intertrust®

White Paper

ExpressPlay

# New challenges and solutions to protecting live-streamed video

## Part 2

Finding a comprehensive solution to battle live streaming piracy

# Contents

# Executive summary

**The OTT market's landmark shift to live streaming sports and other linear content calls for a new, comprehensive approach to battling piracy that can support effective action against illegal access by vast numbers of simultaneous viewers.**

Indeed, given the far-reaching complexities of these issues, just identifying what really constitutes an effective approach to protecting live-streamed content is a challenge. Speed of execution, of course, is an obvious priority given that the sooner disruption occurs, the greater the impact on viewers and potential to improve revenue.

But there are many other aspects to live streaming that complicate security strategies compared to strategies applied with time-shifted content. Typically, with live streaming there are:

- More variations in licensing policies, especially when cross-border distribution is involved (accommodated through DRM policy management)
- Requirements to reduce latency to accomodate a live viewing experience
- Vastly more streams to parse all at once in the search for illegal flows
- More illicit sources to identify and disrupt

Fortunately, these challenges are not insurmountable. The key to taking them on is to choose a tightly integrated platform that brings together best-of-breed tools to ensure streamlined, rapid execution of everything that's required to mount an effective response.

The purpose of this document is to explain how a modern multi-DRM and anti-piracy service, such as the ExpressPlay media security suite, is well suited to this task. This solution includes ExpressPlay Multi-DRM service, ExpressPlay Anti-Piracy, and ExpressPlay XCA - all developed by Intertrust and its partners to offer an effective response to illicit distribution of live-streamed content. This paper will outline the requirements that must be met to mount an effective defense.

Such a solution must include support for:

- Robust execution of multi-DRM protection suited to high-value content, meeting all licensing policies between producers and distributors for each engagement
- Techniques that ensure DRM protection will not add latency to live video streams
- Approaches to forensic watermarking to address different types of linear content
- Effective means of immediately identifying stolen content as a first step to tracking sources through detection of watermarks
- Additional measures spelled out in MovieLabs' Enhanced Content Protection specifications for 4K UHD and HDR-enhanced content

Producers and distributors of high-value sports and other live-streamed content now have the opportunity to combat piracy for a long time to come.

# Defining content protection for the live streaming era

**As noted in the first paper in this series, a piracy ecosystem has emerged around new approaches to marketing, monetizing and facilitating access to illegally streamed sports and live TV channels.**

This sophisticated approach is driving legitimate providers' revenue losses to unimaginable heights. But, given the tools now at hand, this is not an inevitable outcome.

## Multi-DRM support at ultra-low latency

Such results underscore the benefits to be realized from investing in a well-designed comprehensive solution to meet the challenges posed by live streaming piracy. As in so many other aspects of OTT operations, the ability to cost effectively set up and manage such an approach has been greatly facilitated by advances in cloud technology. Large-scale processing and multi-faceted workflows can now be realized with far greater technical and financial agility than the on-premises server installations of the past.

Implementing a cloud-based next-generation security solution optimized for live streaming starts with a multi-DRM operations platform. Given the realities of device fragmentation, such a platform must work seamlessly with the major proprietary DRM systems – Apple's FairPlay Streaming, Google's Widevine, Microsoft's PlayReady and Adobe's Primetime – as well as with the open-standard Marlin DRM, which is natively supported in chipsets running on millions of devices worldwide.

Keys have to be provisioned on a per-session basis in accord with all the types of encryption methods and file formats these DRMs use to convey licenses and policy information. All provisioning processes associated with these interactions must be rigorously secured. The same is true of the keys themselves, which must be protected at all times.

FairPlay Streaming marlin Microsoft PlayReady WIDEVINE

With linear OTT video, content owners typically require that keys be refreshed multiple times during a viewing session. The platform also must support instant delivery of keys and licensing enforcement policies whenever a new program is accessed so that users can switch from one live channel stream to another just as easily as they do with legacy TV services.

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.

MVPDs also need to rely on the multi-DRM platform to help them serve as aggregators of OTT providers' services. Given the hassles subscribers used to face in dealing with the fragmented OTT ecosystem, this has become a major trend among MVPDs looking to leverage convenience as a retention tool. This began with incorporation of interfaces within the Netflix UI and now includes multiple OTT streaming app options as part of the managed walled-garden experience.

These strategies are best accommodated through a uniform approach to content protection that marries the rights policies the MVPD must adhere to with the rights policies governing their OTT partners. An integrated approach to content protection on live streamed services allows MVPDs to adhere to all policies without having to re-encrypt content under a separate protection regime.

All the steps entailed in managing execution of rights policies tied to multi-DRM services, whether under control of an OTT provider or an MVPD, pose a serious latency challenge when it comes to securing live sports and other time-sensitive linear content. There's no room for adding a second or two of latency in live streaming situations where distributors have gone to extraordinary lengths to cut streaming lag times to broadcast-level latencies.

Consequently, the multi-DRM 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. This applies to key refreshments as well as key provisioning with each session. Preventing delays caused by license acquisition by end users' players in the initial authorization process is also vital to maintaining low latency.

## Effective support for flagging stolen content

A basic principle in the battle against consumption of stolen sports and other live-streamed content is that a fast response is directly proportional to its effectiveness. Disruptions to viewing early in a game cause more pain to pirate audiences than later disruptions, and failure to act before the game is over renders action useless.

Timely counteraction begins with the ability to quickly determine which streams carrying a sports event or other piece of live content are emanating from unlicensed sources. Insofar as there might be other sources with licenses to distribute the content, this is essential to ensuring follow-up source tracing with forensic deciphering of watermarks is strictly focused on illegitimate sources.

Many approaches to identifying stolen streams that have been commonly used with stored content offered on demand are either too slow or have been compromised by pirate countermeasures to the point where they are unreliable or ineffective. One technique used with live streaming but has been rendered more or less useless involves monitoring for branding labels and other visible "hash codes" on streams that aren't coming from sources licensed to deliver that content. Pirates regularly employ widely available, low-cost hash-code removal tools, which work in near real-time to strip away any kind of visual marks from a video feed in ways that avoid any noticeable disturbance to the picture.

A much more effective approach involves use of web crawling tools in conjunction with forensic digital fingerprinting technology, a mainstay in automatic content recognition (ACR) applications, to identify licensed content that isn't coming from licensed sources. Digital fingerprinting, as the term is used in media, entails storing a few key video and/or audio descriptors which, together, uniquely define a piece of content licensed to a specific distributor. If automated reference to server-stored listings shows the content isn't coming from one of the listed licensees, the content can be immediately flagged for follow-up in the watermark detection process. The digital fingerprinting technology used in theft detection must be undetectable by pirates and robust enough to remain intact across all video formats and through any aspect ratio change, bitrate reduction and downscaling that occurs during playout processing. Moreover, it must be 100% accurate.

## Watermarking designed for live streaming

Industry expectations that use of watermarking to identify end user premises-based sources of piracy would become an essential security component in high-value video distribution were ignited by the issuance of Enhanced Content Protection specifications by the motion picture studios' MovieLabs in 2013. But, with the slow ramp-up to distribution of movies earmarked for ECP, including 4K UHD-formatted releases and movies distributed in early-release windows, the studios have been slow to implement ECP requirements, although recently they've picked up the pace amid growing alarm over losses to piracy.

However, a much stronger push for watermarking is coming from the live streaming side of the market, especially for sports streaming. The scale of losses to theft is prompting ever more sports producers to include requirements for an effective approach to watermarking in their licensing terms. At the same time, watermarking requirements have taken hold in licensing for other types of live-streamed content, now that 4K UHD and HDR formatting is becoming more commonplace.

To be effective in live streaming applications, watermarking solutions, working in tandem with digital fingerprinting or other means of detecting pirated content, must:

- Make it possible for license holders to disrupt viewing within a few minutes after streaming starts
- Be rigorous enough to withstand pirate detection and the many means as outlined in the previous section that pirates have devised to render watermarks useless
- Be able to survive content degradation in both the legitimate and piracy phases of distribution, including processes such as transcoding, recompression and camcording
- Avoid adding noise or artifacts that could contribute to content degradation
- Work with persistently encrypted content, thereby eliminating the need to decrypt and re-encrypt during content preparation and delivery
- Support extraction of the marks directly from the video for immediate identification of pirate sources, which eliminates traditional "non-blind" approaches to detection that require comparison with the original unmarked video
- Be tightly integrated into a comprehensive security solution that orchestrates all aspects of protection to achieve the best possible results

There are, in general, two approaches to executing watermarking in live streaming scenarios: One uses a server-side per-session injection of watermarks, often at network edge points anchored by CDN facilities that have been enhanced to execute watermarking through integrations with solutions from one or more suppliers. The other relies on client-side solutions securely integrated with media players or embedded in hardware that are sufficiently lightweight and versatile to work with any device.

A rule of thumb for distributors choosing a watermarking solution engineered for live streaming is that the best results in any given instant can be attained by a market-validated client-side solution, provided the rights holder hasn't set requirements that can only be met through application of a market-proven server-side solution.

Fundamentally, the intrinsic advantage of a client-side over a server-side solution stems from the fact that, in live streaming scenarios, the watermark extraction process leading to identity of the source can be performed in a minute or so compared to much longer identification processes that can take up to 15 minutes in server-side applications. Watermark identifiers in client-side applications are encapsulated in shorter video segments, which is possible in live scenarios because pirates don't have time to execute the counter measures that could be taken against this approach to watermarking if it were used with on-demand content.

License holders have adjusted requirements accordingly to enable rapid action against theft of live content. But in the case of linear streams delivering episodic programming that people will also want to access at later times in on-demand mode, imposition of watermarking requirements with high-value linear streams formatted in 4K UHD and HDR will likely require server-side watermarking.

The studios, for example, have made it clear that in licensing 4K-formatted movies for network distribution they will continue to adhere to the more stringent watermarking requirements set by the MovieLabs ECP specifications. In these cases, the accessibility of client code to every end user, no matter how vigorously protected, is perceived as too great a vulnerability.

Many server-side and even some client-side solutions designed for live streaming rely on an "A/B" approach to marking, which avoids delays in the watermarking process that are untenable with live content. In these cases, each of two versions of the same live video sequence created in the encoding process has been injected with one of two different invisible digital codes that remain the same for all viewing sessions. The system assigns a unique sequence of watermarked chunks from the two streams which are delivered either at the point of unicast streaming from an edge server or with client player-directed rendering of the sequence on the device.

This solves the problem of executing on-the-fly injection of the watermarks into each unicast stream. But proponents of purportedly superior approaches say they've chosen those alternatives because the A/B method adds to the workloads on encoders, increases storage requirements in conjunction with temporarily queueing up A/B chunks in the delivery network and consumes more bandwidth over distribution links to the points where the A/B switching occurs.

Now that other solutions have appeared that claim advantages over the A/B approach with no loss and, in some cases, gains in speed both at the injection and extraction steps in watermark processing, the A/B choice for live streaming can no longer be taken for granted. These distinctions add to the factors that distributors need to consider in choosing a solution.

A well-designed comprehensive security platform supporting multi-DRM, watermarking and other requirements suited to protecting live-streamed content should provide distributors the option to use either client-side or server-side approaches based on requirements set by rights holders and other considerations.

## Other requirements impacting live content licensing

Security mechanisms incorporated into any comprehensive content protection platform should also provide protection against app attacks where sources of pirated content substitute a phony ID for the real source's ID. Attacks on apps, which, as mentioned in Part 1, are a growing source of industry concern, are thwarted with advanced shielding that hardens apps against static and dynamic analysis, hacking and reverse engineering.

In addition, beyond watermarking, there are other elements of MovieLabs' ECP specifications that license holders are including in their requirements for rights to stream live content. Even though these requirements were proposed in the motion picture context, they, like watermarking, have moved into the broader realm of protection for multiple categories of content as piracy exacts an ever-higher toll on revenue.

While extended ECP requirements aren't universally in play as yet, distributors must be sure the security platform they choose is equipped to meet these stipulations as they gain greater currency. These requirements include:

- Expanded hardware-level protection, using hardware roots of trust at the factory or through firmware reconfiguration (as MovieLabs puts it, "to provide a secure mechanisms for DRM systems to store secrets in local, persistent storage in a form encrypted uniquely for the device.")
- Maintaining a secure video path (SVP), and leveraging Trusted Execution Environment (TEE) for separate protection-related processing, including encryption, decryption, and device authentication.
- Extending ECP protections beyond streaming to include instances involving content downloads, offline playbacks, device-to-device side loading and time shifting.
- Protection for all in-the-clear content transitions.
- Rigorous enforcement of device certification requirements through "trusted implementors" instead of relying on device OEMs to provide security compliance.

# Multi-DRM and anti-piracy services

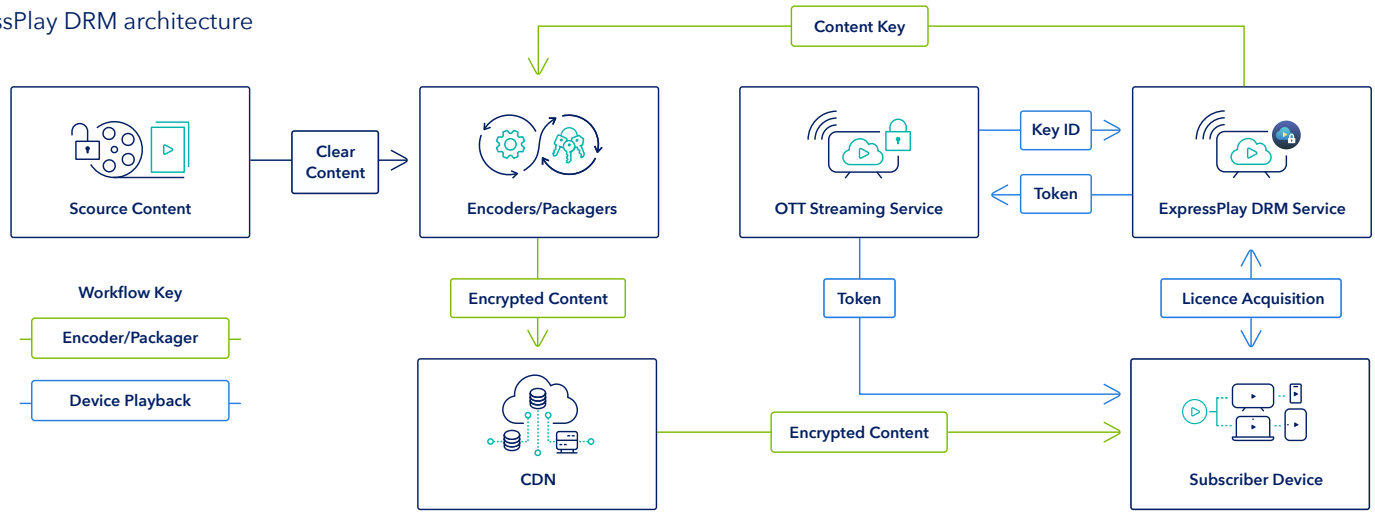
**Comprehensive protection services embodied in Intertrust's ExpressPlay media security suite provide content owners and distributors of live content all the mechanisms they need to meet the requirements described earlier. These live-optimized features exist within the Intertrust framework to support protection of all types of content in both OTT and MVPD managed-network environments.**

On the OTT side the foundation for that framework is Intertrust's ExpressPlay DRM, the cloud-based multi-DRM service. Now one of the most widely deployed multi-DRM technology in the world, ExpressPlay DRM provides full turnkey support for OTT video services reaching more than a quarter of the world's population.

As described at greater length in the Intertrust white paper Buy Versus Build Options for Enabling Content Protection in the New OTT Video Market and depicted in Figure 3, ExpressPlay DRM covers all the bases of any OTT video service strategy. Critically, it is the only multi-DRM service that supports all major DRMs, including Adobe Primetime and the open-standard Marlin DRM as well as Apple FairPlay Streaming, Google Widevine, and Microsoft PlayReady.

ExpressPlay DRM, deployed on Amazon Web Services (AWS) facilities across the globe, makes it possible for distributors to implement robust rights management on a usage-driven cost basis without adding new infrastructure or incurring extraneous setup costs. The service operates in all live and on-demand OTT streaming scenarios to provide 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.

**Fig 1.**
ExpressPlay DRM architecture



Support for Marlin, which is based on technology developed by Intertrust, adds another dimension to the practicality of ExpressPlay DRM insofar as this studio-certified alternative to proprietary DRMs is natively embedded in millions of devices in Europe, Asia, and elsewhere.

ExpressPlay DRM also delivers a major cost advantage over fixed-priced solutions as well as build-it-yourself approaches where the investment has to cover nailed-up capacity sufficient to accommodate the heaviest use-case scenarios. The ExpressPlay multi-DRM service success-oriented fee structure leverages Intertrust's ability to amortize costs across a vast customer base with a graduated pricing structure that reduces per-use rates as total usage increases.

## Support for new advances that streamline DRM operations

### Minimizing latency

A key aspect to Intertrust's optimization of ExpressPlay DRM for live streaming involves reducing latencies typically incurred in multi-DRM scenarios. That mitigation starts with the elimination of encryption-related delays through tight integration of ExpressPlay DRM with third-party encoders and packagers via robust APIs tuned to leading encoders/packagers used by content distributors.

Along with eliminating lag time between encryption and encoding, this integration goes hand in hand with ExpressPlay DRM's ability to execute the fast, efficient Content Encryption Key (CEK) acquisition process enabled by the MPEG-DASH Industry Forum's Content Protection Information Exchange (CPIX) standard. Addressing HLS as well as DASH, CPIX facilitates streaming of protected content to every type of device while eliminating the need to rely on proprietary DRM APIs to handle the information exchanges.

The XML-based format cuts OTT service launch times in multi-DRM scenarios by utilizing a common API structure to enable exchanges of keys and DRM policies between a DRM service, key manager, and encryptors. This makes it possible to exchange content protection configurations between different systems that need to interact within a video streaming setup.

These efficiencies are also important to saving time when it comes to specifying multi-key encryption processes, where different key values are associated with different content resolutions or other distinctions assigned to a given content stream. CPIX supports per track encryption as well as key rotation with live content if rotation is a requirement imposed by the licensing policy associated with provisioning the initial key for a given session.

Efficiencies tied to use of CPIX have been augmented with widespread adoption of the Secure Packager and Encoder Key Exchange (SPEKE) protocol, which was developed by AWS as a CPIX subset to define a standard API that streamlines communications between DRM systems and encryptors, which in this case include encoders, packagers, and origin servers. This eliminates any need for separate integrations between proprietary multi-DRM APIs and encryptors and other components from different vendors.

Intertrust leverages SPEKE to facilitate streamlined integration of customers' DRM operations with AWS Media Services. Communications between Media Services and the ExpressPlay Key Management Service (KMS) through AWS API Gateway endpoints support DRM signaling and the delivery of encryption keys for live and VOD content processed by the AWS Elemental MediaPackage, MediaConvert and Elemental Live modules.

ExpressPlay DRM also makes it possible to avoid session startup delays during the issuance of licenses in the user authorization process. Reliance on persistent rather than non-persistent licensing is a fundamental starting point.

This requires use of non-volatile rather than volatile memory to store licenses. As the name implies, persistent licenses continually enable playback from a given service by the licensed user throughout the life of the license, whereas non-persistent licenses terminate with the completion of each session.

But even with elimination of repeated license renewals, there's a need to prevent delays in session startups with the initial licensing process. ExpressPlay DRM gives distributors of live content the option to avoid such delays through proxy-based license delivery. Rather than relying on token-based license delivery, as shown in Figure 2, which requires two roundtrip communications between the player and the licensing source, the proxy model enables players to directly retrieve a DRM license from the proxy server managed by the OTT streaming service provider, as shown in Figure 3.

**Figure 2**
Direct DRM license acquisition model

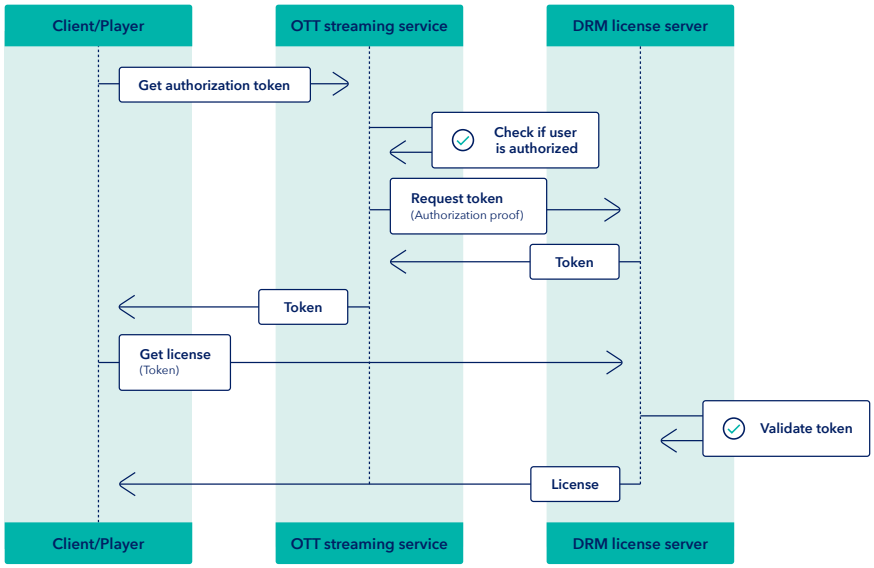
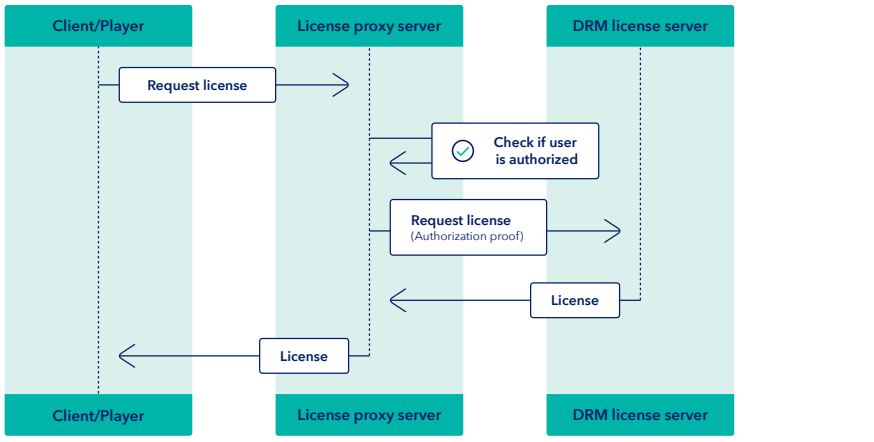



**Figure 3**
Proxy DRM license acquisition model



License Proxy licensing authorization is performed as part of the license acquisition process triggered by the player when it detects that a content key is needed. This greatly simplifies support for complex use cases such as key rotation and/or multi-party packaging workflows.

There are other important benefits to be realized with proxy-based license delivery. As the licensees are bound to the specific session they were requested for, unauthorized redistribution of the licenses will not be an effective replay attack. Because it is not possible to use the license for another session/device, viewers will not be able to process the licenses. Proxy Licensing also simplifies client-side logic, which makes it easier to set up players. Because the player will always retrieve the license from a known endpoint, there's no need to configure the player to prefetch tokens. Any errors in retrieving the license can be handled on the server side.

## Support for live-optimized watermarking systems

ExpressPlay watermarking also offers two types of solutions, providing distributors a choice of client-side or server-side solutions; however, as noted earlier, the preferred choice for live content distribution is a client-side solution.

Intertrust has partnered with best-of-breed suppliers in both categories. Notably, both have chosen other approaches to watermarking injection which they believe are more efficient than the A/B approach. ExpressPlay Watermarking enables a holistic live content protection environment that allows watermarking-related applications to be managed together with ExpressPlay multi-DRM service.

### Client-side watermarking

In the case of the client-side offering, the ExpressPlay Anti-Piracy and Watermarking service (powered by Friend MTS) incorporates content monitoring and legal enforcement with high-performance watermarking.

The Friend MTS Advanced Subscriber ID (ASiD) service comprises world-leading content monitoring with watermarking. The content monitoring operates at massive scale, protecting linear channels, live events and non-live VOD content. The ASiD watermarking service is the most widely used watermarking solution globally.

Friend MTS, which counts many major content owners, broadcasters, and operators among its clientele, has designed ASiD to provide highly robust protection against pirate attacks, including complex collusion attacks, making it suitable to meet the challenges posed by both live sports streaming as well as high-value Hollywood studios' early-release PVOD content. Rather than offering a set of independent tools with backup services, ASiD is delivered as a managed and integrated service to provide a truly effective capability with convenience for the customer.

The fully automated content monitoring service utilizes digital fingerprinting to quickly identify pirated content streams and send legal notifications to the infringing parties. The service processes many terabytes of video daily on a scale far beyond what can be done manually, and spans illegal streaming devices, Kodi add-ins, mobile apps, websites, and social media.

The ASiD watermarking service includes support for integration of the lightweight client SDK on any category of receiving device, including legacy STBs. ASiD watermarking is entirely imperceptible with no visual impact on the viewer experience, delivers high-performance extraction of watermarks from pirated content, and has proven to be fully robust against all real-world attacks such as collusion, blurring, and reframing.

Once the source of the content theft has been identified the information is communicated to the platform operator, and if necessary the notification can be sent to a subscriber management system for real-time action such as stream playback termination and account suspension. The entire sequence from pirate content detection through to watermark extraction and operator notification can take as little as just two minutes, enabling the rapid response required to protect the highest-value premium live content.

Along with sending notifications to the platform operator, Friend MTS has relationships with CDN providers who can block stream delivery to the restreaming subscriber. For example, the ASiD system is integrated with the Akamai Access Revocation service and as a result can trigger stream disruption in as little as a few seconds, avoiding the delays incurred when submitting takedown requests through other legacy mechanisms.

## Server-side watermarking

The server-side watermarking option is available through ExpressPlay Watermarking (powered by ContentArmor). This solution embeds watermarks directly in the encoded and encrypted video bitstream on the fly with no added latency beyond the profiling that precedes insertion. It does not require any additional encoding/transcoding, storage or bandwidth capacity and therefore can be easily integrated with network edge facilities.

Computational requirements are kept to a minimum at points of insertion through a two-tiered processing architecture. Computationally intensive operations are processed through an isolated offline profiler, which analyses the content bit stream to identify watermark embedding locations and values. This facilitates support for multiple watermarking profiles that adjust distortion to suit the type of content and attendant security requirements in each stream, including the profiles required for adherence to ECP watermarking specifications.

The Watermarking Embedding Metadata formulated by the profiler is transmitted to the watermark Embedder for direct insertion of an appropriately formatted identifier code into the stream. ContentArmor's technology has been endorsed by Hollywood studios, test labs and customers for undetectability and robustness through content conversions and pirate manipulations such as recompression, HDMI stripping, screencasting and camcording.

ContentArmor's partnership with Akamai offers a large-scale edge footprint for the embedding process. The low computational and storage requirements enable a more cost-effective use of these facilities compared to other watermarking systems.

## Live streaming protection optimized for MVPD operating environments

All of the security elements described here are available to MVPDs not only as a holistic solution to the live-streaming piracy challenge but also in conjunction with access to ExpressPlay XCA, the SaaS platform Intertrust has created as a way to address legacy pay TV service protection free of the royalty or other fee structures common to legacy conditional access systems (CAS). As described in the white paper The ideal path to converged content protection for hybrid TV services, Intertrust has made this possible through utilization of the widely embedded open-standard Marlin DRM core to enable cardless CA protection.

In addition, by leveraging the integration of ExpressPlay DRM with ExpressPlay XCA, TV providers can use ExpressPlay XCA for protection with virtually any type of hybrid TV service delivered to any DVB-compatible media gateway, STB, or smart TV, regardless of operating system. By virtue of its compliance with the DVB Simulcrypt standard, ExpressPlay XCA can be deployed alongside legacy CAS on one-way devices as well as interactive networks to facilitate non-disruptive transitions to hybrid services.

The ExpressPlay XCA SaaS also works in concert with Intertrust's ExpressPlay DRM service to provide robust protection for OTT content delivered to smartphones and other connected devices. And, as part of the Intertrust Security Suite, it exists in the cloud-hosted environment that facilitates choosing best-of-breed watermarking and related solutions in tandem with specific operator needs.

## ExpressPlay media security suite support for additional ECP requirements

As noted, many ECP recommendations beyond watermarking are gaining traction in licensing policies for high-value live and other content. In the case of rules specifying hardware roots of trust for unmanaged devices with a distributor's service at the chip level, ExpressPlay DRM supports integration of protection with TEEs and SoCs for UHD and HDR. This is done through Widevine Level 1 and PlayReady SL3000 as well as Marlin, which is designed not only to support TEE-based security but also to meet the ECP SVP.

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 and, in the case of live programming, network DVR applications.

# Conclusion

**The emergence of live streaming as a soon-to-be dominant component of the OTT video services market has spawned a new era in online piracy that requires new approaches to protecting content.**

With losses to live content theft, led by sports piracy, accounting for an increasing share of the billions of dollars siphoned by sophisticated online criminal operations, license holders and distributors need to have a comprehensive approach to fighting the scourge at all points of vulnerability. This means every facet of protection, including multi-DRM operations, locating instances of piracy, identifying pirate sources, and disrupting their operations, must be accomplished in near real time without adding latency to the live viewing experience.

Intertrust has met this challenge with implementation of the ExpressPlay media security suite. Anchored by the ExpressPlayDRM cloud service, the solution combines multi-DRM protection, piracy monitoring, white-box cryptography, watermarking and other mechanisms associated with MovieLabs ECP specifications. Providers can now cover every tactic in the pirate attack arsenal.

Offering all these components of live-streamed video security has been enabled by ExpressPlay media security suite, which includes a multi-DRM cloud service and best-of-breed client-side and server-side watermarking solutions. The Suite also encompasses the ExpressPlay Anti-Piracy Service (powered by Friend MTS) with a global fingerprinting-based piracy monitoring service.

Reversing the worrisome live streaming piracy trend requires a new, innovative approach that goes well beyond security platforms optimized for an on-demand viewing environment. To ensure robust content protection in this new era, ExpressPlay media security suite is the optimal foundation for mounting a full-scale assault against theft of live-streamed sports and other high-value content.

Service providers now have a cost-effective way to identify re-streamers rapidly and eliminate the stream source early during a live event. “Subscribers” to such illicit services will learn the hard way that the ability to watch live events is by no means guaranteed when the illegal re-streaming service is disabled and the screen goes black. The chilling impact on user behavior that comes with such an experience and exposure has been well documented. When this happens during an important game, viewers are more likely to switch to a legitimate service with superior quality and reliability. After all, a live game is only shown live once!

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