HOW TO TRUST ▷ YOUR PLAYER

Presented by BITMOVIN, Friend MTS, intertrust

BUILDING AN OTT SERVICE FOR TODAY'S WORLD

Article 1 – Tips from the Top: Secure Content Delivery and Playback

Published date: August 20, 2020

Joshua Shulman, Digital Marketing Specialist, Bitmovin
Alan Ogilvie, Lead Product Manager, Friend MTS
Ali Hodjat, Product Marketing Director, Intertrust

Overview of Over-the-Top (OTT) Platforms

Are you in the OTT world? You're not the only player in this business.

Over the last several years, consumer viewing habits have been shifting from linear broadcast to over-the-top (OTT) platforms and streaming services.

Along with a sudden increase in video consumption and in subscriptions to established OTT streaming services, several new OTT consumer streaming services have launched. Some of those have even adjusted their launch timelines to meet the increased consumer demand for unique content.

Developing the advanced technology needed for an OTT service is challenging. On top of that, companies today face the very real issue of securing content delivery and playback at a multi-player level. First is protecting the technology within your player – the consumer playback device. Beyond that, today's media and entertainment world faces the challenge of protecting your content from the ultimate "players": the potential bad actors, or pirates, at the end-user level. Skip a step and the market opportunities will quickly fade and disappear.

The Shift in Content Consumption

Along with the surge in video consumption and streaming subscriptions, there is also a need to understand the corresponding change in OTT audiences, and what impact that has on your plans.

Before the pandemic began, a large portion of OTT streaming was live sports programming. When sporting events were put on hold, audience viewing shifted toward movies and other premium content. For example, a recent survey from **Altman Vilandrie & Company** showed that half of U.S. viewers are watching more TV and movies since COVID-19 started. Twenty-two percent of consumers are watching an additional five hours of TV or movies per week than they did before COVID-19.

That same survey found that approximately 60% of respondents said they are using a streaming video service. And the most recent projections from **Rethink Research** data show that changing behaviors during the lockdown period worldwide will result in an increase in subscriptions of almost 9% and an increase in revenue of almost 8%.

Evolving Piracy

These changes in viewing behaviors and streaming services have generated new content, subscribers, and services – and interest from content pirates. A recent report from **Parks Associates** finds that the value of pirate video services accessed by pay TV and non-pay TV consumers will exceed $67 billion (USD) worldwide by 2023. Another report from **ABI Research** estimates that more than 17% of worldwide video streaming users access content illegally.

Just as viewing audiences are changing, so is piracy. Now, with the resumption of some sports leagues and live events, pirates who've gained a fitting in movies and other premium content will return to their sports stronghold as well. The current market situation means being continually on the lookout for ways to exploit weaknesses in delivery systems so that they can continue and resume, their illicit (but major revenue-generating) services. For OTT streaming services, it means a real potential blow to the bottom line.

Protecting Your Bottom Line

Launching an OTT service is a complex, labor-intensive, and expensive venture. There are challenges in content acquisition, preparation, and delivery to your audience. Some may think about building a working video consumption environment as simply bolting a few complimentary services together: encoding audio/video, with packaging, for target devices; enabling a Digital Rights Management (DRM) service for license delivery; distributing assets through a Content Delivery Network (CDN); and setting up playback through a player framework.

Yet, all of that work can quickly become a waste of resources without the steps to protect content and revenue and fully combat piracy. Today, companies creating OTT services need to implement a nuanced approach that requires insight and diligence, especially when it comes to the communication between components, and the delivery of assets from content-preparation systems to consumers.

In the race to launch a service, with looming deadlines and high-value marketing programs providing no latitude for changes in go-live dates, companies often drop features from launch requirements. While this happens across the service delivery pipeline, the systems designed to protect a company's revenue lines through secure content delivery are often among the most frequent victims.

We've seen it happen time and time again. A large service launches with premium exclusive content, only to discover the same exclusive content appearing and being distributed through pirate services within hours. The good news: It doesn't have to happen to you. Take steps upfront to secure content, and you'll not only realize a timely return on your investment but see bottom-line numbers that would be impossible otherwise.

OTT Service Tips and Best Practices From Industry Experts

This is the time to move swiftly, yet carefully and precisely. So, to help guide you in building and implementing an effective, protected OTT service, we've come together to share tips and best practices in a five-part article series. As partners, we've protected OTT content and revenue for media and entertainment companies across the globe. Now, we'll share our collective knowledge with you.

Following the best practices we outline will ensure that you are protecting your content from the technology side as well as the ultimate end-user side. You can make sure that your end users are as trustworthy as the technology you've implemented.

We'll show you how to secure the delivery of your content from origination all the way through to your end users via browser-based players. We'll walk you through the common mistakes companies make when securing access to content catalogs. We'll explain how and when multi-DRM service works, when and how watermarking comes into play, and how hardening the player all play a part in disrupting the redistribution of valuable content outside its legitimate intent.

In discussing the challenges faced during implementation, testing, and delivery, we'll outline best practices for:

- Packaging high-value assets for secure delivery
- Securing and protecting DRM license acquisition workflow
- Authenticating user sessions before content delivery
- Configuring playback session concurrency and device limits
- Hardening the browser playback environment to mitigate attacks
- Forensic watermarking and active monitoring

In addition, we'll demonstrate a Reference Implementation using technology from each partner, addressing the best practices covered in the article series. By reviewing this best-practice implementation of multi-DRM services, watermarking, and hardening the player within a working demonstration environment – on a web browser – you'll clearly understand the process of delivering streaming media content from content through to a player device in the most secure and protective environment achievable.

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.