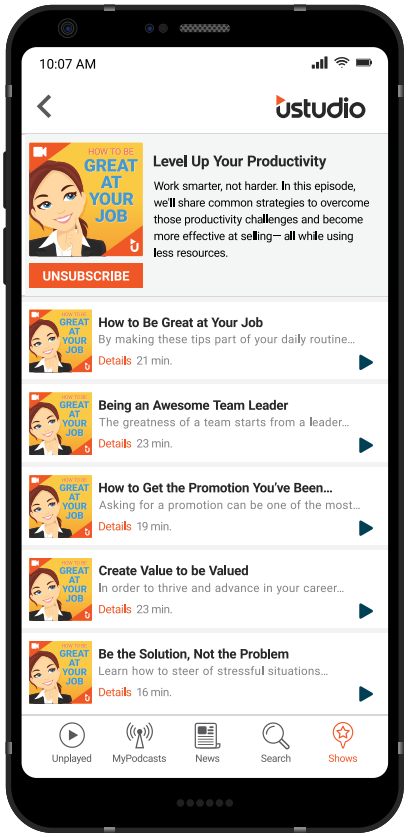
ustudio

WHITEPAPER



Securing Media Delivery in the Enterprise

Securing enterprise content is paramount for any modern business, whether you are restricting access to sensitive, internal content or protecting public content from unauthorized use. Unfortunately, the complexities of streaming media and the unique requirements of today's enterprises can make securing media delivery an onerous task.



uStudio's experience working with large enterprises to secure media delivery has given us a unique perspective on the technical architecture required for success, as well as a roadmap for how enterprises can approach and resolve their security concerns.

uStudio offers a robust, easy-to-use platform for enabling enterprise media strategies while providing a highly configurable set of security capabilities that modern enterprises require. With a multi-tier approach that addresses security at the page, player, and stream levels, and providing controls to restrict access to specific audiences, we are able to collaborate with our customers to configure solutions that meet their unique needs.

IN THIS WHITEPAPER, WE WILL COVER:

- How to determine if and to what extent media security is appropriate for your content
- The importance of a multi-tier approach to securing media delivery
- An overview of uStudio's media delivery security capabilities

Determining Security Requirements

The first step in creating an effective security strategy for media delivery is determining the security requirements for your media based on the audience(s). Best practices start this process by determining the following about your content and audience:

- Restricted vs. Unrestricted access to your content
- Trusted vs. Untrusted users in your audience

RESTRICTED VS. UNRESTRICTED ACCESS | Who can access the content?

To determine the access requirements for a given media asset, it is important to ask to what degree limiting the set of people that have access to consuming the media makes sense. While restrictions on media access are company and use case specific, some access restriction scenarios are quite common. For marketing videos, the content is intended for unrestricted access so that employees, clients and anyone else can consume this media. However, for internal all hands meetings, the sensitive nature of the content demands restriction to only employees. For management training, it may be necessary to restrict access to a particular set of internal users.

TRUSTED VS. UNTRUSTED USERS | What can users do with the content?

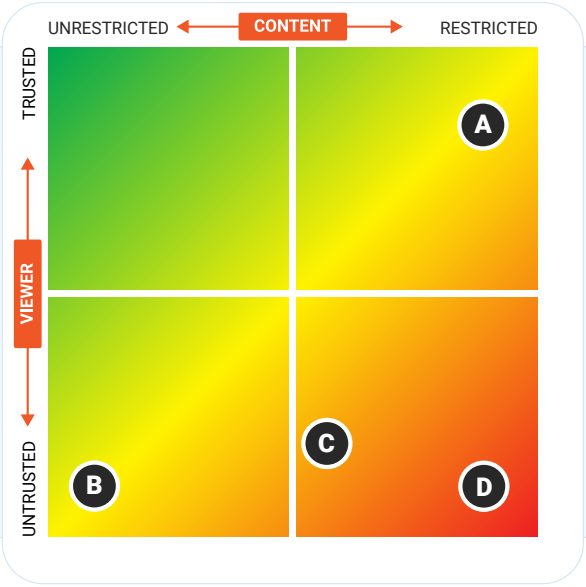
Once you determine whether access to your media should be restricted, the next phase of a media security review is to determine if you trust the audience you've defined with your media content. Essentially, this step will determine if you should be concerned if your media is used inappropriately. Important questions to consider include: Do you need to prevent your restricted audience from sharing your media content with a broader audience? Do you need to prevent them from using your content in an unauthorized way? Enterprise media content often dictates classifying your audience as untrusted.

At the conclusion of these two steps, your media should fall into one of these four categories:

MAPPING CONTENT AND AUDIENCE TO DETERMINE SECURITY REQUIREMENTS

ILLUSTRATIVE EXAMPLES

- **A** Executive team training
- **B** Public marketing content
- **C** Company-wide announcements
- **D** Review and approval



RESTRICTED ACCESS TO TRUSTED USERS | Example: Sharing videos within a small team for review and approval

This security scenario is appropriate when sharing media content with small set of specific users that can be trusted not to share or publish that content in an unauthorized way.

RESTRICTED ACCESS TO UNTRUSTED USERS | Example: Live streaming a corporate town hall meeting to all employees

This security scenario is appropriate for most internal communications use cases, as well as secure external communications to partners and customers. While the desired outcome would be to restrict access to a specific group of users, the possibility exists that any of those users could share the media asset outside the restricted group. Therefore, that audience should be considered untrusted.

UNRESTRICTED ACCESS TO UNTRUSTED USERS | Example: Publishing marketing videos on a public website

This security scenario is appropriate for any publicly available media content. You want as broad an audience as possible, so there is no reason to restrict access. However, it is necessary to protect the asset against unauthorized usage.

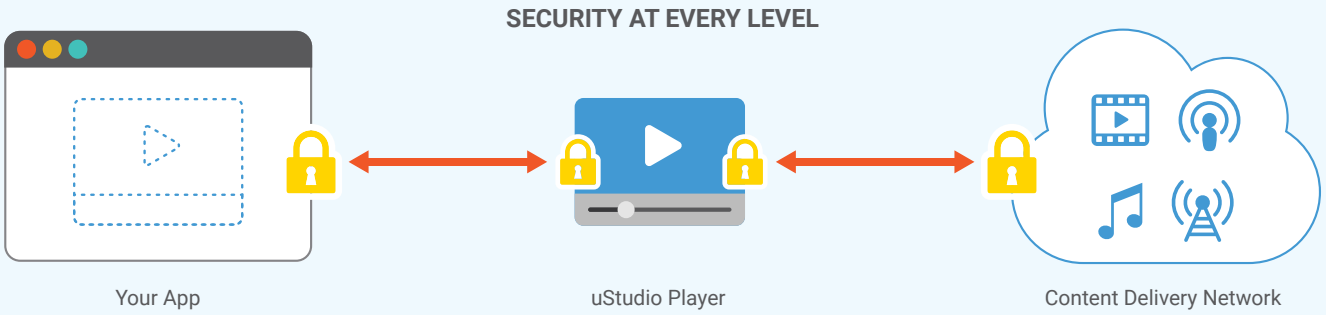
UNRESTRICTED ACCESS TO TRUSTED USERS | Example: Not appropriate for enterprise media use cases

This security scenario exists when an organization makes media available to the public and is comfortable allowing viewers to take that content and potentially use it in a way that their organization didn't authorize.

Finding the balance between security requirements and business objectives can often be challenging. uStudio is designed to help simplify and reduce the implicit complexity of configuring enterprise-level security. We partner with our customers to identify the best security configuration for their unique needs by leveraging a multi-tier approach to securing media delivery.

uStudio's Multi-Tier Security Model

uStudio is the only media platform company with a multi-tier security model that offers security configuration optionality at each of the page, player, and stream levels. After you have completed the security quadrant assessment, the next step is to determine which level of media delivery configuration is needed to best protect your content from unauthorized access and/or untrusted users. It's critical to consider each when establishing an enterprise media security model.



APPLICATION-LEVEL OR PAGE-LEVEL SECURITY

These security measures restrict access to the page or application where media is published. If a media player is published on a website or in a third-party application, page-level authentication is often handled by that third-party system.

To properly ensure your content is secure, page-level security should always be implemented in conjunction with restrictions at the player and stream levels. If you only configure media security at the page level, it's only secure as long as the player is embedded on a private page. Without additional restrictions, anyone with access to that page could easily copy the player embed code and paste it onto any other webpage, making it accessible to anyone.

PLAYER-LEVEL SECURITY

Player-level security provides further access restriction to media embedded in public or unsecure pages and further restricting access to media embedded in private pages. Player-level security prevents the media player from loading unless certain requirements are met. A first line of defense may be requiring the player to be accessed on a certain domain, from a certain region, or from a specific IP address. More restricted access may include requiring user authorization before a player loads, ensuring that only a specific set of users have access to the player.

STREAM-LEVEL SECURITY

Without any security measures at the stream level, any user who can access the content can download, redistribute, or share the content, even if the page and player are secured. By first ensuring that the same access rules are respected at the stream level, authorized users can be prevented from simply sharing a URL that could be accessed in other players or applications. By encrypting the content (via DRM, URL tokenization, or other mechanism), authorized users are further prevented from downloading and redistributing the content manually.

Security at the stream level is particularly critical for protecting against untrusted users.

By supporting a broad range of security configurations at each level of media delivery, uStudio offers the most granular level of security and control in the market.

uStudio's Media Delivery Security Capabilities

PAGE/APPLICATION AUTHENTICATION

If a customer publishes a uStudio player on their website or in a third-party application, page-level restrictions are handled by that third-party system. If a customer publishes media content on a uStudio managed application, like uStudio's Enterprise Podcast App, then we authenticate users into the app using SSO (Single Sign-On) with our customers' preferred authentication technology.

EMBED RESTRICTIONS

Embed restrictions prevent media content from loading when unless the player is being accessed in an approved environment.

Domain whitelisting: Allow media content to be loaded only if the media is embedded on an approved domain.

Geo whitelisting: Allow media content to be loaded only in approved countries.

IP Address whitelisting: Allow media content to be loaded only when accessed from an approved IP address.

Embed restrictions, on their own, are relatively easy to work around for sophisticated users wanting unauthorized access to your media content, so they are best implemented in conjunction with other restrictions at the player and stream level.

PLAYER SSO

With uStudio's Player SSO, the player itself can be configured to require authentication. This enables customers to restrict access to a specific set of users even when a player is embedded in pages or applications that may not have the same level of access restriction. Even if the player is published on a public page, users are still required to log in to view the content.

SIGNED EMBED CODES

Signed embed codes are a developer tool which allow any access control rules to be respected inside any application, regardless of the underlying authentication system. Access tokens are are generated by the application dynamically per user, are time-limited, and generally set to expire very quickly, preventing shared access. Once a user has been authorized to view the video content, access to transcode / segment URLs are tokenized for the client, and are also time-limited (and can be enabled to require unique client strings, IPs, etc).

When using our signed players, uStudio embed codes must be wrapped with an OAuth-style signature for any playback to be enabled. From that point, our system generates secured URLs depending on the functionality supported by the configured CDN. For instance, simple tokenization tied to the client, IP, country, etc. may be supported for both progressive streams as well as HTTP-based segmented live formats. The secret used for signing the embed codes can be provided (and changed) by the customer, and is never shared with a third party (not even via the API), ensuring that only applications with the pre-shared secret are able to generate authorized embeds.

The TTL on the player is configurable every time an embed is signed, and we recommend a small window before immediately displaying the embed to the authorized user.

ENCRYPTION

uStudio players can be configured to support a variety of security options. At minimum, all players support HTTPS for all HTTP requests, including progressive download and streaming protocols over HTTP. Stream-level encryption is subject to desired device compatibility, content requirements, and CDN support. For instance, the HLS specification allows AES-128 encryption for media segments for certain environments, which provides minimal protection, whereas browsers which support EME (Encrypted Media Extensions) may support DRM through numerous providers across transfer protocols including HLS and DASH. Finally, for Flash-fallback environments, HDS may be used which allows for DRM via Adobe.

For live ingest, security is also an important concern, and both RTMPS (using TLS) and RTMPE offer encryption over the wire to ensure that the stream you are delivering cannot be snooped across an untrusted network.

SECURE ADAPTIVE PLAYERS

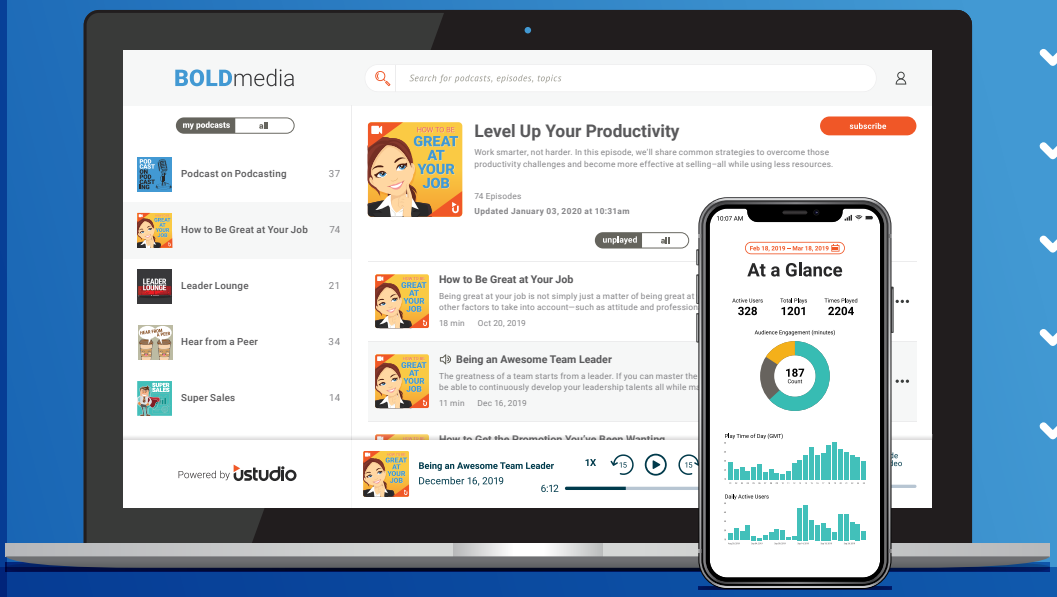
uStudio's secure adaptive players use tokens in the form of query parameters. These query parameters are tied to the browser session, IP, URL base path, and referrer, and have a configurable time to live (TTL).

Players can be further configured to provide security when used in conjunction with restrictions on the embed code, such as with domain, IP, or geo whitelists. The embed restrictions control access to the player, in addition to tokenize access (via SSO or OAuth-style signatures above). These restrictions extend from the player to the stream, making it more difficult for untrusted users to access and download the content.

To learn more about uStudio, contact our sales team at sales@ustudio.com.

Media Solutions for Business

Deliver corporate audio and video content securely to any device in a modern, mobile-first experience



- Web & Mobile Apps
- Live & On Demand
- More Convenient
- Private & Secure
- High Engagement

GET STARTED TODAY!