



Protecting premium live sports from streaming piracy



Protecting premium live sports from streaming piracy

Introduction

Premium sports are at the heart of the broadcast industry. The live and compelling action thrills audiences like no other entertainment. Unsurprisingly, this success has also made live sports a primary target for streaming piracy, and this has rapidly become a major threat to the revenues of legitimate broadcasters worldwide. This menace impacts the whole commercial chain from sports rights owners to broadcasters, including both traditional and OTT delivery.

To address this theft, there's a need for concerted action and an investment in end-to-end content security. The latest developments in subscriber watermarking and global channel monitoring can

virtually eliminate streaming piracy in minutes, without disrupting existing delivery workflows. This speed of response is essential with live sports since the value of the content diminishes rapidly with time, and hence it's essential to maximise the viewership during the event. Importantly, the invisible nature of the latest watermarking means that the critical premium sports viewing experience is unaffected as security is strengthened.



Shifting patterns of streaming piracy

Streaming piracy has matched the wider television market in terms of its speed of evolution. Illegal content can be consumed in a multiscreen environment, ranging from mobiles phones to big screen televisions.

There's now a huge array of viewing options, including illegal streaming devices, Kodi plugins, mobile apps, websites and social media. Many of the streaming piracy services offer a very wide range of premium sports and entertainment, often packaged to match the branding of legitimate pay TV services.

As broadband speeds to the home have increased, streaming piracy has become much more accessible to larger audiences, and the quality delivered has risen steadily.

At the moment, HD 720p is the most popular resolution for premium live sports streaming piracy as it delivers a balance of good quality streaming on large screens with minimal buffering (see *Figure 1*).



Sources of streaming piracy

Unfortunately, commercial DRM and CA systems don't fully protect content in the face of determined video pirates.

One of the most prevalent approaches impacting satellite and cable operators is stream redistribution directly from set-top boxes, using 'HDCP strippers' which are readily available. OTT content can also be captured using off-the-shelf screen recording and streaming software.

The ease of accessing these pirate technologies means it's essential to invest in security services which allow broadcasters and pay TV operators to pinpoint the sources of the illegal redistribution. This can be achieved by using advanced watermarking-based subscriber identification plus worldwide channel monitoring.

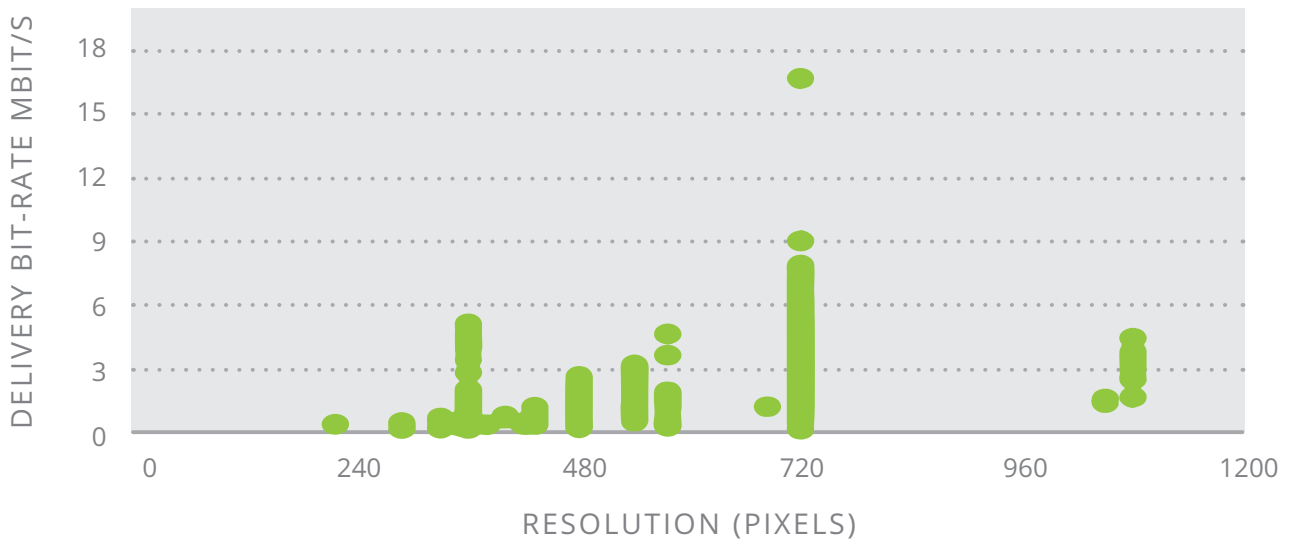


Figure 1: Stream resolutions & bitrates used for illegal redistribution of typical premium live sports



Video fingerprinting allows pirate content to be recognised in just a few seconds

Global monitoring with fingerprint-based content recognition

Highly automated security to monitor thousands of streams

Due to the scale of streaming piracy worldwide, with many thousands of streams deployed for key live sports events, it's not possible to deliver effective content protection across multiple channels without highly automated security systems.

At the heart of an effective content protection strategy is automated, 24/7 global channel monitoring to identify piracy across streaming devices, mobile apps and websites. By using video fingerprinting with the source video, illegal content can be tracked rapidly and accurately worldwide.

Speed of response

Fingerprinting is generated using video motion, and it does not modify the source. To allow rapid content matching, the video fingerprint needs to be lightweight in terms of data size. With the latest monitoring technology, a one hundred percent accurate content match can be performed in just a few seconds.

Another important factor in successful fingerprinting technology is resilience to playout processing, such as aspect ratio changes, downscaling and bit rate reduction. The integrity of the fingerprinting must also withstand the countermeasures deployed by video pirates to disrupt content protection. Additionally, the fingerprinting must work across all key video formats, including 4K, HD and SD, as well as both traditional and OTT delivery.

Network path tracing to locate pirate stream infrastructure

Once content has been identified using video fingerprinting, it can be determined quickly whether the stream is legitimate or theft.

If the content is illegal, there's a need to investigate the video stream to identify the underlying video infrastructure.

The full network path can be evaluated up the chain to determine the host within just a few milliseconds. This path analysis can give a clear picture of the scale of the threat, and how best to address it.

With the most complex streaming piracy infrastructures, this highly automated monitoring and forensic analysis can be augmented by manual investigation.

The next step in the process is to identify the point of content redistribution, and take action against the subscriber responsible for the theft.

Automated, global channel and content monitoring using video fingerprinting



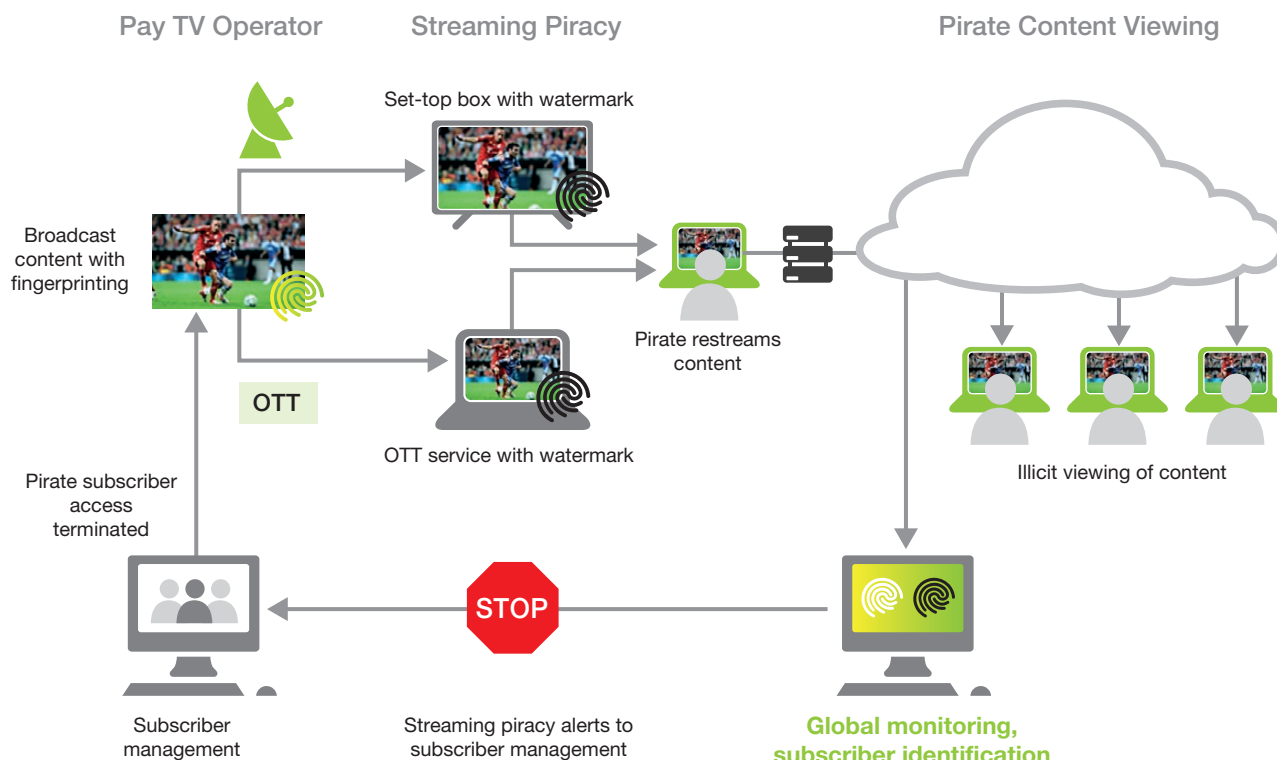
Invisible watermarking for identifying source of streaming piracy

Optimising security and viewing performance


To identify the source of the streaming piracy, the content can be automatically analysed for subscriber-level watermarking. This watermarking is inserted by set-top boxes and OTT players in order to pinpoint any leaks in the video delivery chain.

The best watermarking is completely invisible to optimise the viewing experience with premium sporting content, while also maximising the security.

The watermarking needs to be ultra-robust to any attempts to overcome the identification, such as cropping and masking. It also needs to operate across the latest technology and legacy devices, such as older set-top boxes.



End-to-end content protection workflow combining global channel monitoring with fingerprint-based content recognition plus subscriber level watermarking



Subscriber identification watermarking must meet the stringent requirements of sports rights holders to ensure a high quality viewing experience

Integration with subscriber management systems

Once the global channel monitoring has analysed the watermarking and identified the individual subscriber responsible for a pirate stream, the system can pass the details directly to the broadcaster's subscriber management system.

This high level of integration allows rapid, automated termination of the content theft in just a few minutes.

Conclusion

Premium live sports is under real pressure from streaming piracy worldwide, and this situation is unlikely to change in the near future. However, rights holders, broadcasters and pay TV operators can deploy proven, end-to-end security systems based on advanced monitoring and subscriber watermarking. These systems have been shown to deliver a huge reduction in premium sports streaming piracy, and thereby protect critical revenues for the media and entertainment industry.



Friend MTS

Protecting content + revenue

For more information about protecting premium live sports
from streaming piracy contact:

www.friendmts.com

