Friend MTS
Protecting content + revenue

ASiD OTT

Protecting Exclusive OTT Content from Streaming Piracy

Application Note

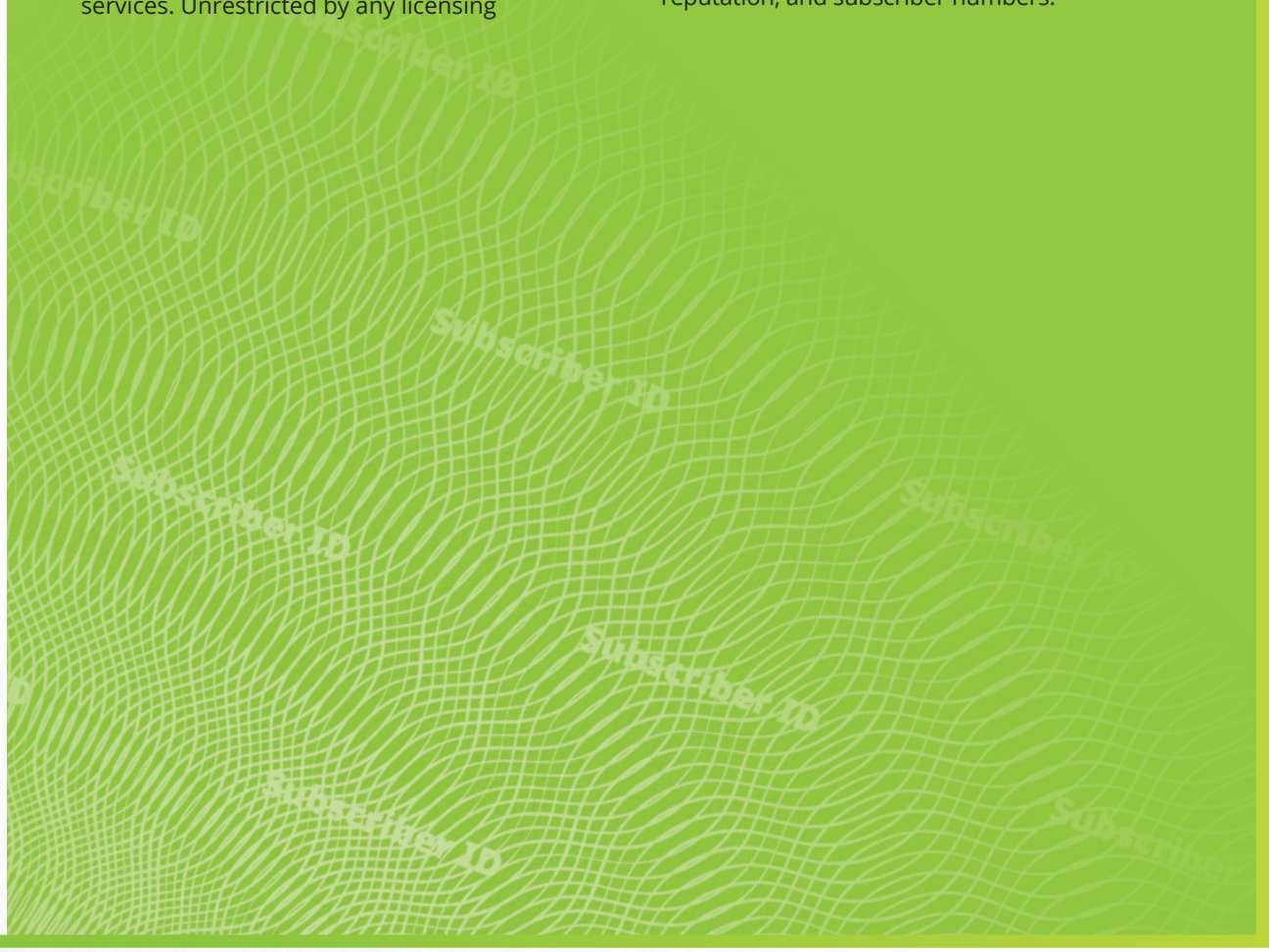
Introduction

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. Competition in the OTT space has been intensifying, and with the constantly growing number of players in the market 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 the recent introduction of such services as premium video on demand (PVOD) and virtual season ticket (VST), these trends have only become stronger – unlike the current economy and the disposable income of many households.

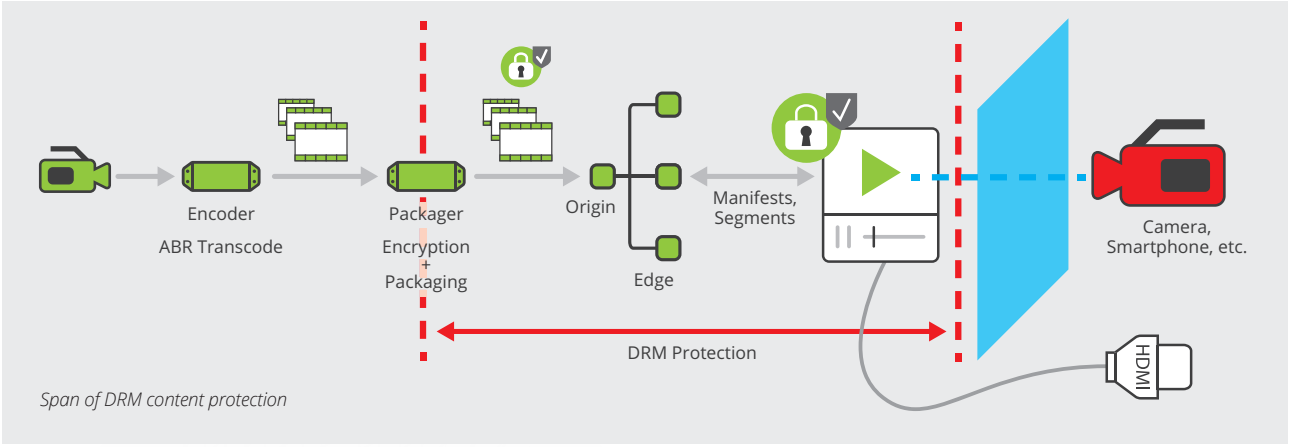
Now more than ever before, OTT service providers offering exclusive premium content, both to attract new subscribers and maintain loyalty, need to protect the content from theft by commercial pirates in order to safeguard its integrity and consequently their profits, reputation, and subscriber numbers.



Is your exclusive content fully protected from theft?

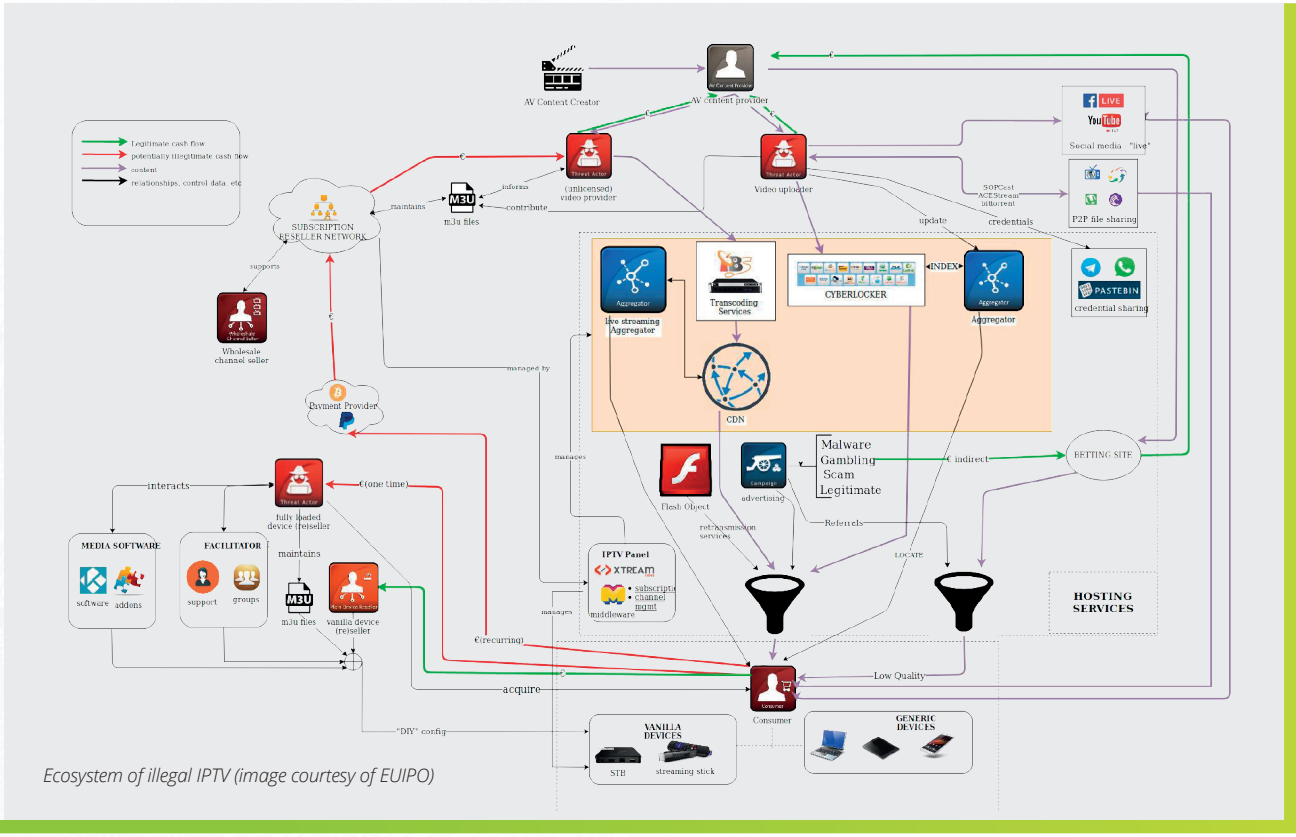
In order to protect their revenue model, content owners and distributors setting up a premium video streaming service typically safeguard their valuable content by employing a digital rights management (DRM) system, however, there appears to be limited awareness among OTT businesses that a DRM system 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 strip HDCP), commercial 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 technologies are 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 accordingly stopping pirates gaining financially from selling the content.

The most widely used subscriber-level watermarking solution today is ASiD (Advanced Subscriber Identification) from Friend MTS. This client-composited watermarking technology is a key component of the Friend MTS content protection service, trusted by many of the biggest brands in the pay-TV 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 commercial 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 content owners and distributors are up against pirate services operating behind non-compliant infrastructure vendors, where sending DMCA notifications is a slow or even an entirely ineffective measure.

ASiD OTT watermarking is highly secure and totally imperceptible. ASiD has been independently tested for robustness by Cartesian and evaluated by 'golden eyes', making it Hollywood Studio approved.

Large-scale, high-precision 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.

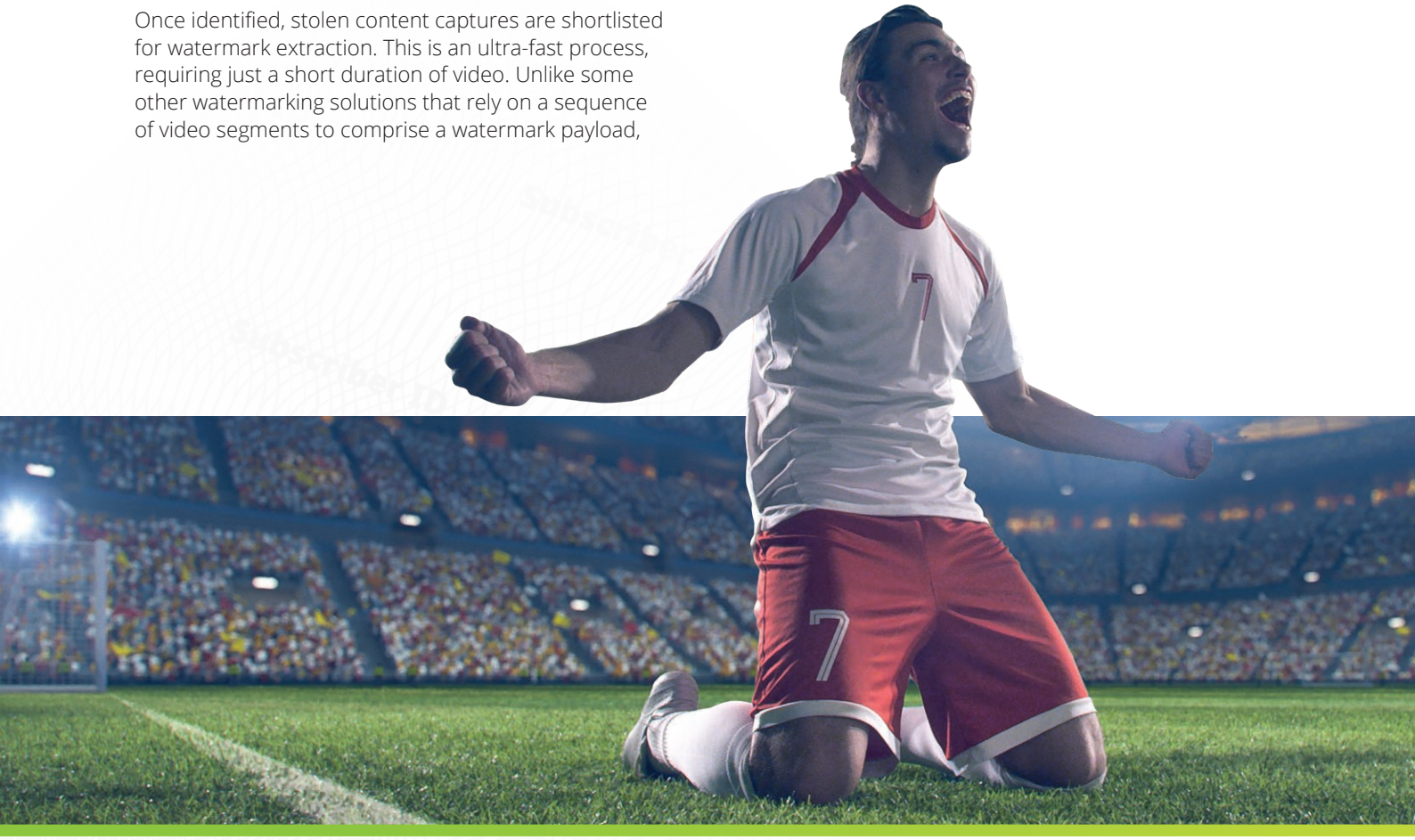
The ASiD service operates on top of the Friend MTS Global Monitoring Platform which automatically captures and analyses millions of videos every day. Video content is captured from websites, social media platforms, Kodi and Android-based illicit streaming services, and mobile apps for comprehensive illicit 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 identification of captured videos at massive scale, with next-to-zero false positives.

Once identified, stolen content captures are shortlisted for watermark extraction. This is an ultra-fast process, requiring just a short duration of video. Unlike some other watermarking solutions that rely on a sequence of video segments to comprise a watermark payload, ASiD implements a graphical overlay structure with an imperceptible pattern that covers the whole screen at all times.

Designed for both live and on-demand content, ASiD has a proven track record of successfully scaling for the most popular global live sports 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 provide a smooth viewer experience from the start while ensuring full protection for their premium video content.



A turnkey watermarking solution for fast OTT service launch

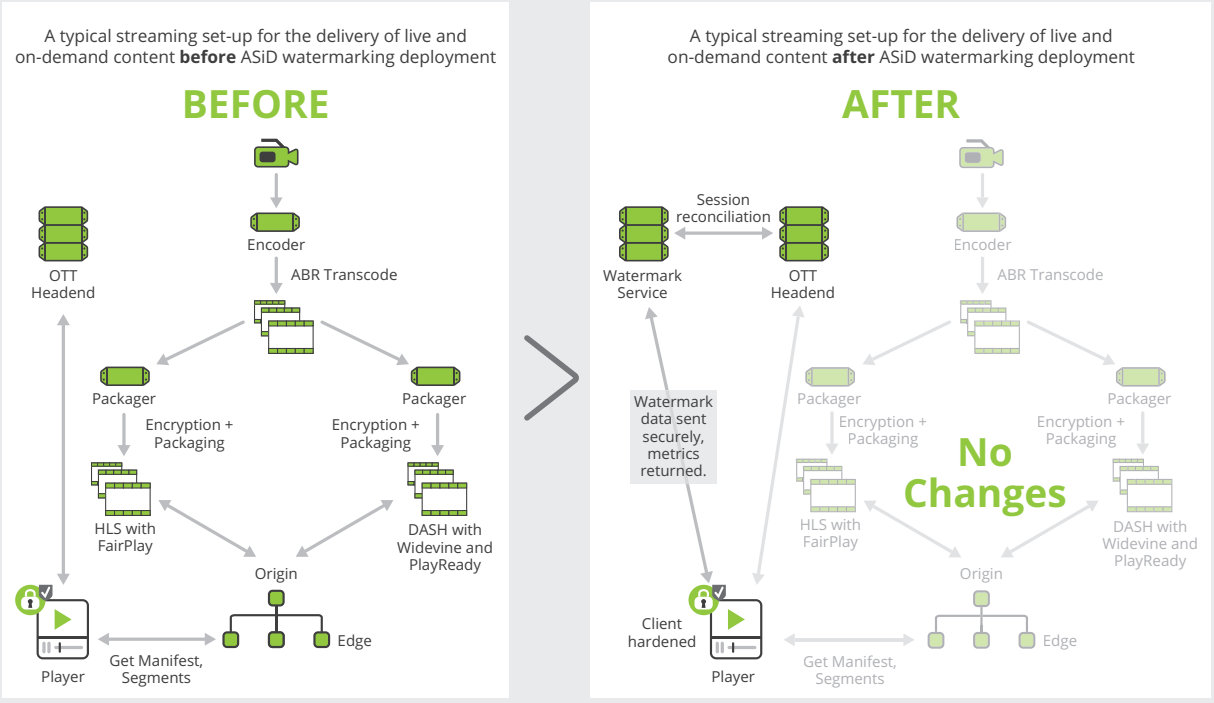
Without the need to introduce any delivery pipeline changes or non-standard modifications, ASiD can be implemented quickly by customer engineering teams, with simple SDKs for all platforms plus full documentation and support from Friend MTS as required.

As the ASiD watermark is composited on top of the video at the client side, it does not require access to decoded video, and for services implementing a multi-CDN architecture, ASiD does not impose any technical burden.

Secure delivery of the content to the client is a prerequisite for deployment of ASiD, and the client should be effectively hardened with a commercial-grade solution (according to the Open Web Application Security Project/OWASP guidelines, all watermarking solutions, regardless of whether they use server-side or client-side technology, require client environments to be obfuscated and hardened to resist tampering).

The securing of streaming content with DRM however is a must for any security-conscious platform that carries premium content, while hardening of OTT clients is also necessary to support other key functionality, for example, scalable concurrency management.

ASiD OTT from Friend MTS is effectively a turnkey 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.



Friend MTS ASiD watermarking deployment in an OTT environment

A single watermarking solution for a complex distribution strategy

ASiD watermarking is a truly universal solution that can solve piracy issues in multiple scenarios. In addition to pure streaming/OTT players, it supports broadcast-only and streaming-enabled set-top boxes (STBs) as well as multicast and unicast streamed delivery.

Applications	ASiD from Friend MTS
Broadcast STB	✓
Hybrid Broadcast/IP STB	✓
IPTV STB	✓
OTT-enabled STB	✓
OTT apps and players	✓

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 and players are apps and players that enable viewers to access over-the-top/over the web TV delivery method.

Friend MTS ASiD watermarking applications

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 watermarking provides a universal solution that offers broad coverage across new and legacy STBs, gaming platforms, and mobile devices for complete platform protection.

Moreover, ASiD is optimised for live and on-demand content and delivers an equally high level of protection for both. As a result, there is no need to implement different watermarking solutions depending on the type of content requiring 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. By identifying the international or national distribution paths behind content theft, Distribution iD improves the targeting of enhanced security in the regions where piracy is prevalent.

The most cost-effective watermarking solution

As a client-composited watermarking technology, and unlike server-side watermarking solutions, ASiD from Friend MTS does not require any pre-processing, encoding, or repackaging of the original video, all of which impose an additional financial burden.

Also, in contrast to watermarking solutions based on A/B variant server-side technology that utilises a dual-stream approach, ASiD does not require any additional encoding or storage expenses.

Overall, the deployment of ASiD is by far the most cost-effective approach when compared with the deployment of other watermarking solutions available in the market

		ASiD
Type of watermarking technology	A/B Variant, server-side	Client-Composited, client-side
Cost implications	Higher delivery infrastructure and support costs Storage increase Additional expenses for multi-CDN solutions	No additional delivery infrastructure and support costs No storage increase No additional expenses for multi-CDN solutions

Cost implications: A/B variant vs. ASiD client-composited watermarking

Adaptable technology, results-driven service

In order to be successful against streaming piracy, watermarking needs to be robust and withstand attempts at tampering, such as scaling, cropping, masking, recompression, as well as more sophisticated collusion and image processing attacks.

ASiD from Friend MTS safeguards tens of millions of STBs and OTT players, yet even for the largest-scale deployments, ASiD has not been compromised by pirates in either broadcast or OTT environments. The reason for this high level of robustness against attack lies in the nature of the innovative and highly adaptable ASiD technology.

Firstly, in contrast to some other watermarking solutions, the implementation of ASiD cannot be readily observed and subsequently re-engineered. This innovative approach to watermarking prevents pirates from capitalising on their knowledge of well-exploited traditional lines of attack and perfected methods of attack execution.

Secondly, with a lightweight structure and easy deployment, ASiD is a highly agile solution and has proven to be adaptable to the constantly evolving real-world attacks orchestrated by technically sophisticated pirates. Over the course of several years, Friend MTS has constantly evolved the ASiD technology and deployment methods in line with technology developments and new types of attack (or modifications of existing attacks) that the pirates have employed.

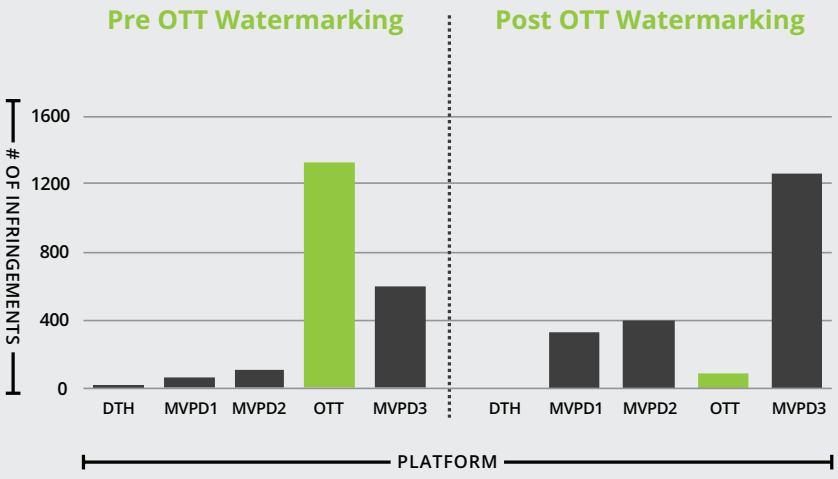
Fully developed in-house, ASiD watermarking is an integral part of the Friend MTS content protection service. Relying on the deep technical expertise of the leading video security specialists in the industry, ASiD technology and service have been rapidly evolving in response to and well ahead of the real-world tactics that technically sophisticated pirates deploy.

Major OTT platform cut sports piracy of protected channels by

97% within days

Tier 1 broadcaster reduced set-top box piracy of protected channels by

98%



ASiD watermarking and content monitoring: achieving real results

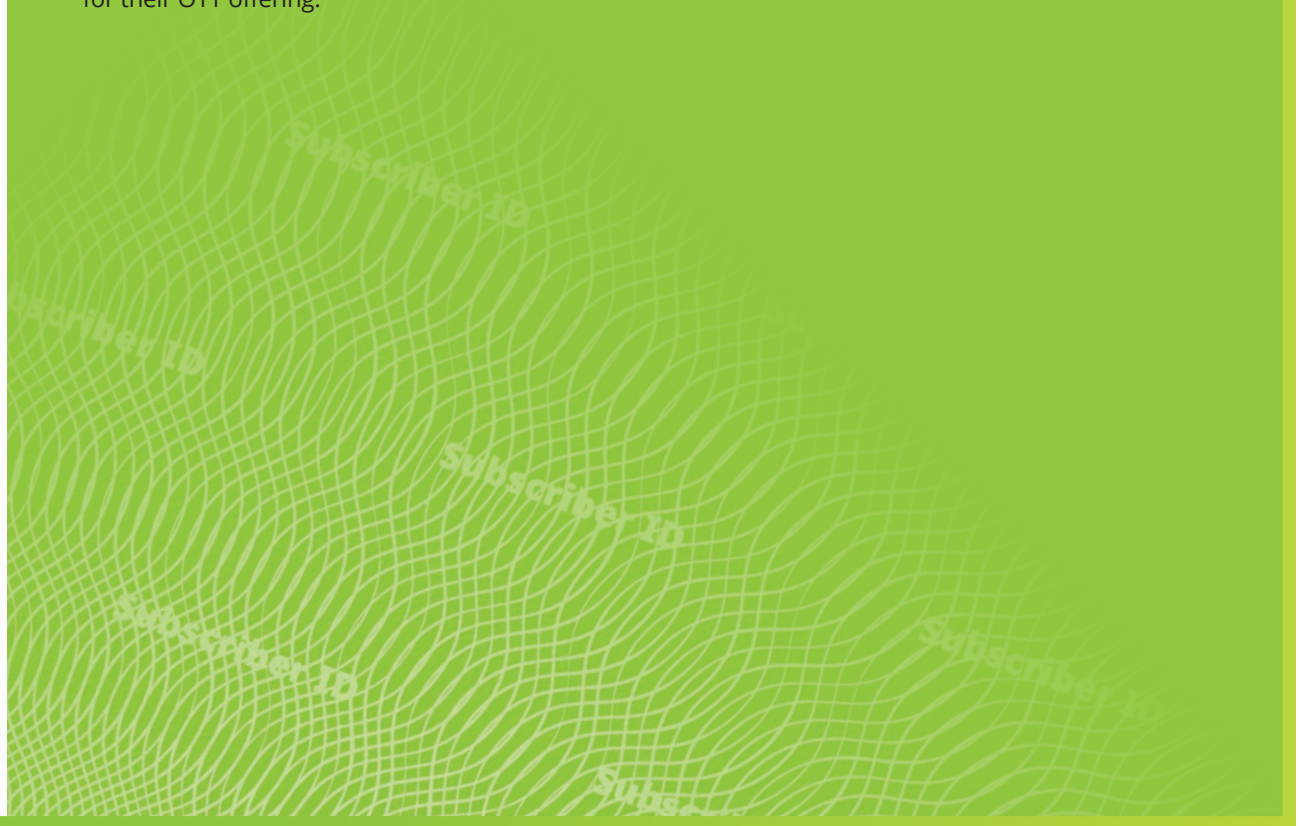
Conclusion

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

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.

OTT businesses aiming to scale their operations by leveraging legacy distribution platforms or third-party distribution networks can ensure that their investment remains cost-effective by deploying a universal watermarking solution that offers equally robust content protection for both broadcast platforms and OTT.

Utilising the Friend MTS ASiD service, OTT businesses can rest assured that their exclusive premium content stays protected with adaptable technology that evolves quickly and remains secure against real-world pirate attacks.



Contact us for a demonstration today

EMEA & APAC
Simon Hanna
shanna@friendmts.com
+44 (0) 203 588 2123

Americas
Brad Parobek
bparobek@friendmts.com
+1 303 902 2209

Friend MTS

www.friendmts.com