White Paper

Multi-DRM Done Right: Simplify Cross-Device Content Protection

Contents

Growing Beyond Managed Pay-TV Business

Content is still king in the world of video. Consumers worldwide are expanding their ways of consuming video content while the Internet of Everything influences their lifestyle - making “anytime, anywhere, any device” the new normal. As a result, the proliferation of diverse unmanaged IP devices is now a critical challenge for service providers.

How can you deliver a satisfying subscriber experience, while protecting your revenue and taking advantage of new business models? And what’s the best way to handle content security, delivery, and management, which are relatively well-defined processes on managed devices but are highly fragmented on unmanaged devices? Device fragmentation also affects your ability to deliver a smooth, engaging, and consistent user experience that optimizes the potential of each type of unmanaged device.

Figure 1. Managed and Unmanaged Networks and Devices

To remain competitive, you need to expand from managed networks to unmanaged networks, including over-the-top (OTT) models (Figure 1). This crucial expansion provides an opportunity to create new services and business models, such as video on demand (VoD) in a multiscreen environment. But it also presents another challenge: supporting multiple digital-rights-management (DRM) products deployed by diverse content providers.

Choosing the right content protection in today’s environment requires multidevice, multinetwork, and multi-DRM support. Fortunately, there is a simplified approach to addressing this complexity.

A Comprehensive Approach to Content Security

The most effective way to choose a DRM product addresses three critical considerations. This holistic approach includes the following criteria:

- **Capabilities:** You need to evolve quickly and deliver extensive end-to-end features in a dynamic market. So you want a rich, modular solution that helps you get the most from your existing infrastructure. It should provide flexible interfaces on multiple levels to allow anything from minimum rights enforcement to full-scale device and entitlement management.

- **Compatibility:** Your solution should help you deliver multiple services over multiple networks in a multi-DRM deployment. So make sure that:
  - It's compatible with popular unmanaged devices, content formats such as HTTP Live Streaming (HLS) or HTTP Smooth Streaming (HSS), and encoders with a wide range of available-bit-rate (ABR) and packaging options.
  - It integrates with major content-delivery network (CDN) vendors.
  - It's interoperable with standards, such as Universal Plug and Play (UPnP), Digital Living Network Alliance (DLNA), or Digital Transmission Content Protection over Internet Protocol (DTCP-IP).
  - It supports virtualization and cloud technologies, such as OpenStack.
  - It gives you the freedom to develop different applications and user experiences using HTML5, Java, or other relevant development languages and platforms.
- **Responsibility:** You need ongoing expertise and support that span the world of managed and unmanaged devices and networks and give you the ability to quickly respond to threats. That's why your content-protection solution should have approvals from several major studios or content owners. And it should come from a vendor that has years of proven, uncompromised experience in securing content - and has a robust roadmap that keeps pace with changes in technology.

Unifying Security beyond a Single DRM Solution

A unified approach to today's multidevice, multinetwork, and multi-DRM world should meet the following goals:

- Provide users with a transparent experience, whether they are viewing content delivered over managed or OTT networks. Your DRM solution should be able to associate multiple managed and unmanaged devices with the same household and provide proximity and concurrency control across all of them. Any content-protection elements, such as transcoding, repackaging, and rights transfer, should be practically transparent to users. That way, they can enjoy an optimal experience when consuming and sharing content no matter what device they use.
- Consolidate all content to reduce the quantity of copies, while delivering that content to the broadest possible range of devices. With this approach, you can support the multiple formats required for various devices, manage the authentication and entitlement validation, and flexibly support multiple DRM systems used by the different content and devices. Establish a single point from which you can enforce device registration, entitlement, and authorization for traditional broadcast platforms or unmanaged devices. You should be able to enforce a different set of usage rules with each program or channel, including policies such as concurrency and location restrictions.

With a unified, robust, and flexible multi-DRM framework, you can deliver content more efficiently, minimize costs, and accelerate return on investment. This type of active security framework employs a moving-target approach to security. Unlike other DRM systems that react to security threats, it proactively modifies critical DRM components, helping neutralize any threats from hackers before they affect the service.

Unifying DRM with Conditional Access Systems

It may be appropriate to have a unified solution work alongside conditional access systems to provide a transparent experience across a subscriber's IP devices in the home. Conditional access would terminate at the managed set-top box or gateway device, which would act as a bridge between conditional access and DRM. It would transcode the content by adjusting parameters, such as resolution or bit rate, for optimized high-quality viewing on the subscriber's target device.

How Multi-DRM Done Right Creates Value

Digital-rights management is about more than protecting content. It's also about adding value to your platform. Subscribers can watch content on a wide variety of devices while you control all the devices and services running on your platform. When a multi-DRM is done right, with a holistic and unified approach to content security, it helps ensure that you can package and manage the services flexibly and optimally for many years in the future.

About Cisco VideoGuard Multi-DRM Framework

With more than 25 years of experience, Cisco is a leader in content security, and our solutions are deployed globally by leading pay-TV operators. The Cisco VideoGuard™ Security Solution includes the VideoGuard Everywhere DRM, that uses a holistic and unified approach to content protection and a framework to support multiple DRMs. Cisco VideoGuard Security Solution is part of the wider Cisco Videoscape™ portfolio, designed to provide an end-to-end, open, and modular platform that smoothly integrates with servicer providers' back-end, in-house, or third-party systems, helping deliver new customer experiences swiftly, securely, and within budget.

For More Information

For more information about the Cisco VideoGuard Security Solution, please visit: http://www.cisco.com/c/en/us/products/video/videoguard-drm/index.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-734000-01 06/15