ASiD OTT

Protecting Exclusive OTT Content
from Streaming Piracy

Introduction

In recent years, the global penetration of online streaming has been steadily rising, with an increasing number of consumers paying for one or more OTT services, attracted by the wide array of content, flexible subscription options, and a low price point. With intensifying competition in the OTT space and a limit on consumers' monthly video spending, OTT churn has also been on the rise.

Fragmentation of content, requiring consumers to subscribe to multiple streaming services to access all of the content they want to watch, has been making it especially hard for legitimate content owners and service providers to compete with illegal subscription services. Unrestricted by any licensing agreements, the pirate content aggregators have been ardently monetising stolen content, offering a one-stop shop with the best sports and entertainment programming.

With shifts in consumer viewing habits and theatrical windows, the pandemic has further accelerated these industry trends. Pirates that have always been looking for ways to break anti-piracy technologies have upped their game with new more sophisticated circumvention techniques to serve the increased demand for premium video online including high-value PVOD content.

Now more than ever before, OTT service providers offering exclusive premium content, both to attract new subscribers and maintain loyalty, need to protect this content from theft by commercial pirates in order to safeguard its integrity and consequently their profits, reputation, and subscriber numbers.

Is your exclusive content fully protected from theft?

In order to protect their revenue model, content owners and distributors setting up a premium video streaming service typically safeguard their valuable content by employing a digital rights management (DRM) system, however, there appears to be limited awareness among OTT businesses that a DRM system is designed to provide content protection only up to the point of consumption by viewers, and video assets also need to be protected "beyond the screen".

In the meantime, using a legitimate service subscription with freely available screen recording software or a cheap HDMI splitter (to remove HDCP), pirate distributors are easily capturing video output to redistribute and monetise premium content on their own infrastructure.

Span of DRM content protection
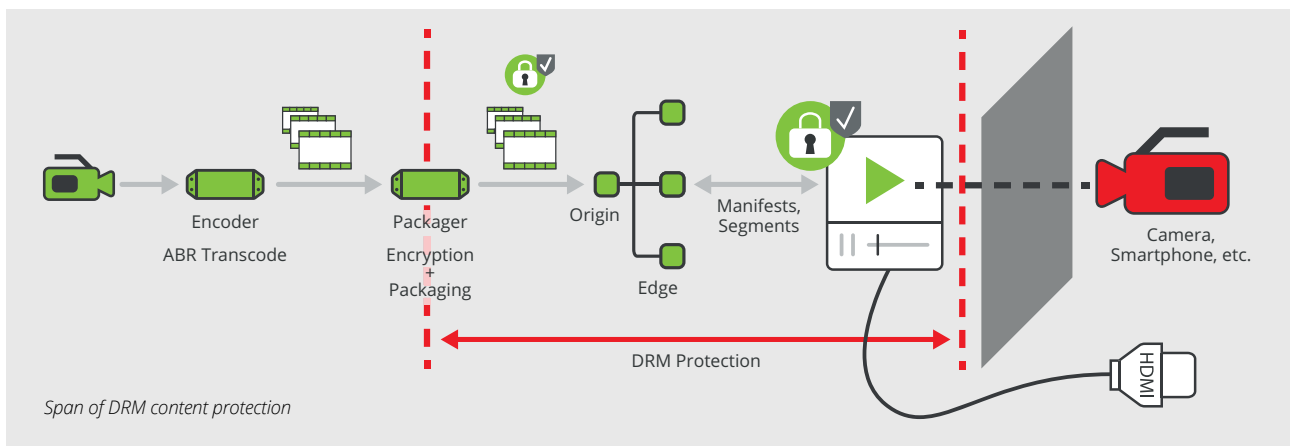
The complexity of the problem of commercial piracy worldwide is illustrated in a **report from the European Union Intellectual Property Office (EUIPO)**. It reveals sophisticated pirate ecosystems comprising a whole host of different illegal players that support and profit from illegitimate redistribution of premium content. These complicated criminal networks use ordinary service subscriptions offered by legitimate content owners or providers as a source of video content.

Ecosystem of illegal IPTV (image courtesy of EUIPO)
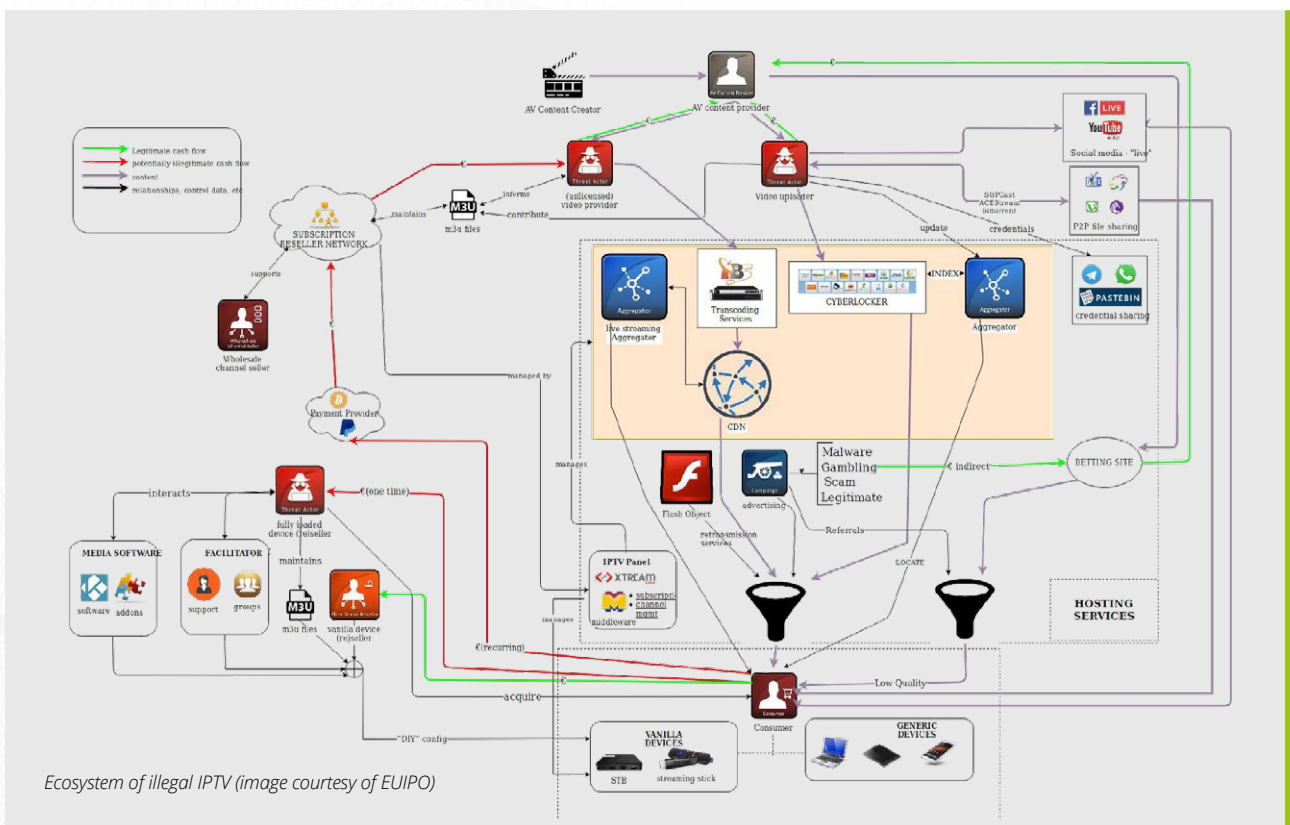
Solid protection from the commercial piracy revenue drain

To detect theft from a player's output, subscriber-level watermarking is used. Such a solution enables identification of legitimate streams that are being pirated, allowing content distributors to revoke access as necessary to effectively control where their content flows and stop pirates gaining financially from illegally reselling the assets.

The most widely used subscriber-level watermarking today is ASiD (Advanced Subscriber Identification) from Friend MTS. Combined with in-house content monitoring, ASiD end-to-end solutions effectively disrupt content theft and are trusted by many of the biggest brands in the media and entertainment industry.

The primary reason behind the widespread deployment of ASiD across the globe is its proven ability to identify the source of stolen content, helping to make the complex problem of large-scale for-profit piracy manageable through effective disruption of the illicit content redistribution chain.

Through integration with a customer's subscriber management system, ASiD enables rapid automated termination of content theft in just a few minutes, plugging the source of a leak that feeds the criminal network downstream and thus erodes the brand and profit of the legitimate content owner or provider.

Decisive and timely action is crucial when owners or distributors of exclusive content are up against pirate services operating behind non-compliant infrastructure vendors, where sending DMCA notifications is a slow or even an entirely ineffective measure to protect this valuable content.

Robust compliant protection

ASiD OTT watermarking solutions are highly secure and totally imperceptible. Fully compliant with the MovieLabs Specification for Enhanced Content Protection, including 4K/UHD and HDR content, ASiD solutions provide robust protection against illegal redistribution of high-value VOD content including early-window PVOD.

Smart large-scale piracy takedown for the biggest content brands

To protect the integrity of exclusive content, it is important to ensure that all financially damaging pirated content is detected and taken down rapidly and responsibly. It requires a watermarking content protection service to offer scalability and precision as key characteristics. Enhanced with ASiD iQ, ASiD OTT solutions can deliver smart proactive anti-piracy response.

In search of the watermarked content, Friend MTS' content monitoring platform automatically captures and analyses millions of videos every day. Video content is captured from websites, social media platforms, Kodi and Android-based illicit streaming services, and mobile apps for comprehensive illicit content detection regardless of the distribution channel that pirates are using to monetise stolen content.

Friend MTS' proprietary fingerprint-based content recognition technology enables the automated analysis of captured videos at massive scale and identification of stolen assets with next-to-zero false positives.

Once identified, stolen content captures are shortlisted for watermark extraction[1]. As only captures of very short duration are needed to extract a watermark from[2], the extraction process is ultra-fast.

1 With ASiD iQ a list of abused subscription accounts can be collated to proactively reduce the suspect pool for even faster watermark extraction and pirate takedown.
2 The required length of the video capture for watermark extraction can vary based on a particular ASiD OTT solution.

With this highly-automated fingerprint-augmented content monitoring and subsequent ultra-fast watermark extraction, ASiD has a proven track record of successfully scaling for the most popular global live sporting events, able to handle huge spikes in the number of concurrent viewers.

With unpredictability of the number of subscribers flocking to a newly offered highly-anticipated OTT service, the scalability of ASiD helps the service provider to be confident in their ability to offer a smooth viewer experience from the start while ensuring full protection for their premium video content.

ASiD iQ

An enhancement of ASiD OTT solutions, ASiD iQ is an account monitoring tool that feeds back and aggregates intelligence on user behaviours to automatically recognise fraudulent behavioral patterns.

This active device monitoring generating live metrics, allows to adapt the watermark scheme in real time to appropriately counter pirate attacks at the time when OTT / streaming services are becoming the focus for piracy.

A family of end-to-end solutions for a complex distribution strategy

For the OTT streaming service providers that are planning to maximise distribution of their exclusive content by leveraging legacy distribution platforms or third-party distribution networks, ASiD offers a breadth of watermarking solutions for complete platform protection across new and legacy STBs, gaming platforms, mobile devices, etc.

	ASiD Embedded	ASiD OTT Client-composited	ASiD OTT Edge-switched
Operator-Supplied & Managed			
Broadcast STB	✓		
Hybrid Broadcast/IP STB	✓	✓	
IPTV STB	✓	✓	
OTT-enabled STB	✓	✓	
Operator-Supplied, Not Managed			
IPTV STB		✓	✓
OTT-enabled STB		✓	✓
Third-Party Clients/Devices			
OTT apps (e.g. iOS/tvOS, Android, Fire TV)		✓	✓
OTT web-browser based		✓	✓

Broadcast STB is a set-top box that enables viewers to access the broadcast TV delivery method.
Hybrid Broadcast/IP STB is a set-top box that enables viewers to access both broadcast and over-the-top / over the web TV delivery methods.
IPTV STB is a set-top box that enables viewers to access the IP (e.g. multicast) TV delivery method.
OTT-enabled STB is a set-top box that enables viewers to access over-the-top / over the web TV delivery method.
OTT apps are apps that enable viewers to access over-the-top/over the web TV delivery method.
OTT web-browser based are web-browser based solutions that enable viewers to access over-the-top/over the web TV delivery method.

Friend MTS ASiD watermarking applications

All watermarking solutions from Friend MTS, both distributor- and subscriber-level, work seamlessly together. In a mixed device environment (broadcast, managed and unmanaged OTT) a single watermark extraction pipeline enables the most device-appropriate solution to be used in each case to provide effective and efficient end-to-end protection.

Distribution iD

Subscriber-level ASiD can be also combined with Distribution iD, the distributor-level watermarking solution from Friend MTS. This multi-layer content protection ensures that valuable content is safeguarded across the whole delivery chain. With Distribution iD, a partner with a security breach can be rapidly traced, and content protection measures can be focused in the right place.

Proven protection for exclusive content

Following successful protection of exclusive content at the 64th BFI London Film Festival, Friend MTS partnered with the British Film Institute (BFI) to provide watermarking protection for 20+ exclusive titles at the BFI Flare: London LGBTIQ+ Film Festival, the annual event that was held online. The premieres were streamed for the BFI Player festival ticket holders only. This exclusive content was geo-restricted to the UK audience and the access time was limited for each festival film.

ASiD OTT provided BFI with robust content security for these exclusive titles premiered online. Lightweight and totally imperceptible, ASiD watermarking technology had no impact on the delivery of content or quality of experience and viewers' engagement.

Quickly and seamlessly integrated, ASiD OTT Client-composited solution effectively protected from illegal restreaming all available feature films on BFI Player as part of the festival programme.

ASiD iQ, a business intelligence enhancement of the ASiD OTT solution, was used to retrospectively interrogate and analyse watermark session log information in order to further support the identification of any suspected bad actor through watermark extraction.

"Friend MTS' ASiD solution has given us more confidence presenting exclusive online premieres. Their service is easy to integrate with, cost-effective and their team's support is top-notch."

Margo Cayla, Product Manager, Digital & Ventures, British Film Institute

Turnkey implementation

ASiD OTT Client-composited can be implemented quickly by customer engineering teams, with simple SDKs for all platforms plus full documentation and support from Friend MTS as required. It is effectively a turnkey ASiD solution for customers that are looking to launch their OTT service in the shortest time possible without compromising premium video security and ensuring maximum content protection from restreaming piracy.

Conclusion

With implementation of an effective subscriber-level watermarking solution, OTT service providers can ensure their exclusive premium content, including high-value PVOD, is protected beyond DRM and illegally redistributed assets are tracked down and taken down fast across websites, social media platforms, illicit streaming devices, mobile apps, and other distribution channels.

OTT businesses aiming to scale their operations by leveraging legacy distribution platforms or third-party distribution networks can ensure efficient and effective protection with a single watermark extraction pipeline and a suite of watermarking solutions that work seamlessly together.

With the acceleration of online streaming penetration, content owners and distributors can ensure that implementation of watermarking does not increase time-to-market for their OTT offering.

Utilising ASiD end-to-end solutions from Friend MTS, OTT businesses can rest assured that their exclusive premium content is fully protected. With its proprietary state-of-the-art technologies and highly effective services and solutions Friend MTS rapidly disrupts illegal for-profit content redistribution helping exclusive content owners and distributors to reduce subscriber churn and stay ahead of the competition.