4 HOW TO TRUST ▷ YOUR PLAYER

Presented by BITMOVIN Friend MTS intertrust

BUILDING AN OTT SERVICE FOR TODAY'S WORLD

Article 4 – Beyond Digital Rights Management: Video Watermarking Weighs In

Published Date: October 23, 2020

Alan Ogilvie, Lead Product Manager, Friend MTS
Andy Wilson, Senior Product Architect, Friend MTS
Chris O'Brien, Engineering Manager, Friend MTS

In the continually evolving OTT world, we've established that savvy pirates are implementing new and advanced methods to steal valuable content – to the tune of **more than $67 billion** (USD) in value by 2023. Another report from **ABI Research** estimates that more than 17% of worldwide video streaming users access content illegally.

We also know that launching an OTT service is costly, resource-intensive and complicated. Getting it right is critical. Beyond building the video consumption environment and content acquisition, companies must incorporate up-to-date content protection methods. In this "How to Trust Your Player" series, we've learned about **Digital Rights Management (DRM) from Intertrust Technologies**, and about content packaging, license acquisition models – and **best practices for implementation within the video player environment from Bitmovin**.

Understanding Content Protection

But what about the other players? They are the users, the consumers of all this valuable content. To ensure content protection among these players, we have to look at watermarking. Working together with OTT services throughout the world, we have seen how companies are working hard to protect their content at the front end with DRM, but are not commonly implementing readily accessible, advanced watermarking techniques to protect the content once it reaches the end user.

As a result, they are risking subscriber loyalty, growth, and revenue by not covering the last hole in the content delivery system. This scenario is one case where the overused "end-to-end" term is applicable: OTT companies must protect their content end to end in order to truly protect their content and revenue.

Protection Beyond DRM

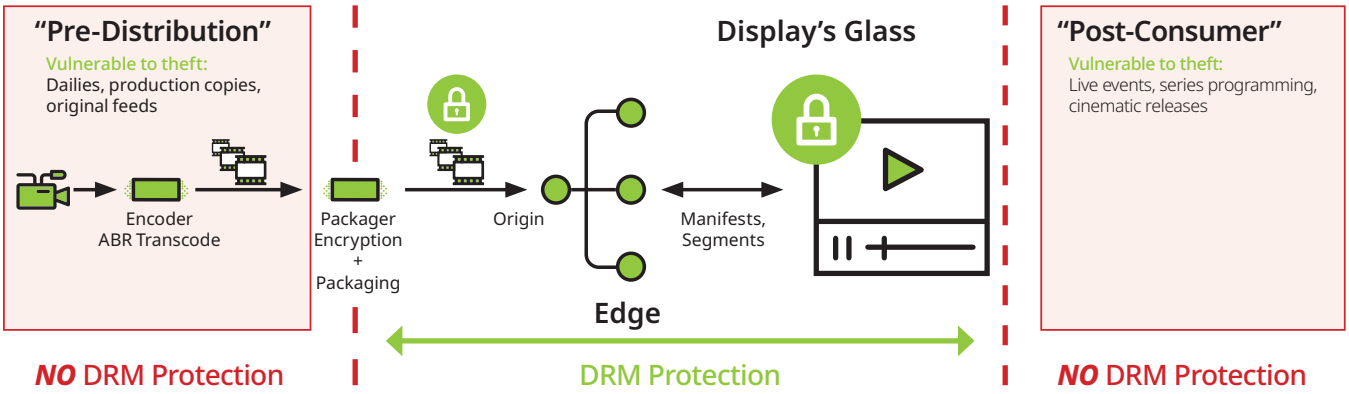
So what's an OTT service provider to do?

We know that DRM is absolutely necessary in this journey, and needs careful, considered implementation. As Intertrust pointed out in its article, "**Securing Content Access with Digital Rights Management Best Practices**", recommended DRM best practices are essential to:

- Maintain a secure interface for delivery of content keys to the encoder and packagers;
- Secure session tokens for authentication and authorisation;
- Prevent attacks against the DRM license acquisition servers;
- Make sure only verified browsers and players can access the media and DRM license in different devices.

A default option for any premium content service provider, DRM is designed to protect audio/video content during transit to the consumer's player. As discussed in the above-mentioned article, DRM manages the robust content encryption key exchange between the secured playback device (the player) and the license service. DRM is also responsible for setting usage policies for the content, and for enforcing this within the playback environment. However, once the material has started playing, a new threat emerges – the consumer. A common misconception is that playback devices are secure.

DRM can do little to isolate pirated content, or identify the wrongdoers, when content is stolen and made freely available. Once content arrives at its intended legitimate destination, DRM can do nothing to stop it from being redistributed by those who have no rights to do so. The crux of the problem is that DRM protects only the legitimate path from origination to the point of consumption.



See "**Beyond DRM: The Complete Content Protection Story**," for further details.

It's also important to understand that practices to curb sharing and theft of credentials (such as passwords) do not help reduce the distribution of content once it has escaped the boundaries of a video service.

In short, DRM is a key part of any rigorous approach to piracy defence. But if we want to talk about end-to-end protection, there's more.

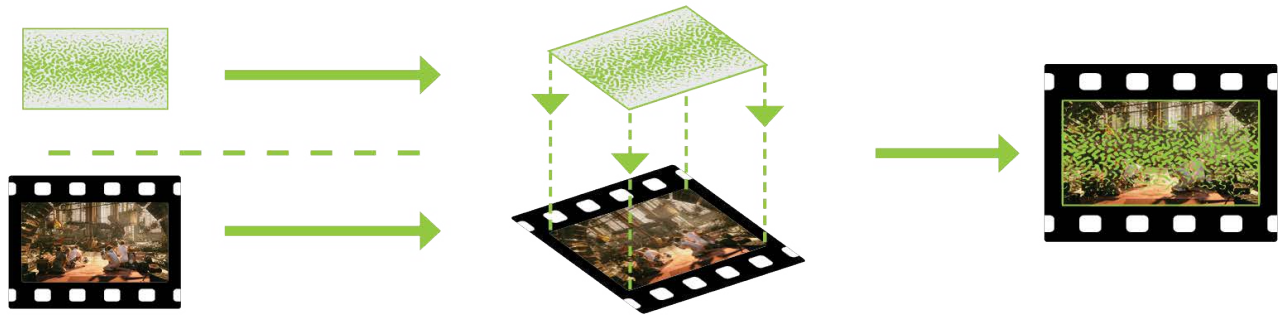
Enter Video Watermarking

To protect the value of video content – whether original or rights-managed – outside of these legitimate service boundaries, you'll need to identify the video itself. Specifically, you'll need information to confirm its outermost point of legitimate use. With that, you can identify the "bad actors": the infringing users and industrial-scale pirates.

To accomplish this, video providers can embed information into the video itself, at the point of origin, in the Content Distribution Network (CDN) during distribution, or within the player device. Information might include the device IP address, session details, and subscriber identifier.

The most effective way to do it? Client-composited (client-side) watermarking. It's clever, as consumers can't see the watermarks. Only automated analysis can.

Client-composited watermarking occurs within the consumer device. The embedded player accesses a software library database that replies with a unique identifier. The watermark information is converted into a pattern, similar in concept to a QR code, and then is "composited" with the video via an overlay.



Source: Friend MTS. Image source: frames from (CC) ***Blender Foundation***

Client-composited watermarking is fast. Time to detection of content theft can be as little as a few seconds – important for any service, but particularly so for live sporting events. It's also lower in cost than other watermarking options, such as A/B watermarking.

For a more thorough discussion of watermarking methods, their advantages and disadvantages, see our "**Subscriber Watermarking Technologies – White Paper Quick Facts**."

Best Practices in Video Watermarking: Detect, Deter, Disable

No matter which way you go with watermarking, you must keep the end goals in mind: to deter piracy, detect it when it occurs, and disable the source of the pirated content. The truth is that embedding watermarks alone is not very helpful unless there is a way to use the watermarks to find stolen video content, identify its source, and take appropriate action. Herein lies the hallmark of a robust watermarking solution.

Detecting involves monitoring suspected pirate outlets, and then matching the digital "fingerprint" of a suspected piece of content with a reference fingerprint that generates during the production process. Then, advanced watermarking analysis can see the identifying watermark and extract the information that it contains.

Determent is about defending against pirate "attacks." To reduce the chances that an instance of stolen content could be traced back to its last legitimate distribution end point (or to the pirates themselves), content thieves may try to make the watermark unreadable by applying "transformations" to the content. These "attacks" make the watermark no longer available or readable. However, a strong, advanced watermarking program has a far better chance of surviving these attacks and remaining readable.

Disabling is about treating the incident after determining the identity of a pirated video stream. This can include direct actions against the pirate, ranging from take-down notices to reporting to law enforcement. Typically, video providers take actions against subscribers whose accounts they detect to be restreaming. Those actions might be interrupting the session, requiring the user to re-enter access credentials, suspending the end user's account, disallowing the use of the device on the account, or even initiating legal action.

Choosing a Watermarking Service

What do you want from your watermarking service? What *should* you want from your watermarking service?

Deployment

How widely deployed is the service? How many set-top boxes and OTT players is it securing around the globe? In the OTT world, and in the content protection world, experience does count. Make sure you are getting a system with a proven, demonstrable track record in detecting, deterring and disabling piracy across multiple illegal redistribution channels.

Strength Against Attacks

OTT players need to choose a watermarking service that is effective. How effective? Ask the provider for details. At Friend MTS, we know that our Advanced Subscriber Identification (**ASiD**) service has remained secure against every attack made to date in both broadcast and OTT environments.

Keep in mind that staying abreast of attacks is a constantly changing process. Your watermarking provider has to not only keep up with the latest pirate schemes, but stay ahead of them. Those bad actors are clever, and don't always appear "bad" on the surface. In general, they use a legitimate subscription and easily available screen recording software for screen scraping – or even $10 (USD) switches that can remove HDCP. Commercial pirate distributors can easily capture video output, then re-encode and redistribute the premium video using their own infrastructure to monetise stolen content.

Fragmentation of content – which happens when consumers need to subscribe to more than one streaming service to get access to all the content they want to watch – makes it even harder for legitimate content owners and providers to compete with illegal subscription services. These pirate content aggregators, not restricted by licensing agreements, monetise stolen content by offering the end user a one-stop shop for the best sports and entertainment programming.

Be sure the service you are considering is highly adaptable to ever-evolving pirate attacks.

Speed

As explained, client-composited watermarking will provide the fastest identification of piracy. If you're dealing with live sports and entertainment, pay-per-view, and on-demand content, this factor should play an important part in your decision on the type of watermarking system to deploy. Think about it in these terms: Several years ago, a major broadcaster – the original source for 60% of the sports channel piracy in its market – introduced ASiD. OTT piracy reduced to less than 1% within weeks.

Global Reach

With today's technology and the speed of the Internet, OTT players will need to protect content in markets throughout the world. Even if you are servicing customers in one country or on one continent, remember that content thieves can and do act without physical borders.

Multi-CDN Service

Some watermarking mechanisms may incur additional charges to support multi-CDN usage. Since OTT services have enough expense and complexity, know that it is possible to find a robust service that incurs no additional expenses for multi-CDN content delivery.

Every OTT operator will have its own criteria, but the bottom line is to carefully select a watermarking service that is cost-effective and results-driven.

Understanding the Human Factor

One of the most challenging aspects in securing an OTT service is the understanding of the human factor in content protection: the end users who are consuming content.

It is essential to start at a level of zero trust, assuming that some users of your service will attempt to circumvent security controls or use your service in a way you didn't intend. This could mean something as simple as sharing their credentials with family or friends, or a more direct attack against your content security systems by bypassing/overcoming licensing restrictions.

To overcome this challenge, understand that the point of zero trust begins as early as sign-up to your service. Protection steps include validation of the presented user profile, location checks, payment fraud detection (such as comparison with other existing users), and enforcement of a suitably complex password with multi-factor authentication to prevent brute force attacks.

Video Viewer Personas

Errant or undesired behavior within your service can typically be broken down into the following personas.

The Over-Consumer

Running an OTT service is expensive. The cost of delivering compressed video to your consumers is one of the most costly aspects, even with high competition driving CDN pricing down. Your service pricing and tiers model against costs, and per–user delivery/CDN cost – driven by view time per user session – is a major factor. Is a user's consumption patterns far more than your predicted model suggests? That could indicate the "over-consumer".

The Frequent Mover

Here, an authenticated and authorised user's sessions change IP addresses frequently in a short period of time, spanning multiple geographies. This is a good indication of a compromised account, with multiple users accessing the service unbeknown to the legitimate account holder.

The Account Sharer

The Account Sharer is characterised by multiple authentication authorisations over time, with different IP addresses/ISPs, and possibly different geographies. As with the Frequent Mover, this pattern could indicate a compromised account. But, it is also possible that a legitimate user has shared their credentials with friends and family – or worse, with a much wider group.

The Out-of-Bounds Viewer

In this case, the user viewing the content is outside of a designated geographic area. Initial authorisation attempts may have been genuine, but other data sources may reveal the user's true location.

The Anonymous IP Viewer

The Anonymous IP Viewer's traffic comes from a suspected, or known, proxy/VPN, or a suspect network source (i.e. cloud infrastructure vendor, rather than ISP).

The Long Viewer

This user watches only live channels, for very long periods in one session.

The Tamperer

The Tamperer's session data indicates tampering with the playback environment Tamper warnings from the code obfuscation solution may have fired. Session token data mismatches may have been logged. You may also see multiple authorisation attempts, and multiple content license request attempts for a single use token.

From sign-up forward, every component within your service should provide user behaviour monitoring to aid in identification of patterns that could indicate fraudulent or suspicious activity. This analysis is important to protect your interests under the terms of your content licensing deals – and critically important for revenue protection.

Using Watermarks for End-to-End Protection

To combat the increasing number of piracy attacks, OTT services must implement solid watermarking and detection as well as DRM. There's a lot at stake: content, revenue and brand – and even investment in delivery infrastructure of systems, software, operations, and technical support.

Start by developing and enhancing understanding of the full content protection strategy, and continue with following the considerations and best practices we've outlined to choose and implement a watermarking service. Only then can you make sure that your players – from one end to the other – are as trustworthy as the technology you've implemented.

To learn more about "How to Trust Your Player," check out the other articles in our series:

- **Article 1 – Tips from the Top: Secure Content Delivery and Playback**
- **Article 2 – Securing Content Access with Digital Rights Management Best Practices**
- **Article 3 – Tips and Tricks: How to Secure Your Content in Challenging Streaming Environments**
- **Article 4 – Beyond Digital Rights Management: Video Watermarking Weighs In**
- **Article 5 – From One End to the Other: Protecting Content From Origination to Playback, Once and for All**

Still want to learn more? View our associated Fireside Chat sessions:

- **Video 1 – Tips from the Top: Secure Content Delivery and Playback**
- **Video 2 – Securing Content Access with Digital Rights Management Best Practices**
- **Video 3 – Tips and Tricks: How to Secure Your Content in Challenging Streaming Environments**
- **Video 4 – Beyond Digital Rights Management: Video Watermarking Weighs In**

Check out the recording of our How To Trust Your Player Webinar: **View Recording**.

For information on redistributing this content, please reach out to **pr@friendmts.com**.

How To Trust Your Player is a collaborative effort between Bitmovin, Friend MTS and Intertrust. Our goal is to educate media and content providers on the importance of delivering streaming content in the most secure ways possible from the video player to the end-consumer while protecting both their content and revenue.

Bitmovin

Bitmovin is a developer of video streaming technology. Built for technical professionals in the OTT video market, the company's software solutions work to provide the best viewer experience imaginable by optimizing customer operations and reducing time to market.

Bitmovin's solution suite – a video encoder, player, and analytics platform – lets content owners redefine the viewer experience through API-based workflow optimization, fast content turnaround, and scalability.

Founded in 2012, the company is based in San Francisco, with offices in major cities in Europe, North America and South America. With more than 250 enterprise customers around the globe, Bitmovin helps power clients like BBC, fuboTV, Hulu Japan, RTL, and iFlix.

Friend MTS

Friend MTS helps media and entertainment businesses secure content so that revenue can grow and creativity can thrive.

With advanced services that measure, monitor, detect and disable content piracy, Friend MTS provides a 360-degree
view of the constantly shifting content piracy protection ecosystem and stays a step ahead of ever-advancing and sophisticated content piracy behavior and technology with a sharp, deliberate, laser-focused commitment to continual monitoring and innovation.

Businesses and nonprofit organizations throughout the world recognize Friend MTS as the leading authority for content and revenue protection. The company also has donated its digital fingerprint technology to the International Center for Missing and Exploited Children to tackle child abuse content online.

Founded in 2000, Friend MTS is headquartered in Birmingham, England, with operations throughout Europe, the Middle East, Africa, Latin America, and North America. Friend MTS is the recipient of an Emmy® Award for Technology and Engineering, presented by the National Academy of Television Arts and Sciences (2018).

Intertrust Technologies

Intertrust provides the world's leading digital rights management (DRM) cloud service with a complete ecosystem of security and rights management products. We empower businesses to securely manage all of their data and devices, regardless of location, format, or type–enabling innovative multi-party apps and services.

Intertrust Media Solutions provides robust content protection solutions for Media and Entertainment. Intertrust ExpressPlay consists of a cloud-based multi-DRM service, broadcast TV security and anti-piracy services with proven scalability in the largest OTT streaming platforms globally.

ExpressPlay DRM™ is today's most complete multi-DRM monetization service for OTT streaming supporting Apple FairPlay Streaming, Google Widevine, Microsoft PlayReady, Adobe Primetime, and the open-standard Marlin DRM. Intertrust also offers ExpressPlay DRM Offline to enable secure streaming of premium content through an offline multi-DRM platform.

Founded in 1990, Intertrust is headquartered in Sunnyvale, California, with regional offices in London, Tokyo, Mumbai, Bangalore, Beijing, Seoul, Riga, and Tallinn.