

FROST & SULLIVAN

# WATERMARKING SOLUTIONS:

A Content Owner's Shield from Piracy



Authors:

**Swetha R K**, *Senior Research Analyst*

**Vidya S Nath**, *Senior Research Director*



INTRODUCTION.....	3
OVER-THE-TOP AND CONVERGED VIDEO SERVICES: DRIVING NEW MEANS OF CONTENT THEFT.....	5
CONTENT PROTECTION:NEW MEANS OF SECURITY FOR VIDEO DISTRIBUTION .....	6
THE BENEFITS OF DIGITAL WATERMARKING.....	9
WATERMARKING: AT THE EDGE OF THE CONTENT DELIVERY NETWORK .....	10
CONCLUSIONS.....	13
CALL TO ACTION.....	14

# CONTENTS

# INTRODUCTION



Revenue losses due to content theft and piracy continue to plague the media and entertainment industry. Ubiquitous high speed networks, hyper-connected devices along with widespread availability of high quality video content online have made it easier for pirates to gain traffic.

For instance, in 2016 alone, over 191 billion visits<sup>1</sup> were made to piracy websites globally amounting to more than 50 visits per Internet user in just one year. In 2016, there were an astonishing 589 video websites worldwide, as against 480 legal websites, generating advertising revenues to the tune of \$208 million globally<sup>2</sup>.

With a significant proportion of the population watching their content for free, the stakeholders of the media and entertainment industry incur substantial loss in revenue. For instance, despite a 4.2%<sup>3</sup> decrease in the number of illegal accesses in 2016, the entertainment industry in Spain accrued revenue losses to the tune of €1.783 billion, 6.8% higher than in 2015.

In spite of efforts from governments across the globe to drive stringent law enforcements, piracy cannot be restrained. There were 5.4<sup>2</sup> billion downloads of pirated movies and TV shows in 2016 worldwide.

Every year, millions of dollars are spent by content owners, distributors and other media stakeholders towards anti-piracy campaigns, enforcement support, legislative initiatives, as well as protection of theatrical release of new movies. There is a stronger movement not just from governments and businesses, but also from law enforcement agencies, licensing agencies, and associations such as Motion Picture Association for America (MPAA), among many others.

More recently, 30 international companies including HBO, AMC Networks, NBC Universal, Amazon, BBC, alongside several leading Hollywood studios, SVOD services and other media firms joined hands to form the Alliance for Creativity and Entertainment (ACE) to fight piracy at a global level.

1. MUSO
2. Alliance for Creativity & Entertainment
3. La Coalicion



But, while anti-piracy regulations and advocacies can curb pirates and illegal consumer viewership, they cannot provide a foolproof shield for content protection.

Constantly evolving methods of content piracy are pushing content producers to consider content protection solutions at every point of their value chain. Traditional content protection technologies such as Conditional Access System (CAS), Digital Rights Management (DRM) and Watermarking help to not just secure the content but also track its illegal distribution.

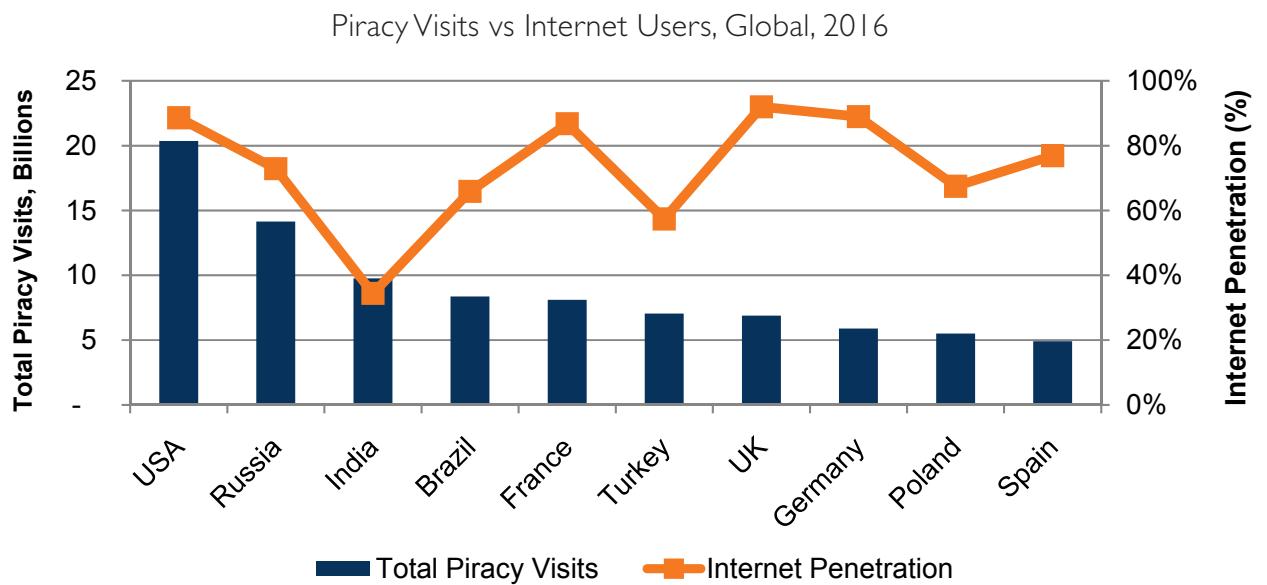
This whitepaper highlights the new-age requirements for content protection that can secure the content right from its creation, till it reaches the end consumer, and after. It also highlights the necessity for watermarking which can strengthen content ownership and rights management for a content producer in any part of the world.



# OVER-THE-TOP AND CONVERGED VIDEO SERVICES: DRIVING NEW MEANS OF CONTENT THEFT



Internet connectivity plays a major role in nurturing content theft. The United States and Europe, which have high Internet penetration rates typically have high prevalence of piracy and occupy the top 10 positions among the global 50 piracy countries<sup>1</sup>.



Over-the-top (OTT) video services, especially subscription video-on-demand (SVOD) grew over the last decade as an attractive alternative for television cord-cutters and viewers. Consumers now have access to tens of thousands of high quality television shows and movies within a few months, or days, or even

concurrent with their television broadcast or theatrical release. Just the availability of choices has driven up the viewership of legitimate content online. According to the UK Intellectual Property Office, the success of OTT services led to significant decline in piracy rates in the UK.

That being said, the rise of OTT services has also led to a slew of legally-grey options. For instance, 60% of piracy visits in 2016 were made to streaming websites<sup>1</sup>, making it the most popular mode of access for pirated content as against torrent sites. The infamous Kodi box is another example of a new avatar of piracy. Kodi boxes are set-top boxes or streaming devices that allow its users to stream

content from any apps or platforms (including subscription content) for free. These boxes are very popular; as evident by the increase in Internet searches for Kodi boxes by 143% last year.

Pirates continue to evolve in their methods, technologies and processes to hack into content, steal and distribute it.



## CONTENT PROTECTION:

### NEW MEANS OF SECURITY FOR VIDEO DISTRIBUTION

The classical definition of a content protection (CP) system is that it is used to secure the content provided by a broadcaster or a PayTV service provider to its subscribers. A CP system ensures protection of service revenues of the broadcaster as well as the content owner by restricting access of the service to only authorized or paid subscribers. But the challenges are compounded in the hybrid distribution ecosystem, where content is disseminated across platforms and geographies, across satellite and Internet networks. This requires content companies to carefully evaluate and invest in content protection across their value chain.




The increasing prevalence of post-decryption theft and pre-distribution theft hinders the

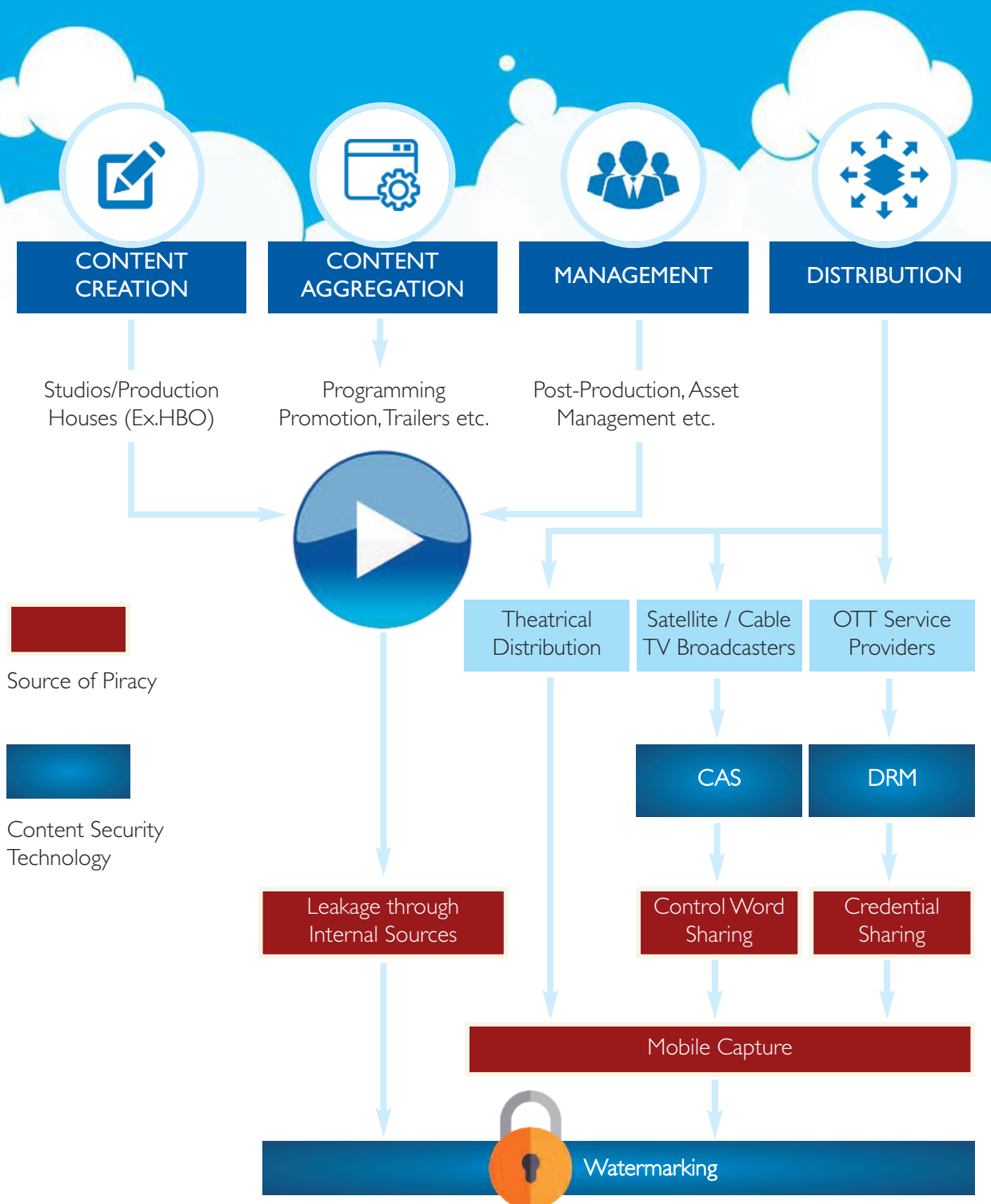
revenue growth of content owners who tend to lose their bargaining power with distributors over licensing prices when their content is available for free.

According to a survey by DigitalTV Europe and Civolution, 45.7% of the respondents considered post-decryption theft to be the major weak link in the content distribution value chain. For instance, after a movie has been screened in a theatre or on TV, mobile devices may be used by pirates to record the movie and distribute it over a DVD or through piracy websites. There is always a developing technology in place to pick up the content available over Internet or from theatres or TV STBs, thereby reducing revenues for content owners.

1. MUSO

5. Intellectual Property Office, UK

Stakeholders	Impact of piracy	What is needed	The Ideal Content Protection Solution
	<p>Inability to find the source of piracy and the illegitimate distribution channel</p>  <p>Revenue Loss Impact</p>	<p>Illegitimate content distribution harms the interests of all in the value chain- the broadcaster, content rights owners, the Pay TV or OTT video operator as well as the genuine subscribers. In a multimedia world, it's pertinent to have a system in place that helps trace the origin of theft and captures the trail through the network to clamp down on pirates.</p>	<p>Watermarking</p>
<p>Content Owners Pay TV Operators OTT Service Providers</p>	<p>Inadequate means to restrict access to content over a paid platform</p>  <p>Revenue Loss Impact</p>	<p>Encryption of content and restricted content access helps in safeguarding the interests of distributors and ensures delivery of content to the rightful subscribers.</p>	<p>CAS</p>
	 <p>Inability to protect copyright Revenue Loss Impact</p>	<p>OTT services are exploding in distribution as more and more aggregators acquire content rights from the entire value chain. Content companies as well as distributors need to secure their copyright and prevent unauthorized distribution and replication of their content.</p>	<p>DRM</p>



In such instances, using Watermarking at an earlier stage in the value chain along with other solutions such as CAS and Multi-DRM can help secure content end to end. This will ensure that the watermark added at the source will always act as a tracker inserted into the content so that the content owner can identify who has received what and where something was

potentially leaked. For instance, HBO uses watermarking effectively to monitor piracy sites that illegally release Game of Throne episodes. In another instance, HBO and Star TV India used watermarking to pin down content theft sources for the leak of an episode of the highly popular programme's latest season.



## THE BENEFITS OF DIGITAL WATERMARKING



Watermarking technologies embed visually imperceptible but robust data into protected content in order to enable persistent identification of copyrighted material and reliable tracing of the source of such material. A digital watermark is usually a sequence of ones and zeroes (bits), which hold copyright information, inserted into the image or video. Watermarking data in a well-designed system is difficult to remove despite cropping, resizing,

re-compression, conversion to analog and re-digitization, and so forth. If protected content is captured after rendering and broadly redistributed over the Internet, watermarking detection can be used to identify, diagnose, and remediate such leaks.

Watermarking has been applied for different purposes in the media & entertainment industry. Some of them are listed below.

- 1 Watermarking provides a unique identity to the content which sticks to it no matter where it gets distributed or copied. This helps in identification of content and the copyright information without interfering in the quality of service offered to the consumer.
- 2 Watermarking is an effective tool to monitor broadcasting of content such as news, live sports etc. The watermark is embedded into the content prior to transmission and extracted by the monitoring site. This ensures that the content is not available for consumers who have not subscribed to the service.
- 3 Watermarking also helps in detection of content copying. When a copy-prohibit watermark is added, the content cannot be copied by any recording device since the watermark detector will refuse access to copying of content.
- 4 Watermarking also helps in detection of any modifications made to the content and thus helps to maintain the authenticity of the content. This is particularly useful in cases where the content is recorded by mobile cameras or surveillance cameras and distributed illegally.

# WATERMARKING

## AT THE EDGE OF THE CONTENT DELIVERY NETWORK

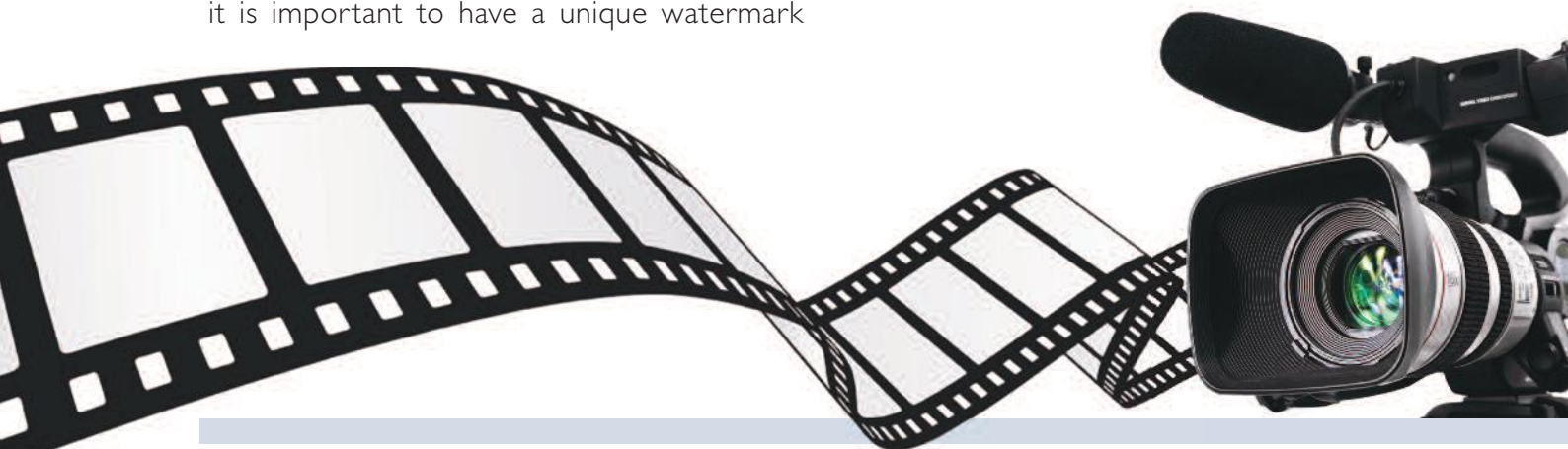


The rise in consumption of content over the Internet and smartphones has necessitated the use of adaptive bit rate streaming technologies. In adaptive streaming, the content is encoded at multiple bit rates and the entire content is segmented by different bitrate segments that are subsequently time-aligned. The information about the content resolutions, bit rates, and the rules for accessing each bitrate segment is provided in a file known as Manifest file. Typically, a DRM system is used to protect content until this stage. However, a DRM system cannot protect content from post decryption piracy.

A digital watermark added to the content in an earlier stage of the value chain enables identification of the proprietor. However, in order to identify and trace the source of leak, it is important to have a unique watermark

distributed to every individual viewer. This is particularly important in the age of OTT video services since content is distributed online using a content delivery network (CDN), which is a large distribution of servers across multiple data centers deployed globally. CDN servers ensure high network availability and performance by storing a cached copy of content at every server and streaming locally rather than across the whole network. While each cached copy has a unique watermark, all viewers receiving the content through that particular server will receive the same watermark, making it difficult to track individual viewers.

The watermarking techniques briefed below give a workaround to handling content security at the CDN edge.



## Manifest Level watermarking

Watermarking solutions for adaptive bit rate streaming at the CDN edge are typically done at the manifest level. This is done by creating two uniquely watermarked versions of a file and customizing the manifest file to mix the different versions and create a unique user specific watermark, which is then sent for distribution. Figure 4 illustrates this technique.

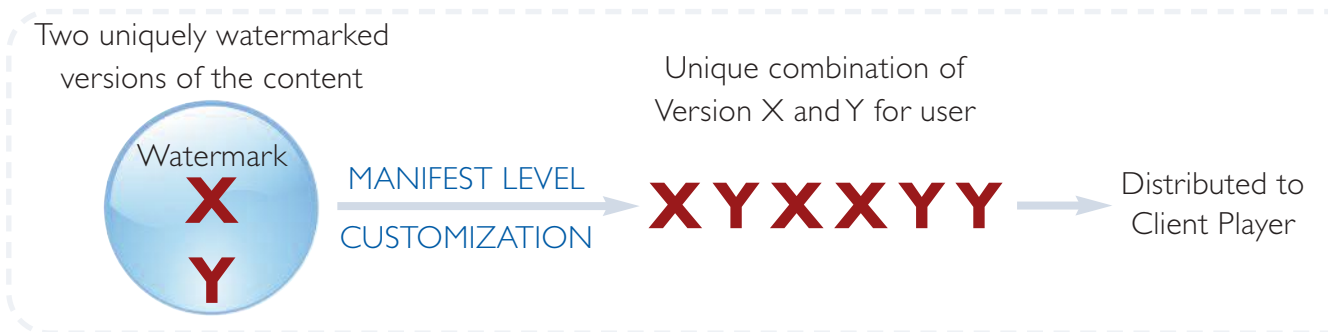


Figure 4: Manifest Level Watermarking

This approach can be cumbersome and inefficient as two versions of every video stream will require to be distributed and stored, and this process can be demanding in terms of time, storage space and resources. Especially, in the case of live streaming, where millions of users consume the content concurrently in different platforms such as smartphones, laptops, Smart TVs, etc., this approach may not be commercially feasible.

## Client Side Watermarking

In Client side watermarking, the two unique watermarked versions of the content is mixed by a client side agent to create a user specific watermark. In this case, the unique combination for each user is done by the client video player instead of at the edge server. While this method reduces the effort and time taken at the CDN side, it involves significant risk since the control of generating unique combination of content is transferred to the client device. Additionally, this method may limit the number of compatible devices that can access the watermarked content.

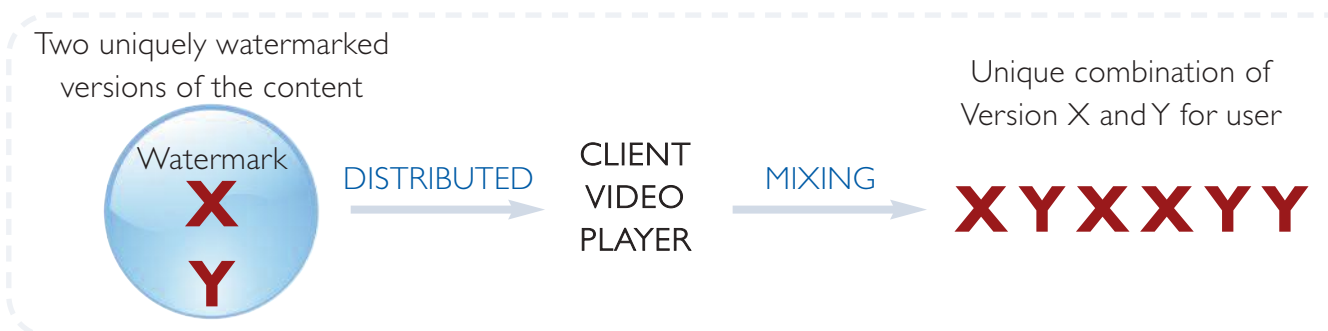


Figure 8: Client Side Watermarking

Both manifest level customization and client side watermarking techniques involve significant preparation and delivery costs, at the same time subjecting the edge server to a heavy burden of maintaining the sequences and managing different segments. Further, neither of these techniques is foolproof. They cannot prevent pirates from masking the watermark by combining it with other streams of the same video. In the case of live streaming, where the service providers may not know the number of viewers beforehand, it might take a lot of time to generate the watermarked content and identify leaks. Consequently, it is important to have a watermarking solution that is scalable, robust, practical and compatible with different platforms and delivery protocols.



## Bit-stream based Watermarking

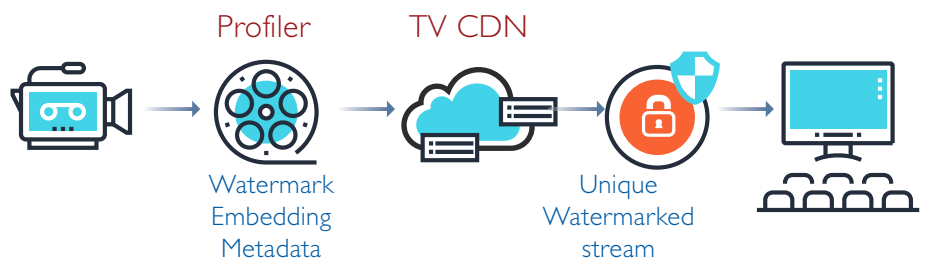
In the case of a bit-stream based watermarking system, watermark insertion is done in real time during streaming by making few byte changes to the bit stream by specialized edge servers. The process involves profiling of the frame to identify candidate blocks and manipulating them without damaging the quality of the picture. The data on which candidate blocks are manipulated and how they are altered is stored in a metadata file and sent along with the content.

This is a more efficient method since the CDN still stores and sends a single copy of content but insertion of the watermark during the adaptive bit rate streaming ensures that each viewer receives a different watermarked version of the copy. Additionally, the process is faster since the embedding is done at a rate of several bits per second. And furthermore, it is very difficult to mask the watermark once it is inserted. However, this process is dependent on the CDN's functionality and ability to manipulate the content and the metadata on the fly.

## Watermarking Solution Brief: Edgware

Edgware's TV CDN architecture supports both manifest and bit-stream based watermarking for both IPTV and OTT services, and even for 4K and VR formats. To support bit-stream based watermarking, Edgware has integrated technology from ContentArmor. ContentArmor is a specialist in providing secure and flexible forensic watermarking for premium content, and its technology is approved by major studios.

Content Armor's technology provides the profiling capability, identifying the blocks within a frame that can be manipulated to embed a watermark, and creates Watermarking Embedded Metadata (WEM). Edgware's TV CDN uses the metadata to embed a unique watermark for each stream, on-the-fly, and correlates the watermark with the viewer:



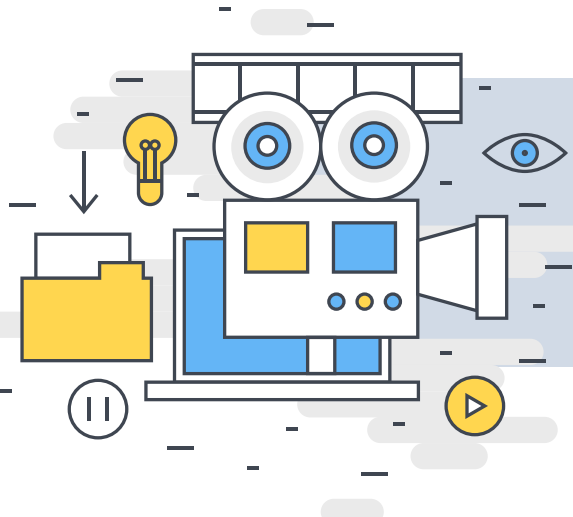
An Edgware and ContentArmor watermarking solution enables operators to pinpoint content thieves.



# CONCLUSIONS



- Growing consumption of content OTT and from multiple devices has given new challenges to the media business stakeholders to protect their content. Additionally, the advent of 4K and virtual reality content has made it even more important to secure content due to the expensive and high volume nature of the content. At the same time, the soaring volumes of content theft despite several measures to combat piracy has made content producers and distributors continually look for advanced content protection solutions.
- High prevalence of pre-distribution and post-decryption theft has necessitated the use of watermarking techniques in conjunction with the encryption based content protection solutions such as CAS and DRM. Robust watermarking techniques that use visually imperceptible images or texts help ensure copyright protection as well as enable tracing of illegal distribution. The existing watermarking technologies that support adaptive bit rate streaming such as manifest level customization and client side watermarking technologies, present challenges in terms of scalability and robustness.
- Watermarking technologies that support concurrent streaming of watermarked content to multiple screens while ensuring savings in terms of cost, time and resources is the need of the hour. Over the next few years, content protection solutions will evolve to enable watermarking at a granular level and ensure unique watermarks for every user without causing a massive overhead to the producers.



## CALL TO ACTION

If you are a content company, you will find it untenable to control the means of distributing your video. Content distribution and video consumption continues to explode across boundaries of networks, devices, platforms, aggregators and even social media. Securing one's content and following its trail through the evolving complex distribution mesh will become more and more difficult.

Frost & Sullivan has put together an essential list of questions for every content owner or distributor. If you answer 'yes' to any of the questions below, it is critical for you to consider a robust content protection solution such as watermarking.

Criteria	Question	Yes/No
Content Producers & Rights Owners	Do you produce high resolution content in HD, 4K/UHD, and HDR?	
	Is your content distributed online?	
	Is the audience for your content distributed across geographies where piracy rates are high?	
	Do you usually find your content stolen post-decryption?	
Content Distributors	Do you offer live streaming of sports or events?	
	Do you operate in regions where consumers have a lot of free options to choose from?	
	Do you offer TV Everywhere /OTT services as part of your portfolio?	
	Do you offer content that has a huge demand among viewers?	



Frost & Sullivan, the Growth Partnership Company, works in collaboration with clients to leverage visionary innovation that addresses the global challenges and related growth opportunities that will make or break today's market participants. For more than 50 years, we have been developing growth strategies for the Global 1000, emerging businesses, the public sector and the investment community. Is your organization prepared for the next profound wave of industry convergence, disruptive technologies, increasing competitive intensity, Mega Trends, breakthrough best practices, changing customer dynamics and emerging economies?

For information regarding Frost & Sullivan's coverage of Digital Media solutions and services, please write to:

[digitalmedia@frost.com](mailto:digitalmedia@frost.com)

---

[www.frost.com](http://www.frost.com)