intertrust®

White Paper

ExpressPlay

How to secure e-learning services as piracy risks intensify

Contents

Introduction

The level of reliance on online video content in the e-learning market has reached a point where rigorous content protection is essential to preventing significant losses to theft in a streaming environment already plagued by massive piracy.

With the ability to connect people across far-flung locations via high-speed wireline and mobile networks, e-learning has become vital to educational institutions and enterprises worldwide more than ever before. At the same time, the video piracy business has morphed into a thriving global shadow industry draining billions of dollars from legal providers each year.

In this new environment, highly specialized educational and training material once deemed to be too limited in scale of usage to be worth stealing is becoming available to anyone in any niche who is willing to benefit from stolen intellectual property.

That's a pretty big pool to draw from considering that use of stolen content is now a normalized activity in the lives of hundreds of millions of people.

For professionals involved in producing and using educational content, this turn of events requires a new perspective on content protection. They still may see themselves as relatively small fish operating in diverse pools, but, in truth, they're now swimming in a global ocean where anything caught in pirates' nets can become targets for monetization. Making matters worse, the casual attitude to theft among consumers has also made regular users' illicit distribution of content a significant source of losses to rights holders.

Half measures applied to protecting e-learning content, such as encryption without securing the distribution of encryption keys, are no longer viable anymore than they are when it comes to streaming high-value entertainment content. As a result, the time has come for producers and distributors of e-learning content to implement the same level of protection that is now the norm in the booming media and entertainment streaming market.

This poses significant operational and cost challenges, starting with the complexities surrounding use of digital rights management (DRM) systems. Multiple DRMs are needed to provide the added layer of security for content distribution across the fragmented device ecosystem. This requires management of the various DRM technologies and their features.

Moreover, the aggressive and ever more technically sophisticated tactics pirates employ often create a need for additional measures such as forensic watermarking, either imperceptible or visible, that add more complexity and cost to content protection. Fortunately, e-learning content providers don't have to choose between providing less than adequate security or incurring prohibitive costs of providing that security in-house.

We will begin with a look at why the threat of losses to piracy has become a major concern in the streaming market including e-learning. That threat has intensified because:

- E-learning has become a much bigger part of corporate and academic life than ever before.
- The surging volume of video content and its importance to e-learning has made it a far more valuable target for aggregation in illicit repositories.
- Online video piracy has become a highly sophisticated business with technical knowhow and efficiency of operations that make it easier to profit from offerings of niche content.

Next, we will take an in-depth review of the multi-DRM and other protection mechanisms that e-learning content providers need to consider as they weigh next steps. Finally, we will explore how e-learning platforms can attain the level of protection they need at the lowest possible total cost of ownership (TCO) through the Intertrust extensive security services such as ExpressPlay DRM, Intertrust Data Platform, whiteCryption application shielding, and ExpressPlay Anti-Piracy Services.

Market trends impacting e-learning content protection

Multiple market projections portray a fast-growing global e-learning marketplace that reached unprecedented dimensions during the Covid-19 pandemic and is destined to keep expanding long after the coronavirus impact fades. By all indications, employees' and students' ongoing reliance on internet-delivered instruction will fuel an ever more technologically sophisticated ecosystem populated by tools, platforms, and turnkey providers serving every need.

In 2019, revenue generated by the online education products and services worldwide totaled $187.88 billion, as estimated by ResearchAndMarkets.[1] The researcher predicts that by 2025 the total will reach almost $320 billion, representing a 9.23% CAGR over that period. A report issued in 2019 by Syngene Research closely tracks these numbers, predicting that the market, growing at a 9.1% CAGR from 2018, will top $336 billion by 2026.[2]

While it remains to be seen how large a role e-learning will play in K-12 and college education once the pandemic is under control, courses and tools that have emerged over the preceding years attest to a growing element of education that is here to stay. At the K-12 level, the dollars spent on tools, platforms, and content are projected by researcher Valuates Reports to increase at a CAGR of 8.24% from 2020 through 2026.[3]

On the enterprise side, ongoing training through online education tools has become a routine aspect of operations everywhere, reflecting global recognition that there's simply no other way to cost-effectively address the increasing frequency of essential knowledge updates across an expanding range of topics. The e-learning scope now encompasses new product introductions, skill-level certifications, and updated company policies on production processes and safety procedures.

The surging role of online video and its impact on other trends

In this environment video has emerged as the essential educational medium and a major force in the evolution of the e-learning ecosystem. Indeed, as noted in a report on e-learning trends from global consultancy Matellio, video "has gained more attention than any e-learning trend ever."[4]

Video is ascendant in e-learning owing to its usefulness in lowering training costs, its impact on information retention, and its role in freeing workers and students from appointment-based education. A recent global survey conducted by cloud video platform operator Kaltura found that 91% of respondents work for companies that are using at least some video for learning and development, 64% have employers who are using virtual classrooms for live learning via video, and 69% would prefer to learn a new skill from video rather than a written document.[5]

As noted by Matellio, learning management system (LMS) supplier Lambda Solutions[6], and others in the field, pervasive use of video has, in turn, triggered most of the other top trends that experts say are reshaping the e-learning marketplace. For example, growing numbers of learning experience platform (LXP) suppliers

are leveraging the abundance of e-learning video content to create cloud-based repositories of material that companies and individuals can easily find for specific training requirements.

In the few years since the first LXPs appeared, these startups have become a $300-million segment of the e-learning market by offering services that are complementary to the LMS platforms enterprises use to amass business rules and course catalogs for specific training programs.[7] Often companies employ a single LXP as a cost-saving content resource for multiple LMSs.

The need for a way to sort through the massive volumes of videos now available for e-learning has inspired still another major trend, which is the emergence of AI-enhanced recommendation engines and services that LXP and LMP suppliers can tap to facilitate content discovery. Just how vast the video-centric aspects to e-learning have become is reflected in the fact that video discovery devoted to specific e-learning market segments is now a business category in its own right.

Paralleling these trends, an important force behind the creation and compilation of videos developed for the academic e-learning realm is the emergence of publicly available Massive Online Courses (MOOCs). First used in the U.S. and UK, they are now opening paths to self-paced learning in pursuit of college degrees and other goals worldwide. In Malaysia, for example, the government recently announced that 20 universities in the country are offering 60 MOOCs on topics in finance, healthcare, languages, and technology.[8] With growing support from an ever-expanding list of educational institutions, the MOOC market is projected to grow 29% annually from a revenue base of $5.16 billion in 2020 to $21.4 billion 2025.[9]

Higher profile makes e-learning video more valuable to pirates

Given the benefits video brings to e-learning, it follows that the heightened value and usage of this content has also introduced higher risks of losses to theft. It's a risk providers can't afford to ignore against a backdrop of a fast-evolving shadow industry that's siphoning tens of billions of dollars from multiple industry sectors through distribution of stolen video content.

The significance of the threat piracy poses to e-learning content providers rests on three major developments:

- The value of that content as something worth stealing stemming from the scale of video usage in e-learning, as described above.
- The ability of pirates to create business models that can serve the interests of anyone willing to engage their services, no matter how small the audience for a given piece of content might be.
- The degree to which people in general are willing to illegally share high-value content.

Calculations of current and projected losses to online video piracy keep going up. In 2017 a widely quoted report from Digital TV Research projected global losses to piracy would hit $26.7 billion that year and would reach $51.6 billion in 2022.[10] In 2020, Parks Associates released a report showing that earlier 2022 projections had already been surpassed in 2019 with a global loss calculated at over $57 billion.[11] Parks predicted the losses would top $67 billion in 2023.

The new protection requirements for e-learning content

Clearly, based on all the trends cited so far, the providers of video content used in e-learning find themselves in a new environment where the threat of content theft poses risks to bottom lines they never had to consider in the past. They not only have to protect against theft by professional pirates; they must take action to stem the losses incurred when paying users share the content with friends who would otherwise be paying for it.

The question now becomes what to do about it.

The DRM imperative

To some extent the answer is obvious. The risks call for implementing content encryption using the virtually unbreakable and most widely deployed version of the Advanced Encryption Standard, AES-128. This is a big improvement over simply limiting access to users with authenticated passwords that can be easily shared or running an unprotected video over YouTube, Vimeo or another streaming platform, which users with easy-to-obtain downloading tools can capture for their own offline use or to share with or even sell to others. But merely encrypting the content and passing out keys on an unprotected per-user basis fails to provide sufficient protection in today's hack-infested environment.

Nor is it enough to rely on authentication tokens with signed URLs, as in the native approaches employed by Apple's HLS Encryption and the open standard RTMP Encryption. While this is a way to limit key availability to legitimate users, any authorized user, including a pirate mercenary who pays for access, can share the first and any subsequent keys with others.

All of these drawbacks to reliance on standalone AES-128 encryption explain why premium video providers require the higher level of security provided by Digital Rights Management (DRM) systems for authorization of distribution online. This is the level of protection that makes sense for valuable e-learning content as well.

This higher level of security is rooted in the fact that DRM systems separate decryption keys from the content and manage the entire decryption flow in a secure process isolated from the user and contained in trusted components. License servers react to requests from authenticated devices under control of authorized users by securely transmitting the keys to enable content decryption on the authenticated device. This enables various business models where streaming content can be bound to one subscriber, device, or a group of devices with or without time limitation.

Figure 1

Global averages of video viewing time per device category

	2017	2017	2019
Computer	33%	33%	26%
Smartphone	27%	27%	28%
Tablet	16%	16%	15%
Smart TV/Connected Device	17%	17%	23%
Other Device	0%	0%	8%

Source: Limelight Networks[13]

The Multi-DRM challenge

The type of DRM system to use with any given content flow depends on which DRM is supported by the receiving device. This greatly complicates use of DRM security in a fragmented environment, where, by one count, there were over 63,000 device profiles in the market as of mid-2019, reflecting a 20% annual increase since 2011. (See Figure 1 for a summary of how viewing time is distributed across the major device categories, and Figure 2 for a summary of the annual global fragmentation count.)

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

But any distributor that wants to maximize reach must also take into account the fact that there are still a significant number of devices that don't support any of the DRMs that have been certified under current licensing policies. That's exactly where a vast ecosystem of devices, primarily in Asia but also in Europe, can be covered with the support of the open-standard Marlin DRM.

Distributors also must contend with the fragmentation within generations of primarily Android OS, which impacts how they interact with OEMs and DRM suppliers to authenticate the devices for access to premium content. To ensure consumers can access content on whatever device is at hand, distributors are required to sign into the core security embedded in the device OS or in the OEM's chipsets.

The only manageable approach to delivering protected content across this fragmented device ecosystem involves implementation of a multi-DRM platform. Otherwise, distributors would have to maintain separate silos for processing each asset for distribution under each protection regime, which would be both cumbersome and costly.

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 encryption schema for execution of PlayReady and Widevine DRMs on devices that 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's FireFox.

The challenges are huge in terms of required expertise, time consumed by building such multi-DRM support infrastructures, and the costs incurred with the initial implementation and ongoing management. These challenges would put the much-needed level of e-learning content protection provided by DRM security out of reach were it not for the availability of hosted cloud services that deliver turnkey support for implementing and operating a DRM infrastructure.

Figure 2

Global device profiles, 2011-201

2011	2012	2013	2014	2015	2016	2017	2018	2019
15,062	16,896	19,666	25,702	33,662	47,507	53,818	57.591	63,272

Source: ScientaMobile[12]

Additional protection requirements

In some instances, depending on the value and audience size of the protected content, there may be a need for one or both of two additional security mechanisms.

One has to do with vulnerabilities that occur when certain keys are stored in an application, allowing attackers to use reverse engineering techniques to steal them. Another concern is related to hackers employing side-channel attacks using analytic techniques like electromagnetic radiation analysis and correlation power analysis to crack the keys. Protection against these tactics requires the ability to secure apps and keys at the source code level with an added layer of security provided by what is known as white-box cryptography.

The other security mechanism is forensic watermarking, which has gone into ever wider use across the media and entertainment industry over the past few years. Watermarking involves injection of invisible digital codes in video streams, which serves to link the identity of each viewer with the viewed content so that anyone who illegally distributes that content can be identified as the source through extraction of the hidden codes.

As noted in the previous section, online piracy is booming and bad actors profit by delivering stolen content to large audiences. Using forensic watermarking to track and deter pirates is the best approach once content has been captured in the clear following decryption. Such theft is typically accomplished through use of cameras to record video directly from high-quality displays or with the help of high-bandwidth digital content protection (HDCP) "strippers" to pull unencrypted video out of the HDMI link to TV sets.

Superior protection at the lowest TCO

Support for all the security requirements as described above can be attained at the lowest possible total cost of ownership (TCO) through the Intertrust ExpressPlay DRM cloud service. ExpressPlay DRM is one of the most widely deployed multi-DRM technologies in the world, and provides full turnkey support for online video services and applications.

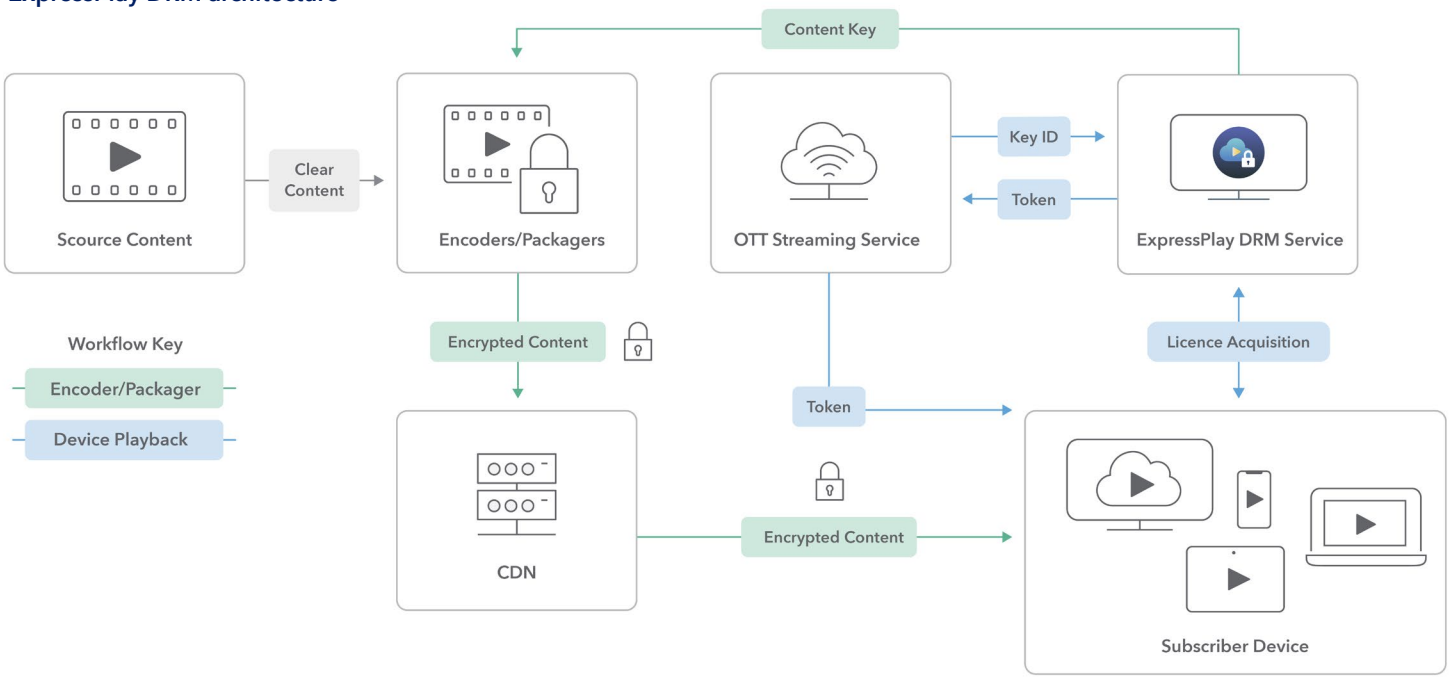
A uniquely comprehensive DRM solution

This cloud service achieves global reach with robust, highly scalable usage rates for live and on-demand content through tight integration with Amazon Web Services. As illustrated in Figure 3, the platform covers all the essential security functions 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 on adherence to licensing terms. Distributors through a few simple integration steps 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.

Beyond supporting the basics of a multi-DRM service, ExpressPlay provides several significant benefits that are not collectively available through other platforms. Notably, ExpressPlay is the only multi-DRM service that supports all major DRMs, including the open-standard Marlin DRM as well as Apple FairPlay, Google Widevine and Microsoft PlayReady. As shown in Figure 4, this comprehensive DRM support extends across all the major device and browser platforms.

Figure 3

ExpressPlay DRM architecture



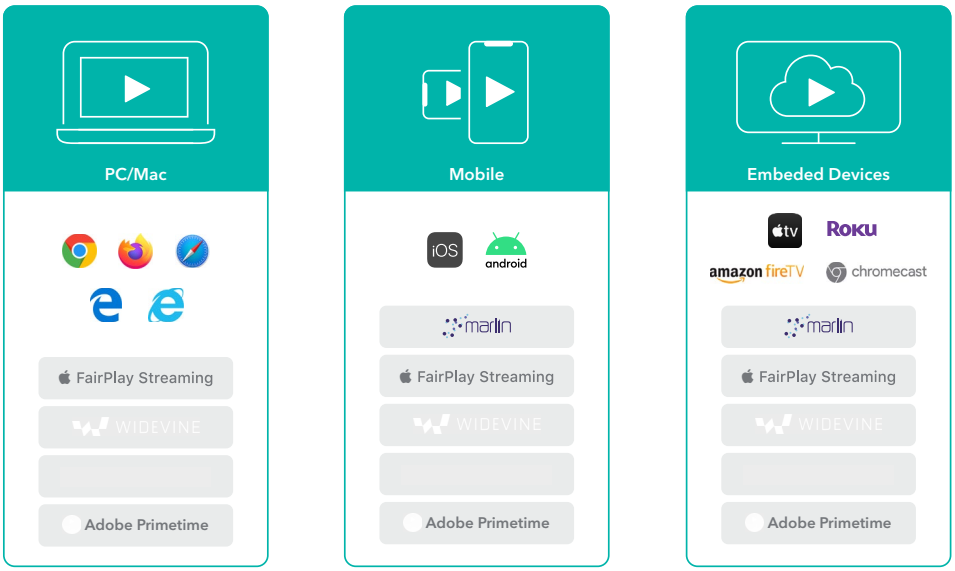


Figure 4

ExpressPlay Multi-DRM – Client support

The support for Marlin DRM, which Intertrust helped create as an open-standard and studio-trusted alternative to proprietary DRMs, is an especially significant advantage. In part, this is the case because Marlin is the native DRM on millions of devices in Asia and other parts of the world. In all such instances there is no need to use the ExpressPlay SDK to integrate the service with device players. (The SDK, which is used with implementations of the ExpressPlay client on Widevine-supported Android devices and FairPlay-supported Apple devices, is also not required with devices that natively employ PlayReady.)

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 use of the SDK.

ExpressPlay DRM also provides support for hardware-level integration that allows hardware roots of trust (HWRoT) to associate unmanaged devices with a distributor's content at the chip level. This is done through Widevine Level 1 and PlayReady SL3000 as well as Marlin.

White-box cryptography solution

Another vital benefit delivered involves securing of apps and keys at the source code level with tamper-resistant white-box cryptography provided by Intertrust's whiteCryption products. Attacks on apps are thwarted with advanced shielding that hardens apps against static and dynamic analysis, hacking and reverse engineering.

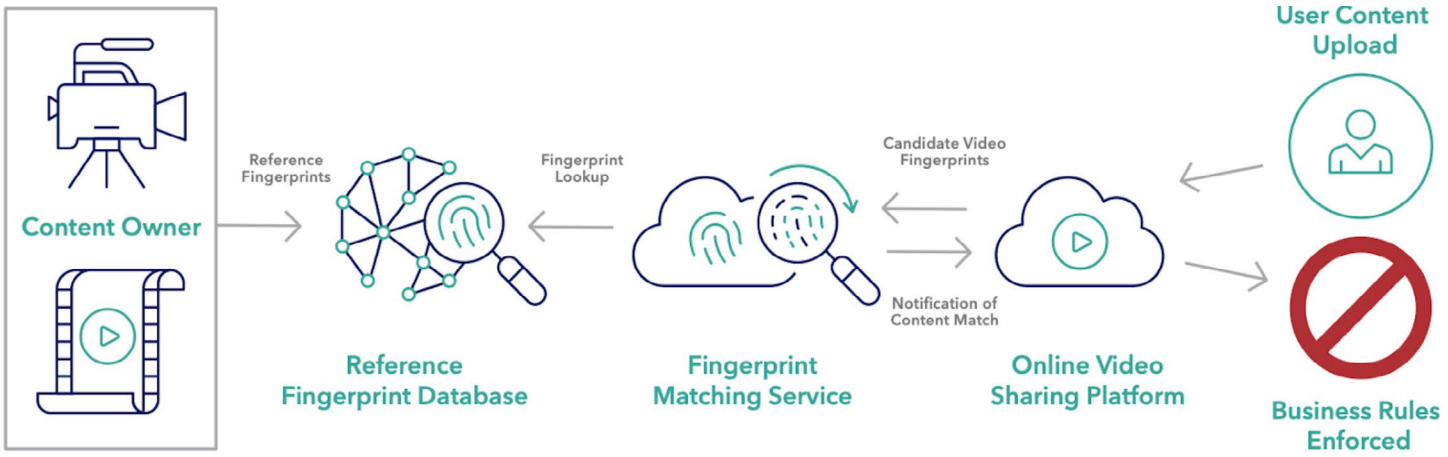


Figure 5

Server-side and client-composite approaches to forensic watermarking

When it comes to executing watermarking, customers can choose from two solutions offered through the ExpressPlay Anti-Piracy and Watermarking: the client-composite solution provided by Friend MTS or a server-side option supplied by ContentArmor. This lets distributors match their specific needs to a solution that perfectly fits their requirements, which isn't possible with multi-DRM platforms that focus on one watermarking technology.

Both watermarking solutions meet the rigorous requirements embodied in the motion picture industry's Enhanced Content Protection (ECP) specifications from MovieLabs. These include robust support for tracking pirated streams, identifying sources, and rapidly responding to live stream theft. see Figure 5).

A success-based TCO

By choosing the cloud-based ExpressPlay multi-DRM service, 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.

Conclusion

As e-learning plays an ever greater role in employee training and academic life with tools and services generating billions of dollars annually, the value of video as the dominant information conduit is growing to unprecedented levels.

Voluminous catalogs of video supporting every need are supplied for academic, industrial and personal use through learning management systems, learning experience platforms, massive online course repositories and individual institutions and enterprises. LXPs alone represent a supply chain generating hundreds of millions dollars in revenue each year.

As the value of video to the e-learning market soars, so, too, does its value to thieves. The professional practitioners of piracy, now costing legitimate providers over $50 billion annually, have built an expansive, high-tech ecosystem that is well positioned to garner returns from any video of value to even the smallest user bases in the e-learning marketplace. At the same time, the normalization of credential sharing and other means of promulgating video illegally on the part of consumers has made casual theft a serious threat as well.

The risks to the business models of everyone involved in the use of video for e-learning have reached a point that calls for the kind of content protection that is commonly used with premium entertainment video but has seldom been considered for use with e-learning related content. This not only requires that content be encrypted at the level of impenetrability afforded by the AES-128 standard; it also means that licensing policies and key distribution must be managed with the robustness provided by DRM systems.

Moreover, e-learning video providers need to have recourse to additional security measures to accomplish the widest possible protection perimeter like implementing forensic watermarking to track sources of illicit redistribution of stolen content.

These requirements introduce the need for a cost-effective approach to working in a multi-DRM environment that's intrinsic to serving a fragmented device marketplace. This entails complexities that would be prohibitively expensive to address through an internally built and operated DRM-based content protection system.

Fortunately, e-learning video producers and distributors have recourse to cloud-based service solutions that can mitigate these burdens. But they must be sure to engage with a service that can cover all DRMs and other protection techniques with unfailing performance at the lowest possible TCO.

The comprehensive approach to content protection needed to meet these requirements is available as a service from Intertrust, the provider of media security solutions serving multiple industries, including the e-learning sector. The firm's ExpressPlay DRM cloud service is the one of the most widely used multi-DRM platforms in the world. Along with providing the most robust and comprehensive protection, ExpressPlay DRM users are assured the broadest possible scale of DRM protection worldwide, including Apple FairPlay, Google Widevine, Microsoft PlayReady, and open-standard Marlin DRM.

Intertrust also offers a best-of-breed white box cryptography and watermarking solutions whenever those needs arise. Critically, all protection modes are offered through the ExpressPlay Media Security Suite on a pay-as-you-go basis, which ensures a predictable TCO as providers accommodate new device formats and licensing requirements.

From its beginnings as a co-founder of Marlin, Intertrust has been in the vanguard of security technology development with scores of innovations addressing protection requirements across multiple verticals, including the enterprise and academic segments of the e-learning marketplace. 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 e-learning content protection.

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.

Sources

[1] Research And Markets, Global Online Education Market Worth $319+ Billion by 2025, April 2020
[2] Market Research, Global E-Learning Market Analysis, March 2019
[3] Valuates Reports, Online Education Market Size Is Projected Reach $245,900 Million by 2026, October 2020
[4] Matellio, 10 Best eLearning Trends and Predictions for 2020-2021, June 2020
[5] Kaltura, The State of Video in Enterprise, November 2019
[6] Lambda Solutions, 5 eLearning Industry Trends You Need to Know, December 2020
[7] Josh Bersin Academy, LXP Market Expands, September 2018
[8] ibid. Research And Markets
[9] Guide2Research, 2020 Data on Higher Learning & Corporate Training, June 2020
[10] Digital TV Research, Online TV & Movie Piracy Losses to Soar to $52 billion, October 2017
[11] Piracy Monitor, 2019: A Year of Awareness for Video Piracy, January 2020
[12] Scientia Mobile, Device Fragmentation Growing 20% per Year, June 2019
[13] Rapid TV News, UK, France Witness Binge Watching Surge as Global Streaming Steams On, October 2019

intertrust®

Building trust for the connected world.

Learn more at: expressplay.com/products
Contact us at: +1 408 616 1600 | onestopshop@expressplay.com

Intertrust Technologies Corporation
400 N McCarthy Blvd, Suite 220, Milpitas, CA 95035