GETTING STARTED WITH DIGITAL RIGHTS MANAGEMENT FOR ONLINE VIDEO

As consumers embrace online video across a broad spectrum of devices, from smartphones and tablets to PCs and connected TVs, publishers need a way to protect their content against piracy and unauthorized viewing no matter how, where, or when it is accessed. Digital rights management (DRM) provides the control publishers require to secure their content for wide-ranging business models and distribution strategies. This brief answers common questions about DRM to help you understand its role in content security, and decide how best to incorporate it into your online video strategy.

DRM Defined

WHAT EXACTLY IS DRM?

DRM is a set of technologies that enable content owners to secure both premium and non-public content, and to enact policies around how consumers can engage with it. These can include payment terms, allowed devices, and copying or sharing permissions. DRM is the primary means for online video publishers to protect against unauthorized use, piracy, and other violations of their terms of use.

WHAT ARE THE DIFFERENT TYPES OF DRM?

There are two kinds of DRM: **Anonymous** and **Authenticated**.

Anonymous DRM, also known as non-authenticated DRM, secures content at its origin (e.g., storage at the content delivery network before content is transported) and allows you to enforce viewing and distribution policies around the content. Anonymous DRM is all publishers need to protect content against unauthorized viewing, and is also sufficient to support many premium content models. Solutions like Adobe Access and Google Widevine offer a turnkey solution for anonymous DRM, as each individual video is secured and encrypted at its origin, including metadata and policies, for the highest level of security on mobiles devices, PCs, connected TVs and gaming consoles.

Authenticated DRM provides an even higher level of control with more sophisticated content protection and video monetization models based on individually authenticated viewers. Authenticated DRM lets publishers offer video on a broader range of terms, including rental, subscription video-on-demand (SVOD), and multi-title packages, as well as define rules for viewing windows. Authenticated DRM can also limit the number of streams or devices a video can be played to.

WHAT IS THE DIFFERENCE BETWEEN ENCRYPTION AND DRM?

Encryption refers to the use of an algorithm to help prevent unauthorized parties from copying or viewing content. Typically, the distributor shares the algorithm and associated key with authorized parties, allowing them to decrypt the encrypted information. For example, when a user logs into their bank account, their password is encrypted on their machine and remains that way as it is passed to the bank so others cannot see the password as it travels over the Internet.

DRM goes beyond encrypting and protecting information; it also allows the content owner to apply additional rules that govern how and where content can be viewed. In the case of encryption, the viewer can then do what they want with the content once it is decrypted, while DRM prohibits the viewer from storing the decrypted version of content. For these reasons, DRM provides a much higher level of protection against content being shared illegally, which is why most major movie studios require DRM on top of encryption when publishers distribute their content.

Why DRM?

WHY DO I NEED TO PROTECT MY CONTENT?

As online video has gone mainstream, organizations of all kinds now produce high-quality branded content that they want to protect and maintain control over distribution.

If you publish or distribute premium content, from short-form and long-form entertainment to commercially available training videos, you need a way to enforce your model and make sure your revenue is not being undermined by unauthorized sharing and viewing. Even publishers who are not in the paid video business need to make sure that their content is secure and not being misused by unauthorized parties. Examples include proprietary company content, national or state confidential materials, internal announcements, and partner or channel communications. Videos like these can be highly useful for meeting internal business needs — and potentially damaging if viewed or shared inappropriately. You wouldn't allow a stranger to browse your servers and help themselves to your data and intellectual property. Your video content deserves the same level of protection.

How does DRM work?

HOW DOES DRM FUNCTION DURING PLAYBACK?

Protected content must be decrypted to play back for a viewer. Playback requires the content, or more precisely the player for that content, to communicate with the DRM system. The DRM software in the player communicates with a central system that handles content licenses and allows or prohibits playback of that content.

THE VIEWER'S EXPERIENCE

Web Browsers

Browsers support the most diverse set of DRM solutions compared to all other platforms. The challenge with DRM in browsers is that user engagement is typically required in the form of installing a plugin the first time a viewer watches DRM-protected content. The one exception is Adobe Access, which auto-installs the plugin in the background when the user first streams Adobe Access content. From a user point of view it is completely transparent. The downside of this solution is that it only works for Flash at this time, although most browser-based video still leverages the Flash player.

iOS & Android

There are two ways to stream content on a mobile device: through a native application that is downloaded from the iTunes App Store or Google Play, or through the Web browsers on the device. All of the DRM solutions only work within a native application, while other encryption methods can be used within the mobile Web browser, e.g. Apple HTTP Live Streaming (HLS) encryption.

As with browsers, a plugin must be included with the native application to decrypt and play back "DRM-ed" content. In the case of native applications, this is packaged with the application when the user downloads it from the application store, creating a seamless experience.

Connected TVs & Gaming Consoles

A variety of connected TVs include DRM as part of their platform. This is typically integrated into the platform on the TV, requiring the owner to protect their content with the same DRM solution. Many of the major TV manufacturers support Widevine today and are beginning to add other DRM solutions into some of their latest TVs.

At the end of 2011, Microsoft announced support for PlayReady on its Xbox LIVE platform. This is the only DRM solution that is currently available on the Xbox. Other gaming consoles such as Sony PlayStation 3 and Nintendo Wii support Widevine.

What do I need for DRM?

POPULAR DRM SOLUTIONS

Adobe Access (formally Flash Access)

Adobe's Access DRM solution is fully integrated with Flash Access. The latest version will protect more than just Flash content. One advantage of Adobe Access is its ability to seamlessly integrate into the browser, allowing it to download in the background the first time a user streams Adobe Access-protected content. In most cases, the user is not even aware Adobe Access is protecting the content.

Google Widevine

Widevine provides protection across multiple streaming protocols, including Apple HLS and Adobe Flash delivery. Widevine has been heavily implemented in connected TVs, Blu-ray players and mobile devices, and is embedded in the hardware of many other devices. The fact that Widevine is deployed in more than 539 million consumer electronics devices has made it a popular choice for DRM.

Microsoft PlayReady

PlayReady is the DRM solution for Xbox, Windows 8 and Windows mobile devices. Microsoft also provides a porting kit to help make PlayReady available on more devices. Microsoft recommends that PlayReady be used with Smooth Stream, with the likelihood that it will move to MPEG-DASH in the future. Some of the most well-known premium video streaming services are using PlayReady, including Netflix and HBO GO.

Marlin

The Marlin DRM platform was developed by the Marlin Developer Community (MDC) open-standards community initiative, which was created by Intertrust, Panasonic, Philips, Samsung, and Sony. Marlin has been studio approved and is most notably being used with the YouView project in the UK.

HOW DOES BRIGHTCOVE PROVIDE DRM?

Brightcove has invested in extensive auditing to ensure that we adhere to a rigid set of security standards related to the personnel maintaining the DRM system, the physical environment that houses the system and the hardware and software configurations themselves.

Today, Brightcove offers DRM solutions based on Adobe Access and Google Widevine, with more to come in the future. A content provider can also purchase DRM software and enable the delivery of secure content itself.

WHAT ARE MY OPTIONS FOR ASSET PROTECTION?

The appropriate DRM system for your business needs will vary based on your content requirements, budget, and device requirements. In addition, this is a very dynamic market — the requirements for some platforms are changing at least every year. For example, there may be multiple options available when targeting a connected TV platform and fewer options on an Android or iOS device. Once the appropriate DRM system(s) is selected, you will need to consider how the content is packaged. The content owner can package and encrypt content before delivering to a service provider, such as Brightcove, or a content delivery network (CDN), or a service provider can do the packaging.

Conclusion

While DRM is still sometimes viewed as a concern only for big-name media companies and content producers, the reality is that it plays an important role in online video initiatives of all kinds. By protecting your content and controlling its use, you can make sure that your online video strategy serves the purposes for which it is intended — and that it won't be undermined or undervalued as a result of unauthorized activity.

290 Congress Street, 4th Floor, Boston MA 02210

brightcove