



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 it is accessed. Digital rights management (DRM) provides the control publishers need 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.

Do I Need DRM?

What exactly is DRM?

Digital Rights Management (DRM) is a set of technologies that enable content owners to secure their content, including both premium and non-public internal content, and to enact policies around how consumers can engage with it. These can include payment terms, allowed devices, and whether users are permitted to copy or share your content. DRM is the main way that online video publishers protect against unauthorized use, piracy, and other violations of their terms of use.

Why would I need to protect my content?

DRM isn't just for major media companies like broadcasters, movie studios, and music labels anymore. 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 how it is distributed.

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 pay model and make sure your customers aren't undermining your revenue potential by copying or sharing your videos with unauthorized viewers.

Even publishers who aren't in the paid video business need to make sure that their content is secure and is not being misused by an unauthorized party. Examples include proprietary company content, national or state confidential materials, internal announcements, partner or channel communications, and other non-public content. 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?

What are the different kinds of DRM?

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

Anonymous DRM, also known as non-authenticated DRM, secures content at its origin (eg. 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 non-paid, non-public content from unauthorized viewing, and is also sufficient to support many premium content models.

Solutions like Adobe Flash Access 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 control for Flash-supported environments.

Advanced DRM provides an even higher level of control over content across platforms, such as Flash, iOS or Linux-based devices or PCs, to support more sophisticated content protection and video monetization models based on the individual authentication of each viewer.



Advanced DRM lets publishers offer video on a broader range of terms, including rental, subscription video-on-demand (SVOD), and multi-title packages, and define rules for the period of time during which it may be played. Advanced DRM can also prevent a video from being output on specific device ports, and tie it to specific machine IDs so users can only play it on a limited number of devices.

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. In the case of Flash Access, the player can seamlessly communicate with centralized Flash Access servers. In the case of other DRM systems, the viewer must install or already have installed compatible DRM software on their device. In either case, the DRM software communicates with a central system that handles content licenses and allows or disallows playback of that content. In the case of Flash Access, no additional software beyond Adobe Flash is required by the viewer.

What do I need to do to implement DRM for my video content?

How do I get DRM?

There are literally dozens of companies in the DRM ecosystem, and a wide variety of anonymous and advanced DRM systems available to address diverse business needs. Different DRM systems may be required to support a wide variety of playback devices, such as mobile phones, tablet computers, and connected televisions. DRM technologies are most commonly available from software companies, such as Adobe, or service providers, such as Brightcove. To offer DRM as a service, the provider must 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 itself. A content provider can also purchase DRM software and enable the delivery of secure content itself. Today, Brightcove offers a DRM solution based on Adobe Flash Access.

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) are 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.



BRIGHTCOVE VIDEO
CLOUD PLAYER



ADOBE FAXS
Flash Access DRM Services

Conclusion

While some people still think of DRM as a concern only for big-name media companies and content producers, the reality is that it has an important role to play 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 by unauthorized activity.