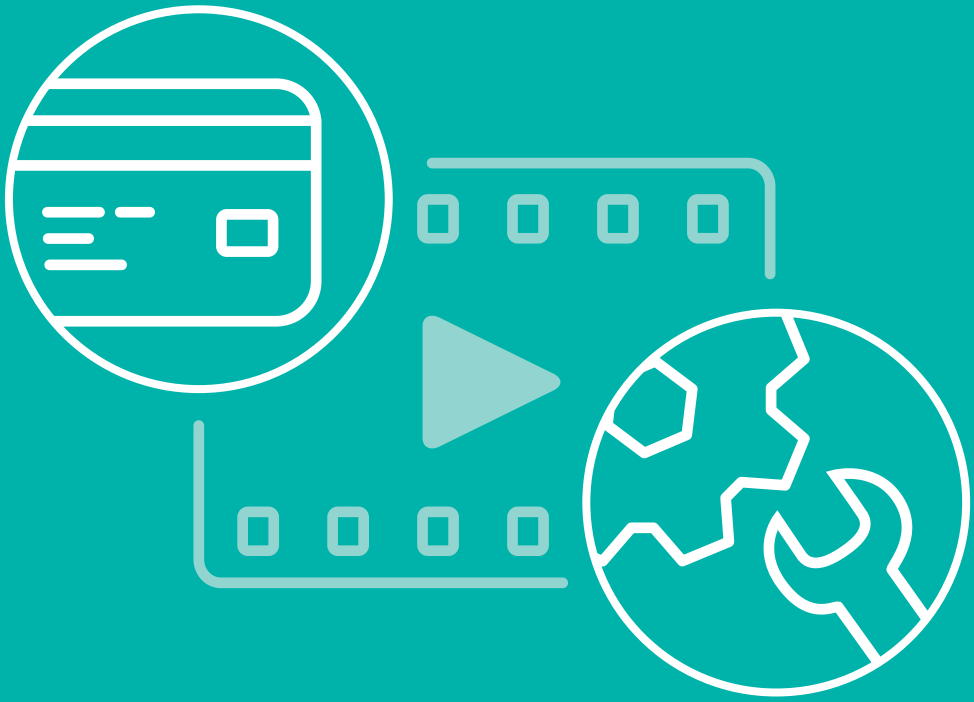
intertrust®

White Paper

Media Solutions

Weighing Buy Versus Build Options for Securing Advanced OTT Video Services



High Performance and Low TCO are the Winning Combination

Contents

Introduction

Online distributors of high-value video are finding themselves in a radically transformed marketplace. Questions on how to provide adequate content protection both now and in the future have moved from the engineering to-do list to the strategic front burner.

The transition of over-the-top (OTT) premium video distribution to mainstream equivalency TV services has saddled distributors with TV-caliber security requirements. Moreover, it has unleashed a wave of new challenges associated with authorizing multiscreen access to linear as well as on-demand content in HD and Ultra HD formats amid a surge of illicit activity by professional pirates and consumers alike.

What are the considerations for deciding on an approach to meet these challenges? First, determine which of the two main paths to develop protection can compete in this new environment:

- One path is selecting an approach that involves in-house creation, operation, and timely updating of a content protection infrastructure. This must support all the digital rights management (DRM) platforms and enhanced protection requirements of an increasingly fragmented device ecosystem.
- The other approach relies on a multi-DRM cloud service platform operated by specialists dedicated to ensuring every base is covered in a rapidly evolving OTT environment.

The purpose of this paper is to provide guidance to strategists who are searching for an answer to the buy versus build question. Our analysis begins with examining the market conditions that are determining the parameters for what must be done. This is followed by an exploration of the best way forward based on a consideration of all the issues that must be weighed in the buy versus build decision-making process. Given the rapid industry changes, a new evaluation makes sense regardless of the level of experience a company might have in the online video business. The ascension of content protection to make or break status impacts companies already offering OTT services as much as it does new entrants.

No one can succeed in this competitive marketplace without a robust content protection strategy that reaches across all targeted device categories and localities. Nor can any service thrive without satisfying the licensing requirements of suppliers whose content is essential to maximize the appeal of that service.

Equally important, success depends on meeting customer expectations. Users can grow frustrated and quickly abandon a service if they have trouble gaining access to protected content they are authorized to receive.

The approaches OTT distributors take today will determine their prospects for success in the future. They must be equipped to:

- Provide support for whichever DRM platform is suited to enable access to content on a given device, including any device that lacks native support for DRM protection
- Maintain performance through all the needed steps involved with enabling authorized access to any content in the service provider’s portfolio for each viewing session
- Meet the scaling and low-latency provisioning challenges that come with protecting high-profile live content
- Deliver protected content to any new devices entering the marketplace at any point in time
- Satisfy all existing and emerging licensing terms as they apply to the device, video format, or user location
- Adapt to any new developments in DRM and related technologies

In a nutshell, the buy versus build question turns on two key issues that apply over the lifespan of any OTT video service: Total cost of ownership (TCO) and performance. Is it possible that the least expensive approach could also produce the best performance?

Part 1
Market Drivers Shaping the New Content Protection Infrastructure

As the worldwide explosion in OTT video streaming services intensifies, so does the risk of failure. As a result, distributors must do everything possible through the implementation of rigorous content protection to minimize risks.

The Irresistible Force of Market Demand and Opportunity

Judging from the pace of OTT market growth, there's ample upside incentive to take on the challenge. Revenue generated by global streaming services in 2018 totaled $68 billion, up $30 billion or 79% from 2016 with 53% generated by subscription fees and the remainder accruing from advertising according to Digital TV Research.[1] The US accounted for $26.8 billion or 39% of the total, which is by far the largest share of any country (see Figure 1).

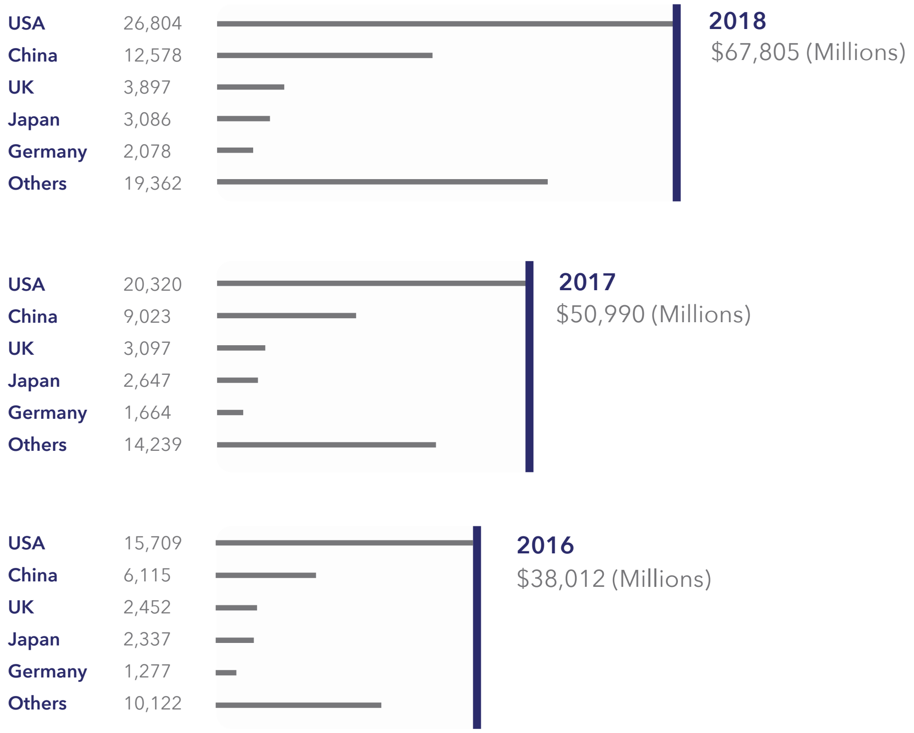
The percentage of video viewing time going to OTT content is surging in tandem with the revenue numbers. According to the researcher Statista, currently this averages to $23.22 per subscription worldwide.[2] Globally, viewers are spending an average of 6.8 hours per week consuming OTT video, with the US topping the national averages at 8.55 hours according to a report from CDN operator Limelight Networks.[3] Globally, among those who view video of any type online, the average number of OTT subscriptions per viewer is 1.2 with the US in the lead again at 1.7 (see Figure 2).

With a new wave of OTT services like Disney+, AT&T's HBO Max, Apple TV+, and Comcast's Peacock entering the US market and many others sprouting up across the globe, there's broad consensus among researchers and investment analysts that revenue totals and viewing metrics will continue to surge. Digital TV Research (in a projection shared by many) states global OTT revenues will reach $159 billion by 2024, doubling from 2019.[4]

Increasingly, OTT distributors are targeting audiences beyond their countries of origin. For example, one fourth of European OTT services are pursuing cross-border audiences according to research conducted by Media Asset Capital.[5] Worldwide, the cross-border reach enabled with OTT distribution has become a driving factor behind the explosion in online video services according to a report on global trends from Parks Associates.[6]

Figure 1.

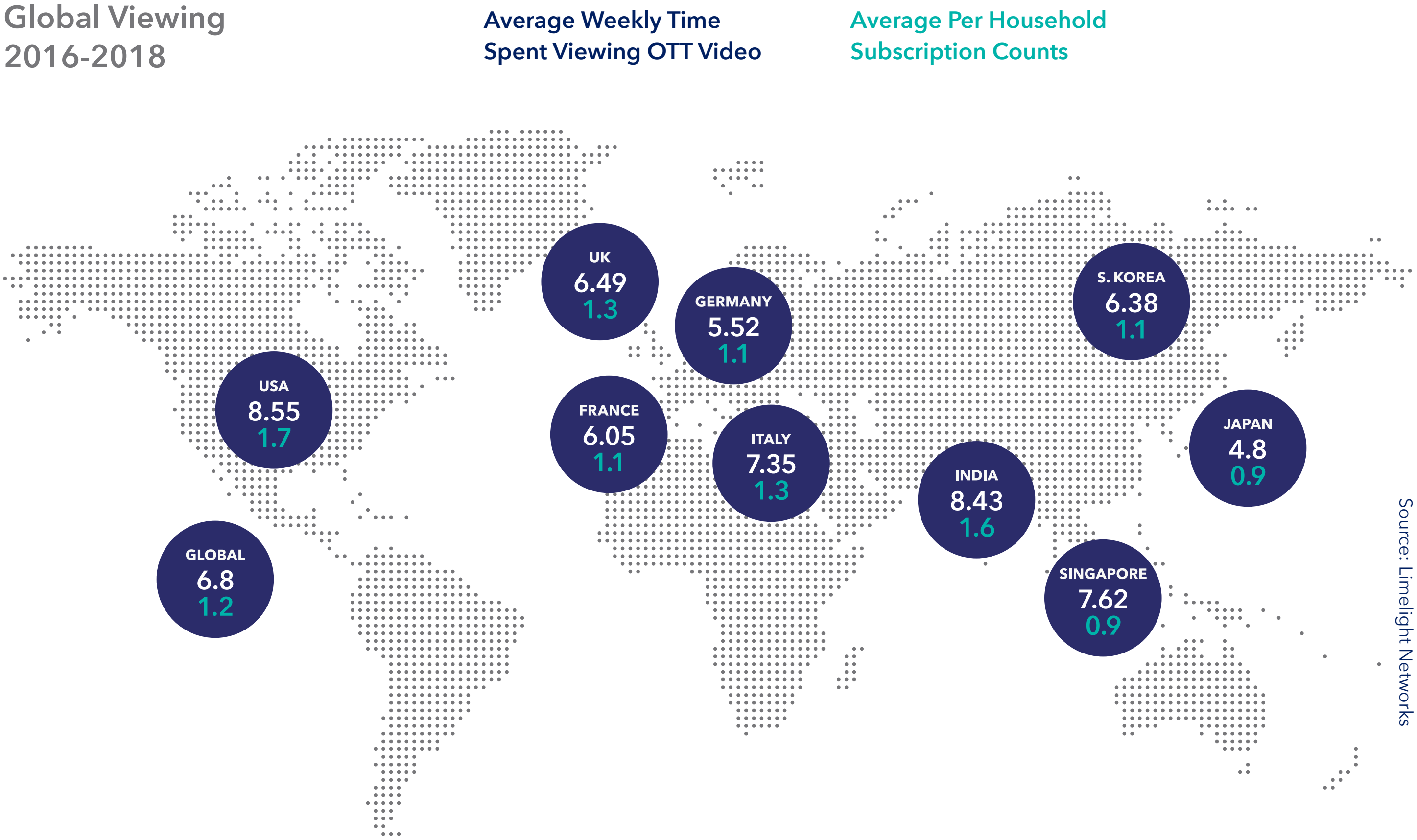
Global OTT Revenues 2016-2018



Source: Digital TV Research

Figure 2.

Global Viewing 2016-2018



Source: Limelight Networks

Amid surging rates of pay TV cord cutting, multichannel video programming distributors (MVPDs) and everyone else with a stake in video distribution are feeling the compulsion to join the OTT stampede. Already the global OTT subscriber count of 613 million is topping cable's 556 million according to the Motion Picture Association of America.[7]

Tier 1 network operators like AT&T, Comcast, Dish, Sky, Vodafone, Orange, Deutsche Telekom, SK Telecom, Telkom Indonesia, NTT Docomo, and many more have made big investments in OTT services, often with cross-border audiences in mind. With video usage on mobile growing at a rate of 50% to 60% annually over the past five years, forecasts from the Mobile Video Industry Council suggest video will eventually account for 90% of 5G traffic.[8]

The question is in such a crowded field where there's no choice but to join the fray, what does it take to ensure the flexibility to license content essential to building audience appeal with assurance the user experience will meet expectations? There are many factors that come into play with any attempt to answer this multifaceted question. The answer starts with having a content protection infrastructure in place that supports achievement of business goals, because if it doesn't, all bets are off.

The Implications for Content Protection

Any assessment of how to structure execution of content protection for success in the OTT TV business requires an understanding of the requirements imposed by today's market conditions, and how those requirements might change as conditions evolve. A good place to start is with the pace of device fragmentation and what that says about the protection challenge.

Challenges Posed by Device Fragmentation

Device proliferation and fragmentation is a big challenge for OTT video distributors and extends across smartphones, tablets, PCs, TVs, and TV media players. Looking at just smartphones and tablets, device tracker ScientiaMobile reports fragmentation has been increasing at a rate of about 20% annually for many years, culminating in an astounding 63,000 device profiles as of mid 2019 (see Figure 3).[9] Any attempts to limit targeted device profiles to the most popular models (as reflected in the Figure 3 smartphone data) severely curtails potential market reach.

In terms of global averages, smartphones have become the most widely used devices for viewing online video of all types, while PCs and smart TVs, or TVs using IP media players remain the preferred platforms for viewing long-form video in most regions. The relatively even spread of video consumption across device categories is reflected in percentages derived from data in the previously cited report from Limelight Networks (see Figure 4).

The lion's share of these devices natively support one of three DRMs associated with the dominant operating systems: Apple FairPlay Streaming with iOS, macOS and tvOS, Microsoft PlayReady with every Windows device and some Android devices, and Google Widevine with every Android device.

But any distributor that wants to maximize reach must also take into account that there are still a significant number of devices natively equipped to support the Adobe Primetime DRM, and others that don't support any of the DRMs that have been certified under current licensing policies. And there's also a vast ecosystem of devices (primarily in Asia with some in Europe as well) that natively support the open standard Marlin DRM.

Distributors also must contend with the fragmentation within the generations of operating systems. This impacts how distributors interact with OEMs and DRM suppliers who are authenticating the devices for the access of premium content. To ensure consumers can access content on whatever device is at hand, distributors must be able to sign in to the core security embedded in the device's OS or in the OEM's chipsets.

This is especially challenging when it comes to dealing with Android devices, which in the smartphone sector accounts for 87% of the global user base according to International Data Corp.[10] There are now six Android OS versions running on anywhere from 4% to 37% of the Android device base and over 24,000 different models of devices running on those OS versions as reported by both AppBrain[11] and OpenSignal.[12] And even with Apple, where there are only a handful of device models, there are differences that must be addressed from one generation of OS to the next.

The Impact of Content Theft On Enhanced Protection Requirements

Trends in Piracy

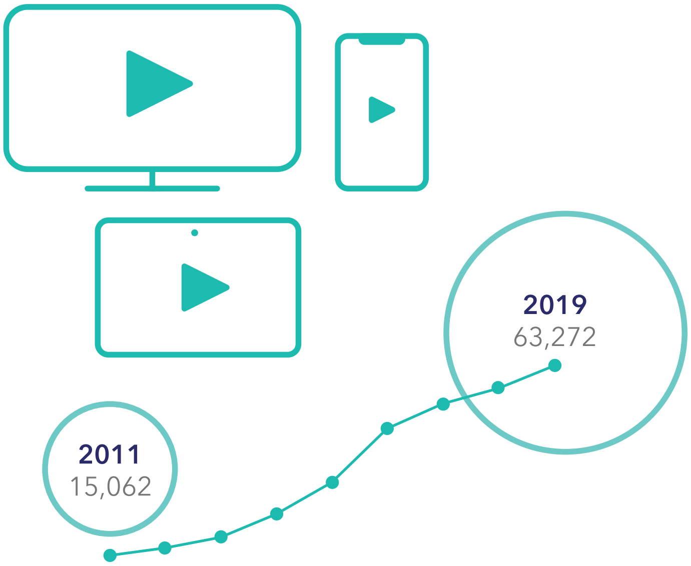
While today's DRM systems utilizing an Advanced Encryption Standard (AES) of 128 or better ciphers make it nearly impossible for hackers to derive the encryption keys through brute force attack, online piracy is flourishing at unprecedented levels. Global losses in subscription and advertising revenue attributable to online piracy exceeded $37 billion in 2018 according to Digital TV Research.[13] Growing alarm over these losses is prompting enforcement of new licensing terms that increasingly incorporate requirements tied to the Enhanced Content Protection (ECP) specifications produced by MovieLabs, the motion picture industry technology consortium.

Pirates can now easily capture and retransmit sports and linear TV channels in near real time. In some cases they record and retransmit video directly from large TV screens. With the high resolution and quality of today's HD and UHD displays, this results in a surprisingly good viewing experience for pirate site users. An even more robust viewing experience is attained with the use of high-bandwidth digital content protection (HDCP) strippers, which makes it easy to pull unencrypted video right out of the HDMI link.

Recently, YouTube Live, and Facebook Live have become centers of illicit activity as well. Pirates are posting stolen content from TV shows and entire movies. And there's a growing number of illicit sports viewing occurring with consumers restreaming video from their smartphones and tablets.

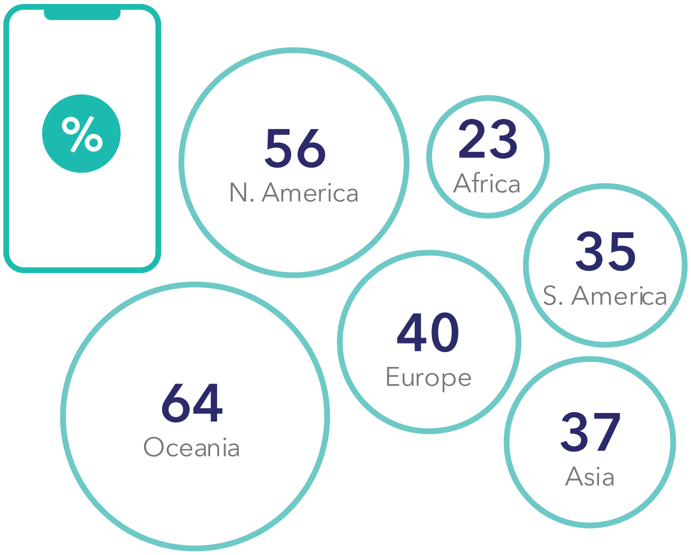
Figure 3.

Internet-Connected Device Profiles



Source: ScientiaMobile

Global Totals 2011-2019



Source: ScientiaMobile

National Smartphone Usage Driven by Top 21 Smartphones

The Expanding Application of ECP in Content Licensing

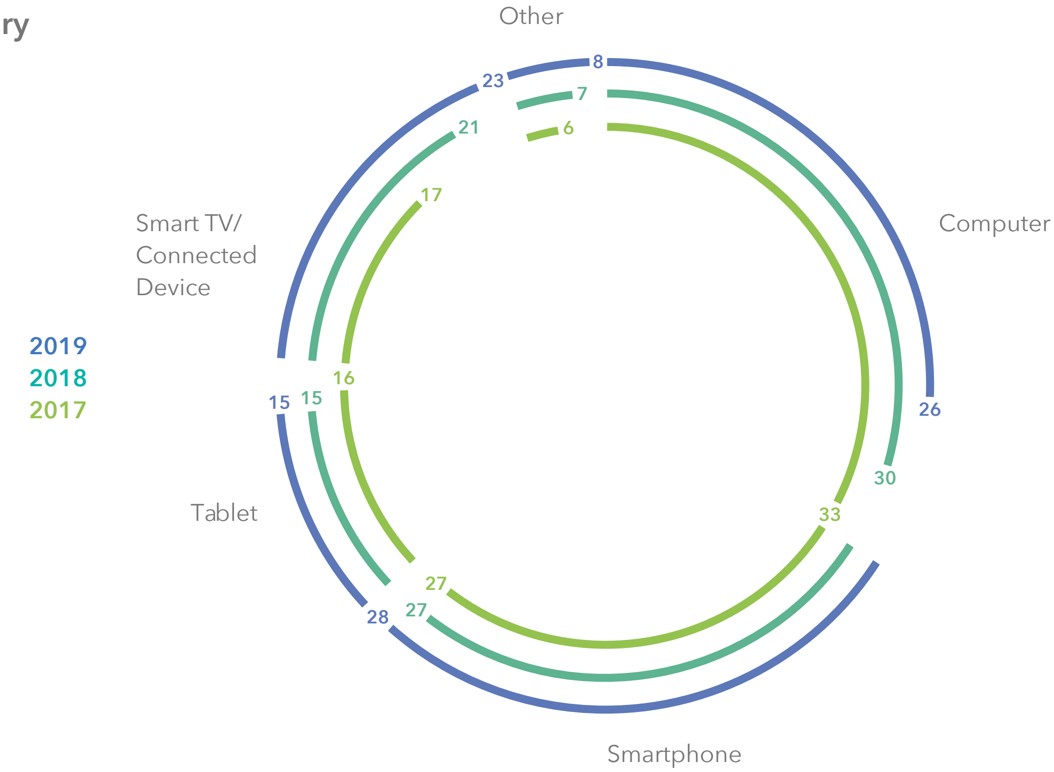
The emergence of 4K/UHD and improvements in display quality enabled by high dynamic range (HDR) modalities are big factors behind the licensing policies that require enhanced protection against piracy. The slow ramp up to UHD-formatted video services is giving way to rollouts worldwide, which are being driven by mass market penetration of UHD TV sets and widespread recognition that HDR provides a better viewing experience.

According to Futuresource Consulting, global shipments of UHD sets will account for 52% of the market by 2020. At this point the vast majority of television households in North America, Western Europe, Japan, South Korea, and many other parts of the world will be watching TV on big displays.[14] Support for UHD and HDR is very important to the OTT providers' ability to compete.

So far, the dominant sources of UHD content have been OTT providers including Netflix, Amazon, Hulu, UltraFlix, Fandango Now, VUDU, iTunes, and YouTube. Nearly all of the original content produced by Netflix and Amazon is offered in UHD, and much of it is enhanced with HDR. Along with connected smart TVs, streaming media players (SMPs) that bring OTT content to TV sets are becoming a big factor in the expanding role of UHD in this market.

Figure 4.

Global Averages of Video Viewing Time Device Category



Source: Limelight Networks

In 2018, for the first time more than half of the SMPs shipped in North America and Europe were equipped to support UHD, which was expected considering the shipment tallies for Asia in 2019, according to S&P Global Market Intelligence.[15] Notably, live sports coverage has become a major driver behind UHD penetration in OTT services as evidenced by Eurosport's recent agreement with Amazon supporting OTT distribution and its heavy schedule of UHD coverage.[16] In light of these developments, distributors shaping content protection strategies to fit current market conditions can no longer look on the ECP specifications issued by MovieLabs as something to worry about in the future, but they have to support them now.

While some of these requirements have long been met in content protection solutions on offer from leading vendors such as with the random generation of encryption keys and use of AES 128, others represent new challenges, especially in the unmanaged OTT domain.

The most prominent new requirement involves use of forensic watermarking. Originally seen as a tool against theft of UHD content and movies during early release windows, watermarking is now becoming part of licensing requirements for high-value HD content as well, especially when it comes to battling live sports piracy.

Challenges Posed by Live Sports Streaming

Market Responses to Surging Demand

Beyond the watermarking-related processes attending action against pirated sports streams, OTT distributors must be mindful of how live sports streaming impacts their ability to use DRM-based protection, without impeding user experience. For any distributor, the rising popularity of streaming sports is making these services essential to subscriber acquisition and retention.

In response to consumer demand, inclusion of sports in linear OTT services has become pervasive. The NBC Sports airing of the 2016 Summer Olympics shows just how important demand is to overall success. The network reported a drop in traditional TV viewing of the 2016 games compared to the 2012 games, but the amount of time viewers spent watching streamed coverage nearly doubled the time spent with the 2012 London Summer Olympics and 2014 Sochi Winter Olympics combined.[17]

Since then sports programming has become a part of leading OTT TV service bundles worldwide, drawing ever larger audiences to online consumption. For example, Amazon, which launched live streaming of Thursday Night NFL Football, Premier League soccer and other high-profile events in 2017, has seen big gains in viewer participation, including an 86% increase in NFL game streaming rates in 2018 with some games reaching 2.4 million viewers.[18]

Far greater numbers of viewers are generated by championship events like the FIFA World Cup, Super Bowl, and Cricket World Cup. The all-time record for concurrent views was set in 2019 when 25.3 million users tuned into Indian distributor Hotstar's coverage of the Cricket World Cup semi-final.[19]

The Risks of Poor Performance in Content Protection

With the expansion in online sports coverage, subscribers often have multiple options to get quality delivery if their chosen suppliers aren't up to the task. This means that if a distributor wants to retain the sports enthusiasts in its subscriber base, it must be sure its DRM operations can support the massive audience surges often associated with these events.

If viewer authorization and key distribution processes can't be supported by available server capacity, viewers will experience the kinds of delays that can lead to subscription terminations.

Of course, delays incurred with content protection aren't the only cause for subscriber dissatisfaction, which can also be triggered by buffering delays or sub-par display quality.

Part 2
Finding an Answer to the Buy Versus Build Question

Clearly, when it comes to assessing today's content protection challenges, newcomers to OTT streaming aren't the only ones facing the need to rethink old approaches. No matter what type of service strategy is in play, execution of content protection for current and future needs will require a wide range of new capabilities in order to deliver content that can draw targeted viewers, which is essential to maximize audience reach.

The overarching question is how best to achieve these goals: Either building and operating a content protection infrastructure in-house or by using a system operated at global scale by a market-proven cloud service. Ultimately, the buy versus build decision comes down to determining the total cost of ownership (TCO), factoring in immediate and long-term CAPEX and OPEX and calculating the difference between costs saved and costs incurred through any compromises on performance.

The TCO analysis begins with an assessment of the technology and infrastructure requirements that must be met to achieve performance matched to current and future service goals. The requirements spelled out in the following sections are generally applicable to any service strategy involving licensing of high-value TV programming, movies, and other long-form professionally produced video content for distribution to a fairly large segment of the consumer market in multiple countries. Of course, elements pertaining to support for sports and other linear content don't apply to distributors pursuing purely on-demand service strategies.

With articulation of the requirements for a given service strategy, planners can assess what it will take in terms of staffing and organizational structuring to build and manage the content protection infrastructure. With this knowledge, the buy versus build question pivots on two things: Can all requirements be met through reliance on a cloud-hosted service, and if so, how does the buy TCO compare with that of the build option?

Technology and Infrastructure

The Multi-DRM System

In light of the market conditions spelled out in Part 1, the only manageable approach for delivering protected content across the fragmented device ecosystem involves implementation of a multi-DRM platform. Otherwise, distributors must maintain separate silos for processing each asset for distribution under each protection regime.

Some Progress Toward Simplification
Fortunately, the industry has reduced the complications attending multi-DRM support to some degree with adoption of the Common Encryption Standard (CENC) as a component of the adaptive bitrate (ABR) streaming standard MPEG-Dynamic Adaptive Streaming over HTTP (DASH). CENC enables a uniform approach to providing encryption keys for execution of PlayReady, Widevine, Adobe, and Marlin DRM on devices that natively support MPEG-DASH, as well as devices that access the content through browsers that support the streaming protocol including Chrome, Microsoft Edge/Explorer, and Mozilla Firefox.

With both Microsoft and Adobe supporting DASH in clients tied to their software, usage of Microsoft's Smooth Streaming and Adobe's HTTP Dynamic Streaming (HDS) has largely given way to DASH. However, because Apple does not support DASH, content sent to Apple devices with native support for FairPlay must be packaged for streaming over Apple's HTTP Live Streaming (HLS) format.

Along with reducing the number of streaming platforms that must be used to reach the vast majority of devices to just DASH and HLS, the industry has come up with another way to mitigate incompatibilities through adoption of Common Encryption, Standardization of MP4 containers, and the Common Media Application Format (CMAF) standard. CMAF makes it possible to tap CENC for assignment of encryption keys for FairPlay along with assignment of the other DRM keys supported by CENC in DASH.

This is possible because CMAF encapsulation is compatible with HTML5 Encrypted Media Extensions (EME), which defines a common API that can be used with CENC to discover, select, and interact with DRMs. Rather than defining DRM functionality, EME standardizes the discovery hooks, moving the responsibility for such interactions from plugins or third-party applications to HTML5-compatible browsers. These include all the major browsers except the Safari Mobile browser used with iOS devices.

Unrelenting Increases in Complexity

More broadly, despite efforts to simplify implementation of multiple DRMs, the level of complexity building a content protection infrastructure suited to enforcing usage, regional blackouts, and other policies at every point of access is greater than ever.

The platform must be able to ensure consistency in user experiences across all devices with delay-free acquisition of keys from DRM servers run by multiple licensing authorities. Keys have to be provisioned on a per-session basis in accord with all the nuances that differentiate DRM systems. This includes the various generations within those DRM systems, including types of encryption methods and file formats used for conveying licenses and policy information.

In the case of linear TV content delivered over OTT connections, licensors typically require that keys be refreshed multiple times during a viewing session. Moreover, the system must support instant delivery of keys and licensing enforcement policies whenever a new program is accessed, allowing users to switch from one live channel stream to another just as they do in the legacy TV viewing experience. Provisioning and security upgrade processes associated with these interactions must be rigorously secured in accordance with established industry practices.

Increasingly, multi-DRM operations involve integration with CDN infrastructure in conjunction with implementation of just-in-time edge processing capabilities that can be applied to speed DRM provisioning and forensic watermarking as well in latency-sensitive situations. As such options gain traction, the ability to work with CDN operators as partners in content protection will become essential to maintaining a competitive advantage.

It's also important to note that additional usage rights policies can come into play when live streams are provided with automated support for time shifting by end users, including catch-up viewing in limited time windows and cloud-based DVR options utilizing long-term storage facilities. Distributors must be sure their system recognizes whether their licenses cover such use cases and that the appropriate protections are provided when they do.

Distributors may also want to support off-line access to content, which can be enabled with a download option or through the use of local device storage to capture streamed content for later viewing. Here as well the protection system must be able to determine whether content licenses permit such options and apply the required protection accordingly.

ECP Parameters Now in Play

Beyond the basic technology requirements of a Multi-DRM platform (as noted in Part 1), distributors must be prepared to exercise content protection in accordance with licensing policies that may implement one or more requirements tied to Enhanced Content Protection (ECP) specifications.

In the case of DRM-based protection, requirements can include rules specifying that hardware roots of trust (HWRoT) be used to associate unmanaged devices with a distributor's service at the chip level. In most cases this involves access to the codes implemented in tandem with the ETSI key ladder standard or its SMPTE variation, the Open Media Security key ladder.

Access can be enabled in either of two scenarios: One where OEMs have exposed HWRoTs for direct access by third parties or one where supplying authentication keys requires access to HWRoTs exposed by the security provisioning processes of OS-specific app stores.

Another complication occurs in cases where content producers impose the ECP requirement that third parties certify new OEM device models are in compliance with industry security standards. Under these rules, distributors must have processes in place that flag any new devices entering their domains to determine whether they have been independently certified before authenticating them for service reception.

Figure 5.

How Technology Requirements Impact the Buy Versus Build Decision

Issue	Buy Option	Build Option
DRM and content security expertise	Included in service, usually covering Apple FairPlay Streaming, Microsoft PlayReady, Google Widevine, sometimes Adobe Access and Marlin DRM	Hire and retain staff with niche security expertise and end-to-end experience of each DRM that will be deployed
Global infrastructure	Cloud-providers like AWS offer global footprint with regional geo-redundancies and fault tolerance, minimizing service delivery latency	Contract with a cloud-provider and absorb the full cost of dedicated capacity, or invest in private cloud infrastructure or on-prem systems with CAPEX/OPEX consequences
Device and OS fragmentation	Managed by DRM provider through a cross-platform client SDK, or by using native DRM clients	Develop and maintain client device security libraries for iOS, Android, Windows, and Linux, or resort to using native DRM clients
Following a road map that stays ahead of developments, including new standards	Effortless since this is part of the DRM provider's core activities, with new releases at regular intervals incorporating the latest security features activated automatically as part of the SaaS	Building a content security system is not a one-off project; a continuous effort and investment is required to stay ahead of constantly evolving piracy threats and security technologies

Forensic Watermarking

Forensic watermarking processes used with identifying pirate sources have become more complicated than they were when the primary focus was on recently released movies formatted in UHD for on-demand access. Now the requirements have been extended to other forms of high-value UHD content as well as some HD programming, especially when enhanced with HDR.

There are many nuances in the application of forensic watermarking technology that distributors should bear in mind when it comes to choosing a supplier. A big one has to do with the surge in piracy of live sports streams and other high-profile linear programming. This introduces the need to quickly identify and disrupt such streams early in the session to maximize the impact of disruption on users' willingness to rely on pirate sources.

This requires acceleration of all the steps used to identify and act against pirate sources. Along with the initial identification of illicit streams, forensic recovery of watermarks, and identification of pirate sources, speed is essential when it comes to notifying entities, including ISPs and CDN operators who are in a position to respond to theft whether through warnings to users or actual disruption of the streams.

Protecting Watermark

Further complicating matters is the fact that pirates are constantly coming up with ways to defeat the effectiveness of watermarks, even when (as prescribed by MovieLabs) they are undetectable. Recent approaches to attacking watermarking effectiveness include intermittent blurring; chopping off the top and bottom of the screen; random combining of multiple streams of the same piece of content into a single stream in a process known as collusion; and hacking of the service app to alter the identity of the perpetrator.

Another technique focused on OTT streams involves obscuring the source identity through direct penetration of the distributor's client app. In such cases, the watermark remains intact but becomes associated with a phony ID. As a result, app shielding and protection have become another component of the new content protection regimen.

Summarizing the Buy Versus Build Implications of Technology Requirements

The discussion so far points to several conclusions in the buy-sell analysis as summarized in Figure 5. Clearly, there's a lot to deal with on the build side that is taken care of under the buy option, which leads to an assessment of the organizational implications for the do-it-yourself (DIY) approach.

Organizational Requirements

Looking at the OTT video service provider's personnel needs and organizational structure for an in-house build, it's clear the requirements go well beyond what was once needed to provide support for securing high-value video. As summarized in Figure 6, there's reason to ask whether it makes sense to create the organizational framework if all the essential tasks can be fulfilled by a third-party provider of a fully equipped content protection service.

A realistic attempt to answer this question will encompass the full organizational implications of the in-house approach, which means looking beyond the early build phase to the levels of staffing and expertise that will be required over the long term. Examples of miscalculations about ultimate staffing needs abound.

Often new entrants get off to a quick start by focusing their content protection apparatus on what's needed to deliver a service to the Apple OS ecosystem of smartphones, tablets, MACs, and TV sets. They quickly discover that building a content protection infrastructure suited to delivering support for a single DRM, namely Apple's FairPlay, over an HLS streaming platform serving a relatively small range of device models doesn't prepare them for the needed steps to expand protection beyond the Apple domain.

In truth, distributors who want to build and operate their content protection infrastructures in-house must establish an organizational unit consisting of experts in every facet of product development, testing, and management. Backed by ongoing investment in R&D, they must be able to ensure every technology component stays current with evolving standards, device hardware, OS versions, licensing policies, and service configurations. And there will be a need to hire additional personnel to handle routine tasks that tax existing staff resources, also taking into account the need to provide 24/7/365 technical support.

Staffing Requirements Related to the Initial Build Phase

One of the most challenging tasks when building the content protection infrastructure comes at the outset. In order to create a multi-DRM operational environment that obviates the need for separate asset management and protection silos tied to each of the major DRMs, system architects must be able to create an abstraction layer that can automatically execute the requirements spelled out in the previous section, with minimal manual intervention.

For example, different DRM systems utilize different rights languages. Hence, expertise is necessary to ensure that a system translates a given set of rights equivalently across the rights languages of all the different DRMs. This ensures that the end-user experience on all corresponding devices and browsers is consistent.

Figure 6.

How Organizational and Staffing Requirements Impact the Buy Versus Build Decision

Issue	Buy Option	Build Option
Staffing	Major staffing adjustments are avoided when distributors take advantage of a multi-DRM service offered by a specialist in cross-platform, cross-DRM, and security technologies	Hire and fund a dedicated in-house team of first class security experts including product management, engineering, development, testing (QA), documentation, and training
System Software & DRM Upgrades and Maintenance	Included in SaaS and automatic; always benefit from latest releases	Manage bug-fix updates and platform upgrades, including complex cut-overs and fallback scenarios
Technical Support	Benefit from 24/7/365 vendor support	Hire, fund, and retain a dedicated in-house support team

That may be easier said than done. Most DRM systems have steep learning curves and a limited amount of learning and training material. The challenge is further exacerbated by lack of training courses. If they are offered at all, they may be given only a few times a year. One possible approach is to recruit staff with specific DRM skills, but given the niche characteristics of the content security industry, such staff is not only hard to find, attract, and hire, it comes with high costs. This difficulty is made worse by staff turnover. Once the new content security system has been developed, talented staff may look for new challenges elsewhere and move on.

In designing the system for instantiation on in-house servers, the team must have the IT skills essential to capitalize on the latest advances in data center virtualization technology. This is important not only for maximizing in-house resource efficiency, but also for tapping into advanced virtualization modes employed by public cloud compute systems when service usage exceeds private data center capacity.

The in-house build also requires integration with a multi-DRM client player that can provide assurance that all licensing policies will be adhered with every viewing session. Using a secure player enables the platform to immediately react to the security requirements of the device used in any given viewing session, whether it's a hardware-secure device utilizing a root of trust or an open device requiring implementation of device-specific DRM protection.

A well-designed single player overcomes the inconsistencies of native players by providing the entitlement checks, permissions enforcement, device integrity verification, output controls, and other client-side functions essential to unified security management on all devices. A well-designed player must be designed so that it can optimally work in tandem with the functions related to authentication, trust verification, and key exchange as executed by different core logics across the device ecosystem.

Staffing for Continuous Operations

Managing consistent performance of an advanced content protection infrastructure entails a vast range of responsibilities. Once the system is built, there's a need to maintain relationships that started in the initial build phase, including those with SoC manufacturers, device OEMs, software system suppliers, and licensing authorities. Operations personnel must also be vigilant in tracking new developments with devices, DRMs, operating systems and browsers.

A key operational aspect is to ensure technical support is available 24/7/365. This entails assigning resources to three 8-hour shifts, thus requiring at least three dedicated support staff. In reality, given vacations, sick leave, and other administrative issues, the staffing level would need to be twice that to ensure continuous 24/7/365 support availability. This challenging and costly responsibility is a key reason why operators generally prefer to outsource the content security operations to a third-party that provide the required 24/7/365 support as part of a service level agreement (SLA).

Another aspect is to ensure the in-house developed content security components will fulfill the stringent (ECP) requirements of content providers for premium content licensing. To prove compliance with those requirements, the security system will need to undergo periodic third-party security audits. Such audits are complex and time consuming (apart from the associated cost)—another reason for buying and/or subscribing to a content security service from a company that will also assume responsibility for the security audits.

Data Gathering and Performance Monitoring

Validating license policy enforcement has long been a required component of OTT distributors' engagements with content providers. Like everything else about content protection, this also has become more complicated as distributors find themselves encumbered with the need to follow and document adherence to expanding lists of contract terms from ever more content providers.

Old approaches to setting up and managing auditing procedures where results are tabulated in periodically issued hard-copy reports on contract fulfillment must be replaced with more persistent, verifiable accounting processes. This entails establishing credible, highly automated mechanisms for auditing and electronically reporting back to content providers on performance in all areas of policy enforcement.

Heightened data aggregation and analytics capabilities also come in to play with the use of watermarking. And as discussed earlier, the ability to immediately identify offending individuals and implement remedial action in time is critical to disrupt recipients' viewing experiences. This is critical to making users aware that the risk of relying on illegal sources is not worth it. This requires coordinated efforts across the supply chain to collect, share, and analyze forensics data.

Responding to New Developments

Beyond the regular updates intrinsic to day-to-day operations, the content protection unit must be able to respond to the major shifts in technology and market trends that will impact the platform. Over time, changes in encryption standards, decryption protocols, streaming technologies, ECP requirements, browsers, and much more will require the same level of expertise that went into building the platform.

For example, release of a new OS can require augmenting DRM clients with new approaches to verification, data reporting, and other security mechanisms. New DRMs or new approaches to orchestrating multiple DRMs will require major platform adjustments. And there will be new security requirements associated with emerging video formats such as 8K UHD and virtual reality.

Figure 7.

How the Total Cost of Ownership Impacts the Buy Versus Build Decision

Issue	Buy Option	Build Option
Expenditure Type	Security as a Service = OPEX	Development = CAPEX Running system day-to-day = OPEX
System Scaling	Pay-as-you-go business model scales up or down effortlessly based on needs with no risk or cost of over provisioning	Build a security system that is pre-provisioned to cater for the maximum number of concurrent users, incurring cost of spare capacity during non-peak periods
Service Launch, Time-to-Market	Quick time to market and taking advantage of flexible business models	Long wait if a new operator is going to build and deploy the DRM system first
Cost Effectiveness	Economies of scale enable better service at a lower price point as the infrastructure costs are amortized across multiple operators (multi-tenancy)	All costs borne by operator, whether on-premises or in the cloud

Total Cost of Ownership

Clearly, there are immense costs associated with the staffing requirements for the build-it-yourself option, starting with the CAPEX needed for the initial build process and any major platform adjustments in the future. There is also the OPEX spending on workforce execution of day-to-day operations. And, of course, there are CAPEX outlays related to equipment, software, and DRM-related licensing costs.

The R&D costs incurred in the initial protection platform build phase for a content-rich service operating at regional or global scales can run into the millions of dollars. Along with additional CAPEX related to basic hardware infrastructure, distributors also face other less obvious costs. On the buy side these costs, like all those related to platform construction and ongoing operations, are incorporated into the basic service fees.

For example, while competitive pressures have pushed DRM licensing fees associated with the core DRM logic to the vanishing point, there are significantly higher costs to be accounted for from the client side. When the distributor wants to make access to its services available to a new device entering the market, there's a cost for porting the distributor's secure player to that model, which can go as high as $250,000.

There are also what can be called agility-deficiency cost contributions to TCO related to the delays distributors will inevitably experience when it comes to integrating with new device models, implementing new DRMs, or other time-consuming upgrades. A cloud-based service provider has staffing resources and the benefits of lead time to prepare for new developments in advance of OEMs' and other entities' commercial rollouts of these new components.

As noted earlier, the final buy versus build decision (assuming equal effectiveness in execution of requirements with either approach) comes down to which approach leads to lower TCO. For analytical purposes, input from the managed service side of the equation depends on charges built into the initial and pay-as-you-go fee structures. For those specifics, the analysis offered here focuses on costs associated with Intertrust's ExpressPlay DRM™ service, as discussed in Part 3.

Regardless of the nuances in contract terms, the buy-side TCO benefits from the fact that all costs from build to operations and major upgrades are amortized across multiple distributors.

As we will demonstrate, the TCO incurred with the ExpressPlay DRM iteration of the buy approach makes it clear which option is in the best interests of distributors in the short term as well as in the future. Figure 7 provides a summary of how issues are addressed

Part 3

A Service That Makes the Case for the Buy Option

As the previous sections make clear, OTT video service providers have every reason to choose the buy alternative if they can satisfy the two previously stated conditions: Can they rely on a hosted service to meet all requirements, and if so, is the TCO associated with that option significantly lower than that of the build option?

Distributors can be absolutely certain of an affirmative answer to both questions when they examine the capabilities and TCO that come with choosing ExpressPlay DRM, the cloud-hosted multi-DRM, and the ECP support service provided by Intertrust. The answer to the question of whether ExpressPlay DRM delivers the functionalities necessary to cover all the bases of any OTT video service strategy a distributor might devise can be found in the scale and variety of OTT service configurations supported by ExpressPlay DRM worldwide.

ExpressPlay DRM is one of the most widely deployed multi-DRM technologies in the world, providing full turnkey support for OTT TV services. The service is supporting an average of 500 million viewers consuming six billion hours of programming monthly at a rate of up to 50,000 transactions per second per customer across several continents. On a single day in 2019, the platform supported 100 million activations during the Cricket World Cup, with peak usage registered at 23 million simultaneous sessions.

In one demonstration of the platform's status as a trusted provider of protection for the world's most popular content, ExpressPlay DRM is making it possible for 20+ million subscription video on demand (SVOD) subscribers in 13 countries across Asia to access content from 150 motion picture and TV studios worldwide. In the UK, the platform supports protected distribution of movies and TV shows from all the major studios for YouView, the combination of OTT and free-to-air service spearheaded by BT, TalkTalk, Arquiva, Channels 4 and 5, and other partners.

ExpressPlay DRM achieves global reach with robust, highly scalable usage rates for live and on-demand content through tight integration with Amazon Web Services (AWS). With deployment at multiple AWS facilities within each region, the Intertrust service leverages the cloud computing system's ability to automatically route requests for fastest action per session with automatic failover across all regions.

Figure 8.

ExpressPlay DRM High-level Workflow

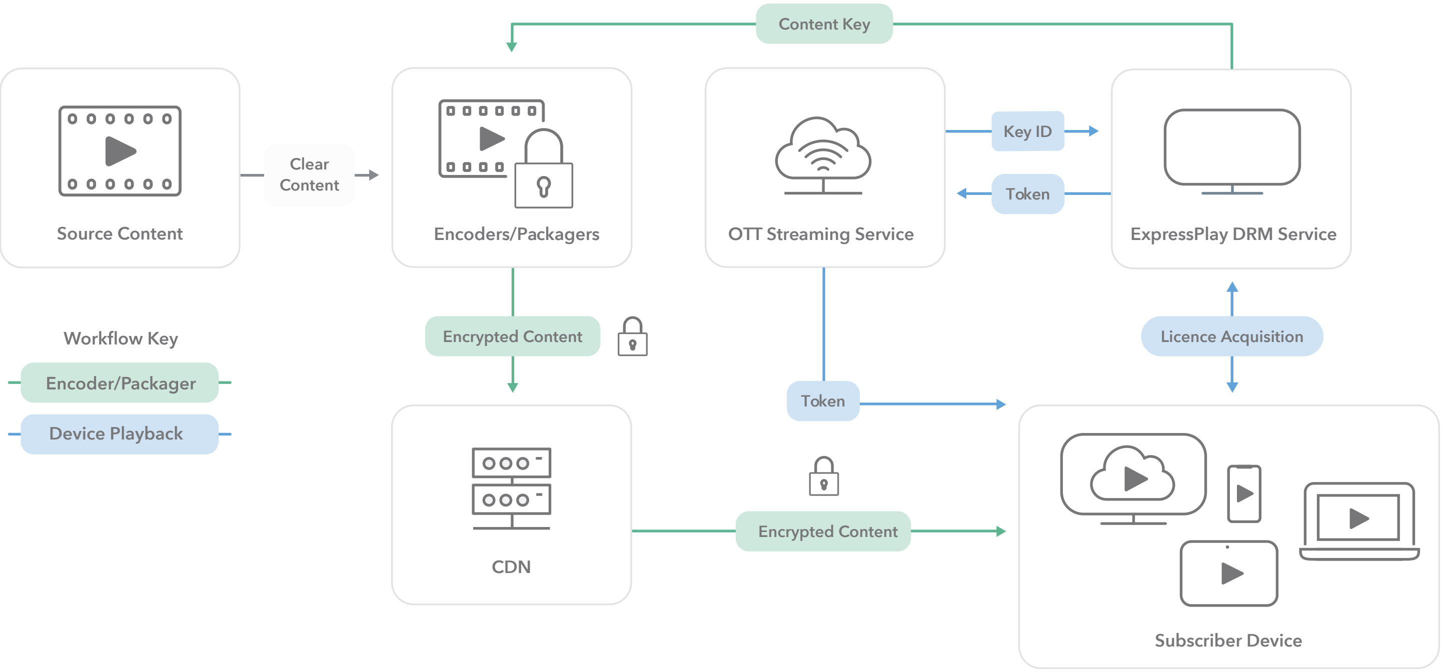
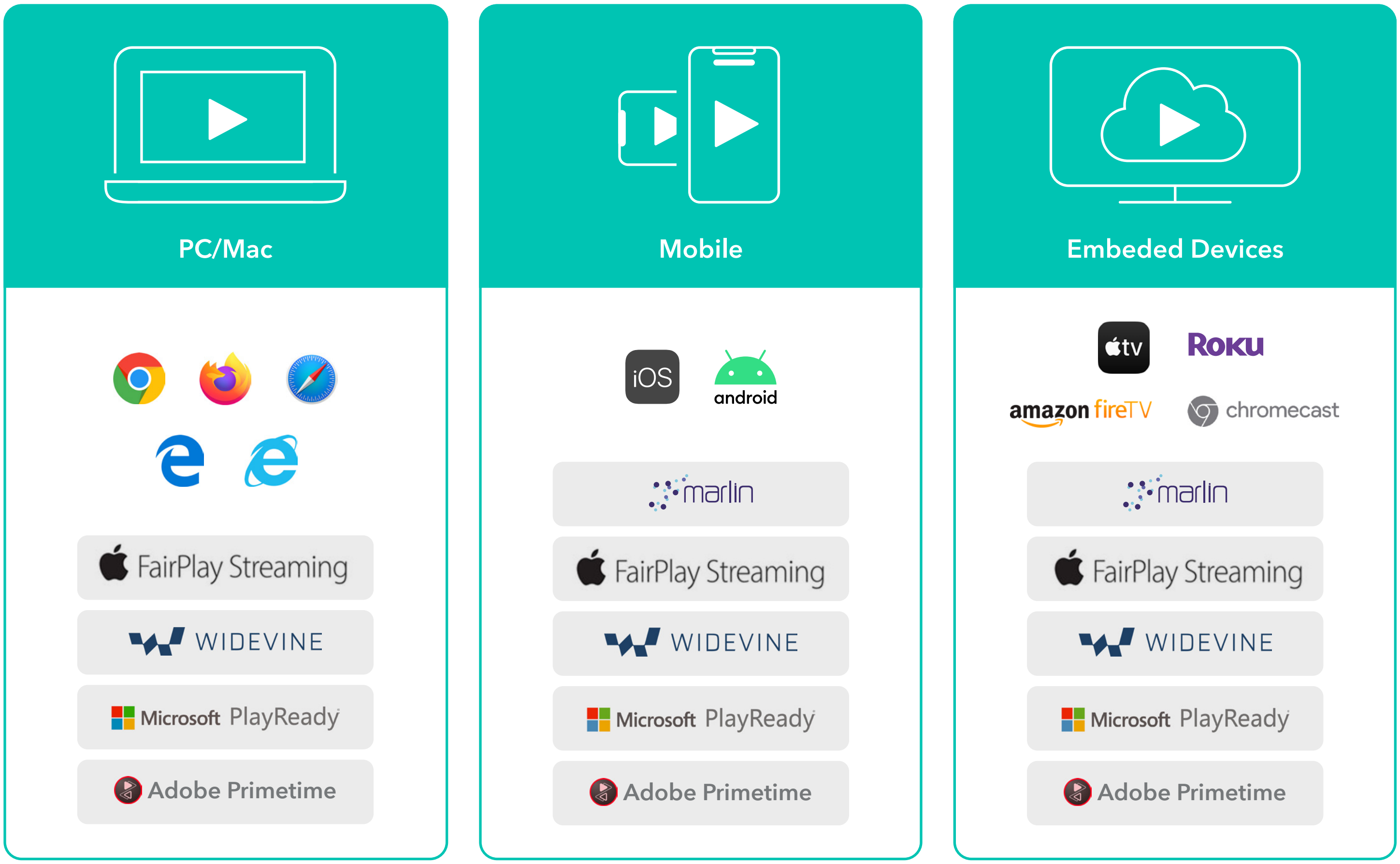


Figure 9.
ExpressPlay DRM Supports All Major Devices and Platforms



As shown in Figure 8, the platform covers all the essential basics of a multi-DRM service providing device credentials, content key storage, content encryption, secure playback with multi-DRM license delivery, and real-time generation of audit reports about the adherence to the licensing terms. Through a few simple integration steps, distributors can implement robust rights management for virtually any service scenario without adding new infrastructure or incurring any of the setup costs that accompany in-house builds.

The Unique Benefits of ExpressPlay DRM

Beyond supporting the basics of a multi-DRM service, ExpressPlay provides several significant benefits that are not collectively available through other platforms, including the previously referenced support for protecting unprecedented volumes of simultaneous live sports streams. Equally important, ExpressPlay is the only multi-DRM service that supports all major DRMs, including the open-standard Marlin DRM and Adobe Access, as well as Apple FairPlay Streaming, Google Widevine, and Microsoft PlayReady.

As shown in Figure 9, this comprehensive DRM support extends across all the major device and browser platforms.

The support for Marlin—the DRM Intertrust helped create as a studio-certified alternative to proprietary DRMs—is especially noteworthy. This is the case because Marlin is the native DRM on millions of devices in Asia and to a lesser extent other parts of the world. In all such instances, ExpressPlay DRM SDK is already pre-integrated in such devices. The support for Marlin also gives distributors the opportunity to provide high-level protection to devices that do not natively support a DRM that meets today's licensing requirements. Marlin can be implemented on these devices through the use of ExpressPlay DRM SDK.

Another vital benefit delivered by ExpressPlay DRM involves code protection and shielding of the SDKs at the source code level with tamper-resistant white-box cryptography. Attacks on apps (as mentioned in Part 1) are a growing source of industry concern and are thwarted with advanced shielding that hardens against static and dynamic analysis, hacking, and reverse engineering.

When allowed by licensing agreements, ExpressPlay DRM also provides protection for content uses not directly related to streaming. Options include support for secure download, offline playback, and device-to-device side loading as well as protection for content accessed in catch-up mode, especially in the case of live programming.

It's also important to note that Intertrust has taken initial steps toward responding to the emergence of advanced edge processing capabilities in CDN networks. Intertrust has integrated ExpressPlay DRM to take advantage of the just-in-time packaging capabilities supported by several CDN vendors. Furthermore, such integrations are possible, depending on customer demand.

Critically, ExpressPlay DRM makes it easy for distributors to adhere to the ECP specifications that content owners are increasingly applying in the licensing of high-value content. When it comes to executing watermarking, ExpressPlay customers can choose from two solutions that have been pre-integrated with the service including Friend MTS and ContentArmor.

Both solutions meet the basic ECP requirements for session-based forensic watermarking with robust support for tracking pirated streams, identifying sources, and rapidly responding to live stream theft. At the same time, they afford distributors an opportunity to optimally match their selection to specific needs based on nuances unique to each, which isn't possible with multi-DRM platforms that focus on one watermarking supplier.

ExpressPlay DRM also supports ECP stipulated integration of protection with Trusted Execution Environment (TEEs) and SoCs for UHD and HDR. This is done through Widevine Level 1 and PlayReady SL3000 as well as Marlin, which was designed not only to support TEE-based security, but also to meet the ECP secure video path requirements.

Addressing Future Needs

As reflected in all the capabilities intrinsic to ExpressPlay DRM, platform customers are well equipped to deal with the full range of current requirements surrounding the protection of high-value video content. This attests to the level of expertise that distributors will be able to rely on as the market continues to evolve.

From its beginnings as a co-developer of Marlin, Intertrust has been in the vanguard of security technology development with hundreds of patents relating to the needs of multiple verticals, including automotive, retail commerce, energy, and media. With experts dedicated to managing ExpressPlay DRM worldwide, the company can be counted on to implement whatever refinements are needed to ensure ExpressPlay remains the leading option in OTT video content protection.

Total Cost of Ownership

Intertrust has also made sure that any assessment of how an in-house build TCO compares to a TCO relying on ExpressPlay DRM will lead to the same conclusion: ExpressPlay DRM is the better choice.

Not only does ExpressPlay DRM offer a TCO far below what can be expected under best-case assumptions in a build-it-yourself scenario, the hosted service option frees distributors from enduring the sudden hits on budgets that occur when those best-case assumptions turn out to be off the mark.

Using ExpressPlay DRM, distributors avoid all the costs of building, operating, and updating a content protection infrastructure. Instead, they can take advantage of a success-oriented fee structure that amortizes all costs across a vast customer base, with payments closely tied to the pace of service usage and expansion.

In this pay-as-you-go model, pricing is tiered starting at a minimum baseline that charges a low monthly fee for licenses and a set per-token fee for usage. With expansion to the next tier in the licensing count, the per-token fee drops, ensuring that as the service gains wide traction with users, costs will be contained within predictable parameters.

Conclusion

With the explosion of OTT video into the vanguard of television entertainment, successful fulfillment of licensing requirements has become as essential to survival with online distribution as it is in traditional pay TV operations. At the same time, creating and operating an OTT content protection infrastructure has become far more complicated and costly than it once was.

Whether an OTT TV provider is new to the market or already running a do-it-yourself protection operation, doing business in this new environment requires considering support from an experienced provider of hosted multi-DRM services as an alternative to managing protection in-house. There are many reasons for reliance on a hosted service, provided distributors can be sure they will gain the full support they need for their current and future operations:

- The technical know-how needed to build a sufficient content protection infrastructure to maximize audience reach and aggregate the content vital to service appeal goes well beyond the expertise that was needed to handle content protection in the past
- The staffing and CAPEX costs incurred with building an adequate content protection infrastructure are greater than ever
- Ongoing operations require additional personnel to handle routine tasks, driving higher OPEX
- The challenges associated with routine updating of components and periodic major upgrades require retention of experts over the long haul, adding another increment to OPEX
- The TCO associated with all these costs is far lower for distributors who take advantage of a hosted content protection service where the costs are amortized across a large user base

Nothing better illustrates the case for the buy option than the hosted multi-DRM service provided by Intertrust. As the most widely used multi-DRM technology worldwide, the ExpressPlay DRM platform has been validated as a solution that can be applied in any service regardless of the reach or scale.

ExpressPlay DRM is the only hosted content protection service that supports all major DRMs. And it's the only one that works at scales suited to any scenario, including live sports streaming with simultaneous usage soaring beyond 20 million sessions.

Along with providing all the basic components for successful implementation of multi-DRM protection, ExpressPlay DRM enables distributors to meet the Enhanced Content Protection (ECP) requirements (including watermarking) that content owners are imposing with ever greater frequency for distribution of UHD and other forms of high-value content.

By virtue of the size of its customer base and its access to AWS and Alibaba facilities worldwide, ExpressPlay DRM is positioned to exploit the benefits of cost amortization to the fullest extent possible. Combined with a fee structure that is success oriented and reflects the growth of subscribers over time, distributors can count on ExpressPlay DRM for a TCO that will always remain far below the costs of building and operating an in-house content protection infrastructure.

1 Digital TV Research, Global OTT Revenues at $68 Billion in 2018, September 2019

2 Statista, Video Streaming Worldwide, October 2019

3 Rapid TV News, UK, France Witness Binge Watching Surge as Global Streaming Steams On, October 2019

4 Digital TV Europe, Revenues for OTT Services Will Reach $159 Billion by 2024, October 2019

5 Broadband TV News, Quarter of European OTT Platforms Target Cross-Board Audiences, November 2017

6 Parks Associates, More than 586 Million OTT Subscriptions by 2024, January 2019

7 Venture Beat, Global Video Streaming Market Is Largely Controlled by the Usual Suspects, March 2019

8 Openwave Mobility, Operators Experiencing up to 100% Mobile Video Growth Year-on-Year, February 2019

9 Scientia Mobile, Device Fragmentation Growing 20% per Year, June 2019

10 IDC, Smartphone Market Share, October 2019

11 AppBrain, Google Play Stats: Number of Available Apps, November 2019

12 OpenSignal, Android Fragmentation Visualized, August 2015

13 Digital TV Research, Online TV Y& Movie Piracy Losses to Soar to $52 Billion, October 2017

14 Futuresource Consulting, 4K UHD Is Key Sales Driver for Flat TV Screen Market, April 2016

15 S&P Global Market Intelligence, OTT Video and Connected Devices Drive 4K UHD, December 2018

16 Sports Pro Media, Amazon and Discovery in Eurosport Player Tie-Up

17 Variety, How Rio Ratings Surprised NBC and Will Impact Future Olympics, August 2016

18 Ooyala, State of the Broadcast Industry 2019, January 2019

19 Rapid TV News, Hotstar Breaks Own Record with 25.3MN Concurrent Viewers, July 2019

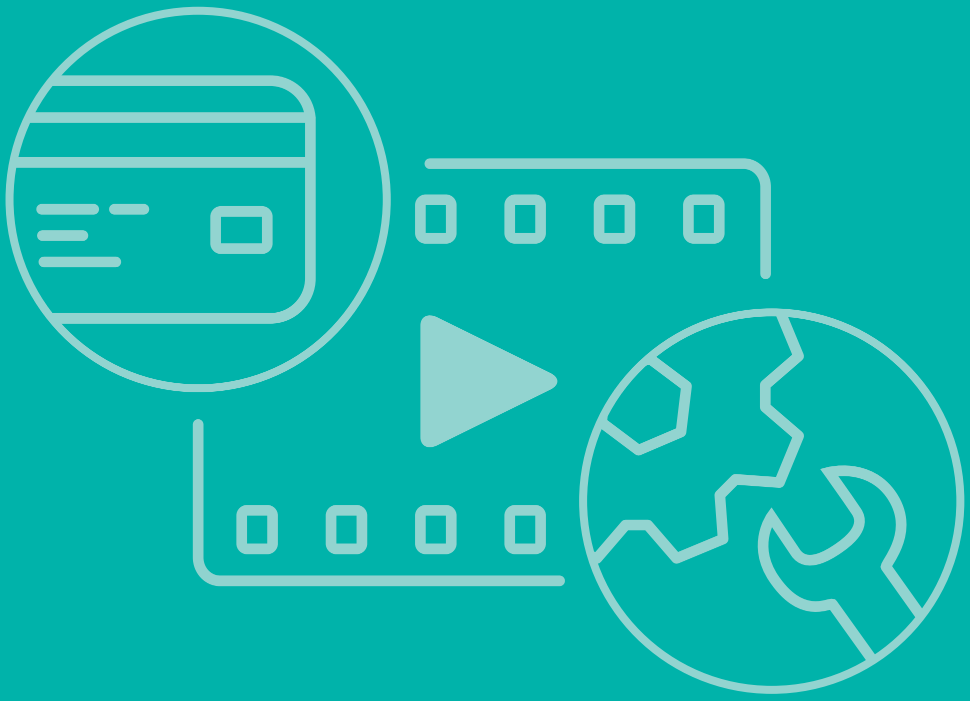
About Intertrust

Intertrust provides trusted computing products for leading corporations – from mobile, CE and IoT manufacturers, to service providers, and enterprise software companies. These products include the world's leading digital rights management (DRM), software tamper resistance, and technologies to enable secure data exchanges for various verticals including energy, entertainment, retail, automotive, and fintech.

Intertrust is headquartered in Silicon Valley with regional offices globally. The company has a legacy of invention, with fundamental contributions in computer security and digital trust. Intertrust holds hundreds of patents that are key to internet security, trust, privacy management, mobile code, networked operating environments, web services, and cloud computing.

As a provider of robust multi-DRM services for media and entertainment companies, our security technology protects the content delivered to any screen and OS platform, over any network.

Intertrust ExpressPlay is the world's most complete multi-DRM security-as-a-service, enabling converged protection for broadcast television and over-the-top (OTT) streaming services.



intertrust®

Building trust for
the connected world

Learn more at: intertrust.com
Contact us at: +1 408 616 1600

Intertrust Technologies Corporation
920 Stewart Drive, Sunnyvale, CA 94085