

EBOOK

**SECURELY WE STREAM,
UNITED WE PLAY**

How Safeguarding Streaming
Sports & Esports from OTT
Piracy Can Impact Your
Bottom Line

Jan 2021

Table of Contents

03

Foreword

04

**Executive
Summary**

06

**Best
Practice #1:**

DRM

08

**Best
Practice #2:**

CODE PROTECTION

10

**Best
Practice #3:**

WATERMARKING

12

Conclusion

FOREWORD

Sport is, at its core, a business of content, one whose value has long existed in intellectual property rights and exclusivity. Protecting these cornerstones of the business has never been more important, particularly at a time when live content remains the industry's most crucial revenue stream.

As is the case in the wider world of media and entertainment, streaming piracy has become one of the gravest threats to the sports and competitive gaming industries. Intellectual property theft in all its forms has only risen in line with the recent proliferation in digital platforms and streaming services, with online hackers and pirates able to prosper in a world of multi-device distribution and rapidly evolving consumption.

We at SportsPro continually hear how rights holders and content publishers in sport and gaming are becoming increasingly aware of this all-too-pervasive threat. Many of those organisations have set out to establish direct relationships with their fanbases through owned and operated over-the-top (OTT) platforms and digital offerings, but most are yet to fully understand what can be done to properly protect their streaming apps and services.

Indeed, for many sports businesses, comprehensive content protection measures, advanced anti-piracy solutions and other technological methods for enhancing security still rank low on the priority list, even if the risk to their bottom line is more serious and more immediate than ever.

It is with this in mind that our partners at Verimatrix present this report on how to thwart video streaming and OTT piracy in sports and esports. With real-world examples and mission-critical insights, the report clearly outlines three all-important best practices for developing an effective and robust security strategy.



Michael Long
Editorial Director
SportsPro

EXECUTIVE SUMMARY

The world of sports, esports and media looks quite different than it did earlier this year. As streaming content takes over as the dominate form of consumption, content protection measures need to be increased as piracy is also on the rise. Sports content has been especially impacted, as coronavirus suddenly halted spectatorship. Now that esports has also gone digital, popular in-person tournaments have been replaced with an emerging new category of competitive gameplay, broadcast to millions of fans around the world. This content is now much more vulnerable to the wiles of hackers, pirates and cheats. In all, sports-related distribution has never been a juicier target for revenue and reputation theft.

Streaming services have changed the way fans consume content – while inadvertently increasing the threat of piracy; the distribution of live sporting events is where the money is, and droves of bad actors are hot on the money trail in search of easy treasure.

A recent study of more than 6,000 sports fans found that 51% still use pirate services to watch live sports on a monthly basis, despite 89% of respondents owning a pay-tv subscription.*

Every day, legitimate streaming services like Netflix, Amazon Prime Video, Apple TV+, HBO Max, Disney+ and Twitch are competing with pirated sites for viewers. For example, in June 2020, Spanish police took down an illegal streaming service offering 40,000+ TV channels, movies and other content via websites hosted on an international network of servers. The illegal service looked legitimate and offered subscription prices much lower than legal market prices.¹

In the last decade, esports has grown into a multi-billion dollar industry, with studies suggesting that it will have more viewers than most major professional sports leagues by 2021. Mirroring traditional sports, professional esports leagues have cropped up in Overwatch, League of Legends and others, led by some of the most talented gamers across the globe and household brands including Coca-Cola, Red Bull and Honda are getting involved.

*In the three-month period
ending September 30, 2020,*

***gamers watched
7.5 billion hours***

of livestreamed content.²

***This was primarily comprised of time
on Twitch, Facebook and YouTube.***

1: <https://advanced-television.com/2020/06/11/spanish-police-takes-down-pirate-service/>

2: <https://www.techspot.com/news/87022-gamers-watched-746-billion-hours-content-livestreaming-platforms.html> Oct 7, 2020

In the streaming wars – where every viewer matters and every dollar counts – digital content providers with comprehensive security in place are the most likely to survive and thrive.

Best Practice #1: Select the Right DRM

Streaming video and gaming companies have an extrinsic need to better protect their businesses by broadening their knowledge and strategic planning around security. It's critical to be quick to market with comprehensive security that does not hinder - but enhances - the user experience.

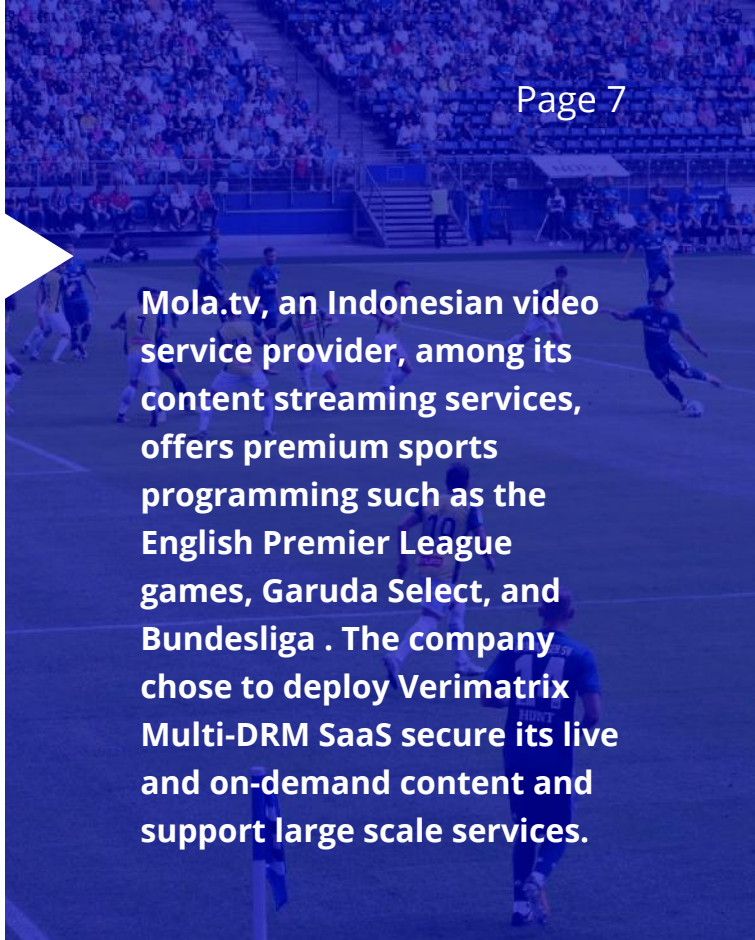
DRM is the first line of defense for streaming video piracy prevention. It ensures content is encrypted, whether in storage, transit or delivery, and delivers the right key and content ID to authenticated users for their playback environment. An effective DRM solution must work with the vast majority of playback devices, integrate easily into the workflow, and appear transparent to users. In the case of esports and gaming, digitization has greatly eased access for consumers, which invites piracy. DRM is used to combat piracy by embedding code that places limits on copying the game, the number of computers the game can be installed on, and/or the number of accounts that can be associated with the game.

Understanding the nuances of encryption encoding, packaging, and overcoming storage and processing requirements are the foundational elements to consider in a multi-DRM implementation. Additional challenges include:


- **Ensuring consistency in user experiences across all devices with the immediate acquisition of keys from DRM servers**
- **Staying on top of ever-changing client devices and associated SDKs along with operating system variations**
- **Monitoring and adhering to complex licensing and protection agreements, such as time shifting, catch-up viewing, cloud-based DVR usage, and offline playback**

To meet this full set of requirements and ensure that content is protected throughout the workflow, you'll need to develop a key management solution, set up license servers, and define and manage security policies that determine the conditions under which the content may be played.

In particular to streaming sports providers, it's important to find a cloud-based multi-DRM service that offers flexibility and scalability so that you remove the risk of over-provisioning and incurring unnecessary costs. The pay-as-you-need model enables maximum global reach and redundancy. The execution speed with low risk is another factor, and best evaluated by previous deployments and the breadth of pre-integrated partners the DRM provider has. To learn more about the benefits of the Verimatrix Multi-DRM solution, [click here](#).



Mola.tv, an Indonesian video service provider, among its content streaming services, offers premium sports programming such as the English Premier League games, Garuda Select, and Bundesliga . The company chose to deploy Verimatrix Multi-DRM SaaS secure its live and on-demand content and support large scale services.



Esports is also a sector with monetized content streams requiring protection from piracy. This multi-million-dollar industry has its own sponsors, leagues and competitors - and every major gaming platform today relies on DRM. Companies like Valve, Epic Games, Microsoft, Sony and Nintendo all own players' libraries in some form. Although there are DRM-free games, the vast majority of digital games employ DRM in one way or another. The DRM does not impact the game in any way; It's simply there to validate a gamer's the license to play. While some players aren't so agreeable when it comes to DRM, it does afford them many features that enable them to restrict how games are distributed.

Best Practice #2: Don't Forget to Protect your Apps/Code

Once competition rises to the professional level, it doesn't matter if the playing field is made of grass or computer graphics – it invites temptation to cheat, and therefore requires strict regulations. Both sponsors and spectators will turn away if they learn software was used to achieve victory, or that a team intentionally lost for money.

For esports specifically, application shielding can stop modification to games and prevent cheating so that in-game economy is preserved. With competitive esports and tournaments, application shielding can prevent API abuse with the client-server protocol, which could prevent someone from impersonating a player online.

Application vulnerabilities

App repackaging, or cloning, is currently one of the most common attacks. Android is especially prone to this, as [one study analyzed](#) 1.7 million free Android apps and found less than 25% had used any kind of code obfuscation – meaning their app can be read, copied and manipulated very easily. Adding to this, the percentage of apps using robust application shielding beyond simple obfuscation is significantly smaller.

Further research from this study showed the majority of respondents of 70 participating developers failed to protect a sample app, and many believed they had actually done so. Very popular apps with 10 million + downloads used obfuscation only 50% of the time. Not great odds.

It is now essential to protect streaming apps, as well as the video content they deliver. Without sufficient code protection, any app can be reverse engineered, essentially creating a clone, with a various ways of endangering your revenue stream.

STEALING REVENUE

- An illegal copycat app can be created to sell subscriptions, with the subscription revenue going straight into the hackers' pockets.
- Hackers may choose to run their own advertising on the content, where the ad revenue again goes to them.

STEALING DATA

- The app can install malicious code, logging passwords, or other confidential/personal information.
- Hackers may go after user data stored in backend databases.
- Ability to replicate credentials may also create an access point into other corporate data.

STEALING CONTENT

- The content from within the app can be redistributed. Real credentials are used to logon and then a cloud recorder can capture and push the content elsewhere to be restreamed.

To select the proper app protection solution, start by looking at emerging video app requirements. Movie studios are starting to mandate app security in their licensing contracts, the same way they do with DRM, which have two components:

Obfuscation to make code difficult to read and understand, which protects it from static analysis.

Environmental checks to ensure the app is only running on a trusted device and hasn't been sideloaded elsewhere.

Service providers can take this a step further. In order to trust that the code base is executing as intended by the developer, they can also implement anti-tamper technology. Using anti-tamper, any attempt by an attacker to circumvent security measures or otherwise modify code, will be blocked. This greatly increases the security level of the whole app. Anti-tamper also prevents repacking attacks mentioned earlier.

By differentiating mobile video apps with application shielding techniques, you can demonstrate you are using best practice to protect content. Therefore, you can gain access to a larger and better content library than your competition and thus, help grow your business. To learn more about app security, [click here](#).

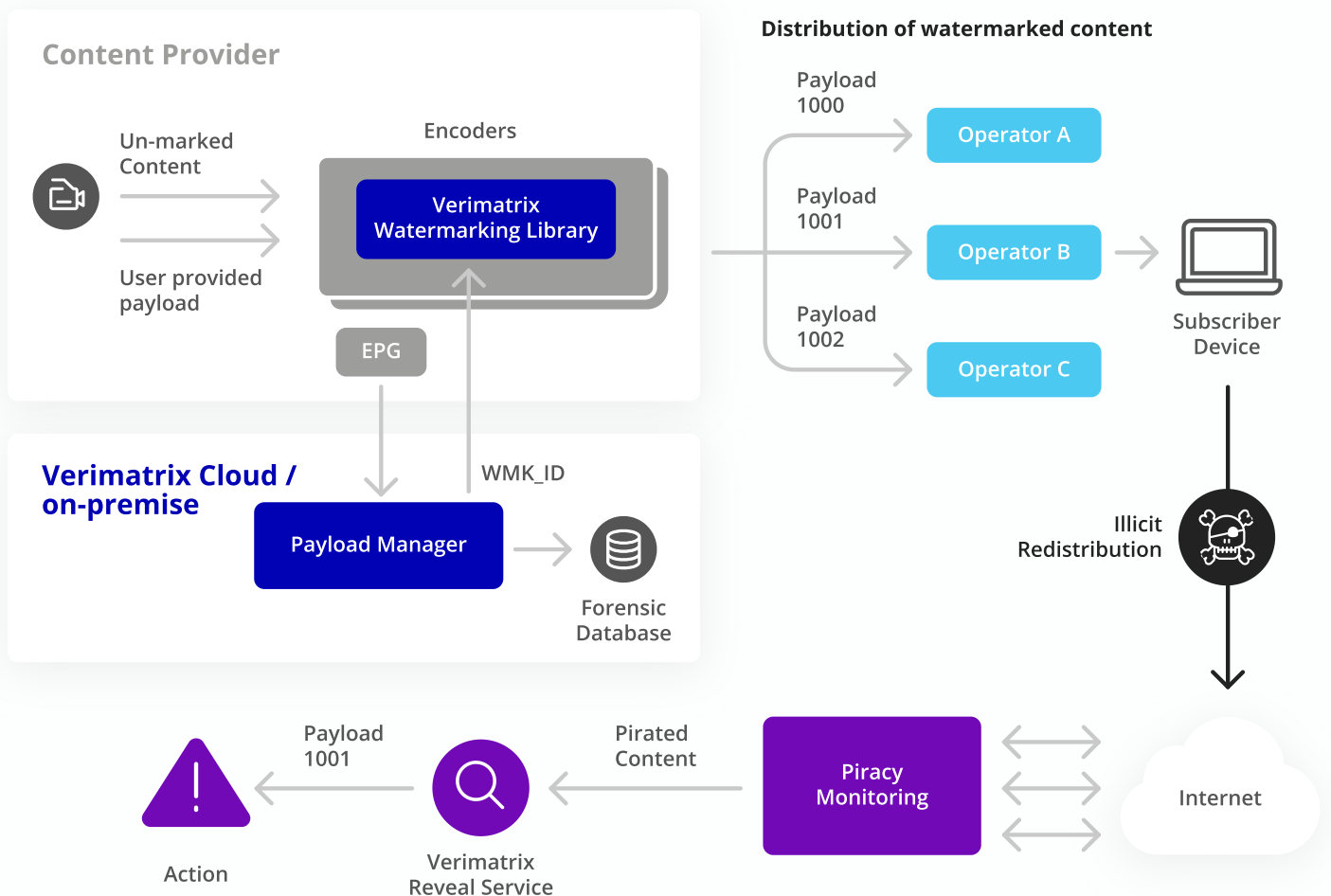
Verimatrix's suite of Application Shielding solutions are used to protect the KARA smart fitness system, which uses gamification to harness users' passion for gaming and perform more engaging and fun workouts. [Learn more.](#)

Best Practice #3: Make Watermarking Part of your Anti-Piracy Solution

Content protection and anti-piracy solutions go hand-in-hand as part of a layered security approach, especially for ultra-high value content, and when attached to a timeframe, like live sports or e-gaming competitions. Forensic watermarking helps identify the source of unauthorized streams or copies by tracing them back to the last authorized recipient. Once illegal sources are identified, they can be shut down, thus protecting key revenue streams for the service provider.

There are three main points where piracy happens in video delivery:

- **In the distribution workflow from post-production to the distributor**
- **Between the distributor and the end consumer**
- **Redirected from the end device**



Each of these use cases requires a different type of watermarking:

1. POST-PRODUCTION TO DISTRIBUTOR

Forensic watermarking is embedded by the content owner, like a movie studio, during encoding from the origin server, also called a B2B origin mark. This is primarily used for theatrical release content and can be used to trace back where a specific content version came from when content is distributed to post-production houses or distribution channels.

2. DISTRIBUTOR TO END CONSUMER



The server-side watermark is done during encoding and can be placed on the adaptive bitrate stream at the head-end for HLS and DASH content, which is required by the multi-device OTT world (iOS, Android, web and streaming device permutations). Server-side watermarking meets studio requirements for higher resolution content and is easier to implement. Plus, the watermark logic is done within the server and this makes it virtually untouchable.

This cloud-based service introduces a small amount of latency and comes with some additional costs, but it is well-suited in a low-latency requirement that live sports demands.

3. END CONSUMER



A watermark is embedded within a stream in order to identify unauthorized streams. The client-side version of this is done on the device at the video player level and requires more upfront integration work.

Watermarks can be inserted at any or all of these main points along the content supply chain – depending on your business need and where you are experiencing the most piracy. Watermarking is an essential component to anti-piracy methods because it allows service providers to identify where the leak happened, and take further identification, disconnection and/or legal actions.

Conclusion

There is an old sports saying that goes, "Go big or go home." Big can mean many things; the number of sporting events during a season, or the number of tickets sold, perhaps the amount of sports merchandise ordered or even the scalability of streaming events to accommodate millions of simultaneous viewers. One thing is for certain; sports fans will continue to consume live sporting events and esports tournaments in greater numbers now that the sports industry has expanded its tent to include so many new sectors and OTT delivery has gone mainstream.

As we like to say, piracy follows the money. Piracy has evolved as digital delivery has matured and expanded into new markets because revenue streams are growing. Protecting these revenue streams from attack is paramount to business success.

Most sports content requires digital rights management — for many, this is the type of secure delivery they know about. But it should never be the last. As new streaming services enter the market, protecting hard-won revenue in other ways is essential. Solutions like watermarking, piracy monitoring, and application shielding solutions are being deployed in greater numbers each day to safeguard the ever-growing sports and esports threat matrix.

Not yet convinced? Go forward at your own peril. Pirates will be more than happy to take advantage of security holes found in the media and entertainment ecosystem to fuel their illegal enterprises. Developing a solid and secure 360 degree delivery strategy is the only way to end the bad guy's free ride, and prevent ongoing damage to your bottom line.

About Verimatrix

Verimatrix (Euronext Paris: VMX) helps power the modern connected world with security made for people. We protect digital content, applications, and devices with intuitive, people-centered and frictionless security. Leading brands turn to Verimatrix to secure everything from premium movies and live streaming sports, to sensitive financial and healthcare data, to mission-critical mobile applications. We enable the trusted connections our customers depend on to deliver compelling content and experiences to millions of consumers around the world. Verimatrix helps partners to get to market faster, scale easily, protect valuable revenue streams, and win new business.

For more information, [visit us](#) and schedule a call with our team to see how Verimatrix can protect your sports and esports revenue streams.

