irdeto

Building a Secure Future.™

White Paper

FORENSIC WATERMARKING IS MUCH MORE THAN JUST AN ANTI-PIRACY TOOL

This paper explores the business benefits that watermarking can bring. It reveals the hidden intelligence that content owners can unlock to shape their strategic goals and refine their operational tactics.

EXECUTIVE SUMMARY

Your content is your investment and lifeblood. Protecting the revenue it generates, when distributed directly or indirectly, is as important as negotiating the deal in the first place. With new devices and plugins making it easier for pirates to steal high quality content, there is even greater pressure on your bottom line.

For content owners, watermarking is a proven way to protect your content as part of your anti-piracy program. The invisible unique mark provides the forensic capability to track and trace, helping you identify the source of leaked content. It complements other content protection technology such as DRM, Conditional Access or BD+. But what might be surprising is that watermarking is much more than just an anti-piracy tool. Yes, uniquely marking content for tracking pirated content is the core purpose of watermarking. But it's when the watermarking technology is combined with a suite of services, including detection, enforcement and data analytics that watermarking is transformed. This combination adds more business value to an organization than solely being used to identify the source of leaked pirated content.

This paper explores the business benefits that watermarking can bring. It also reveals the hidden intelligence that content owners can unlock to shape their strategic goals and refine their operational tactics, such as distribution plans.

TABLE OF CONTENTS

THE ABCS OF WATERMARKING

There are two types of watermarks: visible and invisible. As the name suggests, a visible watermark is one that a viewer can see (a logo, for instance). We've all seen them: at the start of a movie or in the top right hand side of the screen when watching live sports. An invisible watermark is a hidden, unique mark which is embedded into the content, undetectable to the human eye (or ear, in the case of audio content). Both serve to target theft of copyright content but in different ways. A visible watermark is more about immediately identifying the owner. Whereas an invisible watermark helps identify the source of the leaked content rather than discouraging the pirate from stealing it. And it is this invisible watermarking which we are focused on in this white paper.

What's the difference between watermarking and video fingerprinting?

There can be a misperception that fingerprinting and watermarking are the same. They are not. Unlike watermarking which allows you to trace back to the source of the leak, video fingerprinting is only about content identification – validating it is the same as the original content. With video fingerprinting, a summary of a video segment is created (a snap shot) in such a way that similar videos can be compared and matched by automated systems. This means it is possible to validate if the content found on a pirate stream is the same as the legal original version. There is no added information in the digital content to identify the origin of the pirated content. Watermarking on the other hand makes a modification to the content by embedding a unique, persistent, invisible mark into the content. With watermarking, it is about source identification – tracing the source of the leaked content.

"Watermarking is an essential element of any anti-piracy program."

Watermarking is an essential element of any anti-piracy program. Its main purpose is to protect the rights of the content creators against illegal use and distribution of their copyrighted content. And although watermarking can't prevent pirates from stealing the content altogether, it does make it much easier for content owners to detect their pirated content, to identify the people involved and take action.

In other words, watermarking is a tool for enabling control. The business value comes from the actionable forensics that watermarking can provide as well as the decisions and actions taken to improve the bottom line. For instance, if your content is leaked, watermarking provides the means to identify the source of the pirated content – be it from a specific distributor or an individual account. Additionally, it provides positive, irrefutable evidence of the use of that leaked content.

By using watermarking forensics, it is easier to enforce contractual compliance and protect your revenue by having the insight to better manage your distribution network and/or operators and having intelligence for you to refine your content acquisition or release strategy.

How does it work?

Watermarking is the process of embedding unique invisible data into digital content such as an image, audio or video file. The persistent hidden mark provides unambiguous identification of the originator – the content owner, distributor or authorized user. Trillions of different unique marks can be created by using a watermarking switcher. Each individualized mark is added to different versions of the same digital content, allowing you to identify the source of the pirated content.

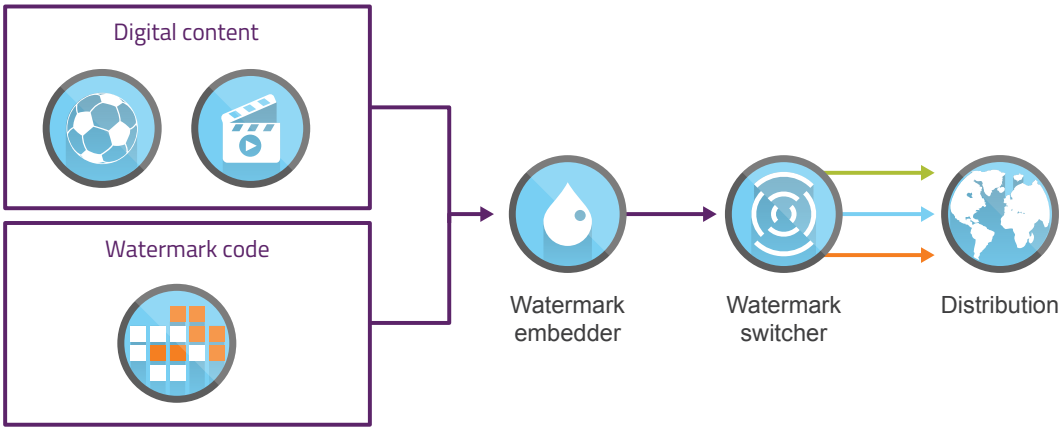

Figure 1: Simple overview of the watermarking process

Although it may seem a basic process, there are other requirements that a watermark must live up to. The imperceptible mark must not degrade the quality of the original content nor affect the viewers' user experience. It's important that the watermark can't be removed even if the content is modified, for instance cropped, encoded, transcoded or resized. And obviously extracting the hidden data must only be possible by authorized personnel with secure access to the watermark detector.

Which gives the most comprehensive protection: headend or client-based watermarking solutions?

There are two options available for implementing watermarking: headend and client-based solutions. When deciding the best option to protect valuable content, two key aspects to consider are playback device reach and renewability.

When considering reach, it is all about ensuring that your content is watermarked when it is delivered to your consumers' devices: STB, tablets, mobile, etc. With a headend watermarking solution all the content is watermarked before the signal arrives at the STB or device. Because there are no hardware or software modifications needed on client devices, there are no unprotected devices: managed or unmanaged. Even existing legacy devices are supported. All consumer devices will always receive watermarked content when using a headend solution.

"All consumer devices will always receive watermarked content when using a headend solution."

Client-based solutions, on the other hand, rely on all the client devices being able to embed a watermark securely. This means that there is hardware and software integration needed per client type and operating system version. In addition, the client devices need to stay watermark-compliant when introducing new clients on new (chip) platforms. With this additional overhead, there is a risk that your content will only be watermarked to consumers with watermarked enabled devices – but what about all the other devices?

Security and ongoing maintenance are both key considerations when it comes to renewability. A headend solution is installed within the secure environment of the provider. The solution is not that easy to tamper with. As such, it is less prone to the reverse engineering efforts of pirates. This is not the case with client-based solutions. Pirates have access to the devices and the client-based solution which can result in pirates taking advantage of the security vulnerabilities that can be exploited. For instance, client-based solutions can be susceptible to circumvention attacks either via firmware or hardware. If that version of the watermark solution is compromised, it is a difficult and costly exercise to upgrade all the clients to the latest version of the software (remember it must be done per client type and individual operating system).

This is not the case with a headend watermarking solution. In the unlikely event that a breach occurs and an upgrade is needed, this is implemented quickly, easily and cost effectively as it is deployed via the headend. What's more, with a headend solution, it is much easier to scale the solution to reach all your consumers even if there is a rapid growth in numbers.

How do you detect your watermarked content?

Embedding the watermark into your digital content is only part of the overall process. Arguably, one of the most important tasks in the fight against piracy is the identification of illegal activity and pirated content. This is crucial to revenue and copyright protection.

Integrating your watermarking to an end-to-end discovery, detection, analysis, enforcement and reporting service ensures that you're able to identify the source of any leaked content and be in a position to enforce your content rights either technically or contractually. In addition, the analysis and reporting is what will provide the basis for the business value that watermarking can unlock.

"When it comes to detection it is sensible to use an intelligence-based approach."

Discovery and detection of pirated content is done using sophisticated web crawlers to identify content, both live and video-on-demand (VOD), leveraging an up-to-date and ever growing set of distribution site profiles. For the best results, it is essential that a wide array of sites is checked, including link aggregation, live streaming and torrent sites as well as web video sites and cyberlockers.

When it comes to detection it is sensible to use an intelligence-based approach. Working with a partner who can identify which of the many sites have the highest volumes ensures that you're spending your anti-piracy budget wisely. Monitoring sites with the most traffic provides you with a greater return on your investment. In addition, having the capability to regularly assess the effectiveness and track the dynamic changing landscape, locally and globally, increases the overall service efficacy.

The other aspect to detection is automation. There are hundreds, if not thousands, of link aggregation sites out there offering your content for free, e.g., live sports. Understandably, this means that there is a lot of data out there to be collected and analyzed. Looking at each of these and validating them manually would be an impossible task without automation. A combination of an automated platform with human verification is the most ideal. This means that the service swiftly identifies infringing content. The detected streams are

analyzed and validated. Evidence is captured for inclusion in your chosen enforcement approach, for instance sending a DMCA infringement notification or working with a specific distributor to improve their anti-piracy measures.

This capability, when combined with the watermarking technology ensures the rapid detection, identification and disruption of all types of online piracy. You have both the data and tools necessary to maximize the return on any content investments.

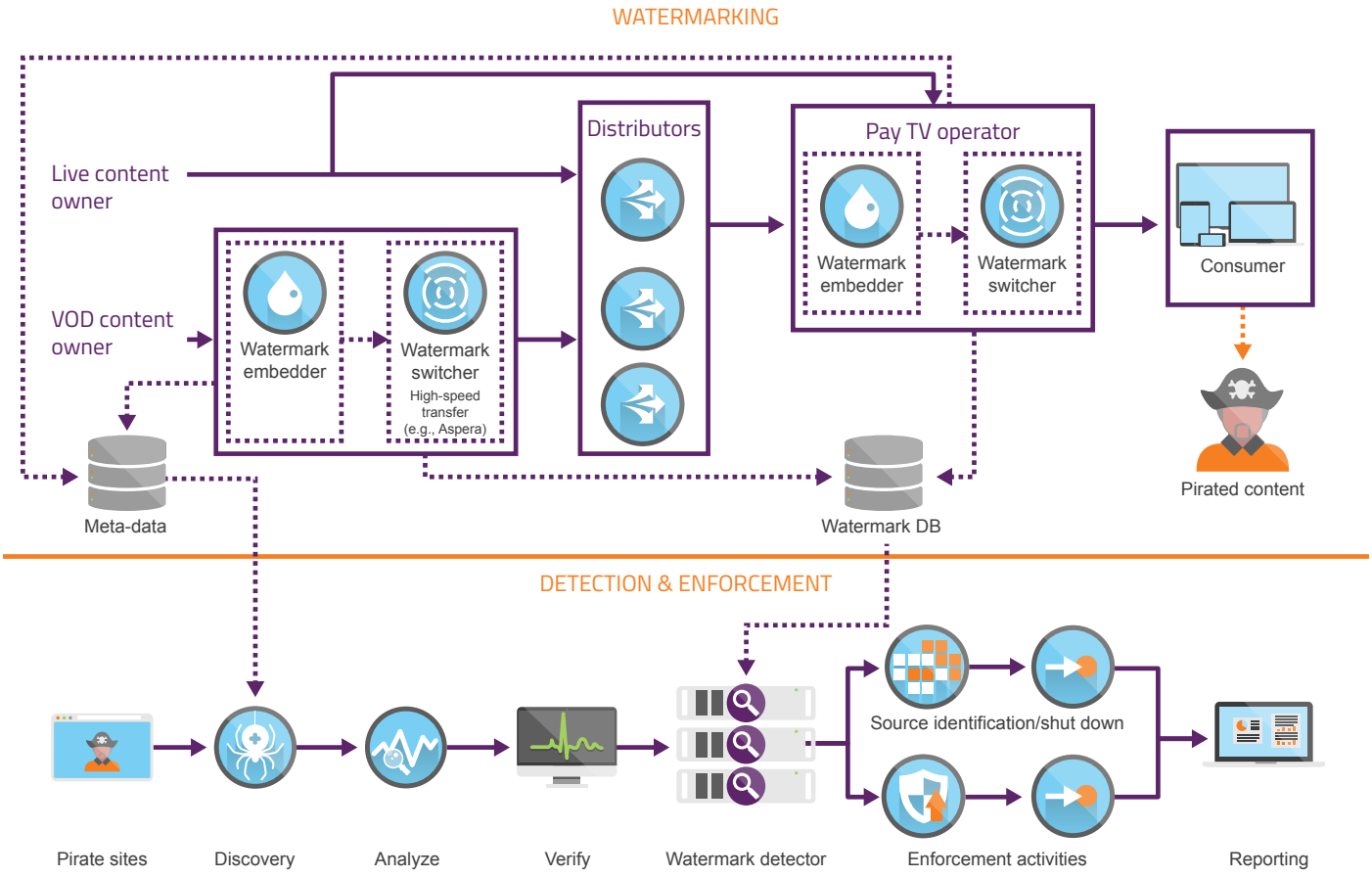

Figure 2: Integrating watermarking with piracy detection and enforcement

DIFFERENT FLAVORS OF WATERMARKING

Whether you chose to deliver your content straight to your consumers (direct) or via a distribution network (indirect), being able to use watermarking in the different situations is essential.

Direct distribution

For those content owners supplying content directly to your consumers, watermarking can be implemented for broadcast and OTT (VOD and Live).

What's important here, is being able to use a watermarking technology that enables you to identify the bad actor leaking the content by means of their OTT account or smart card details. This type of watermarking is called session-based watermarking. It allows you to trace an individual session back to the source. Once identified, you can shut down the pirating account. And importantly, only shut down that bad actor without impacting the rest of the subscribers. It is also possible, in line with your business policies that you can take follow up action against the pirate.

Figures 3 and 4 are examples of how watermarking can be implemented for broadcast and OTT scenarios:

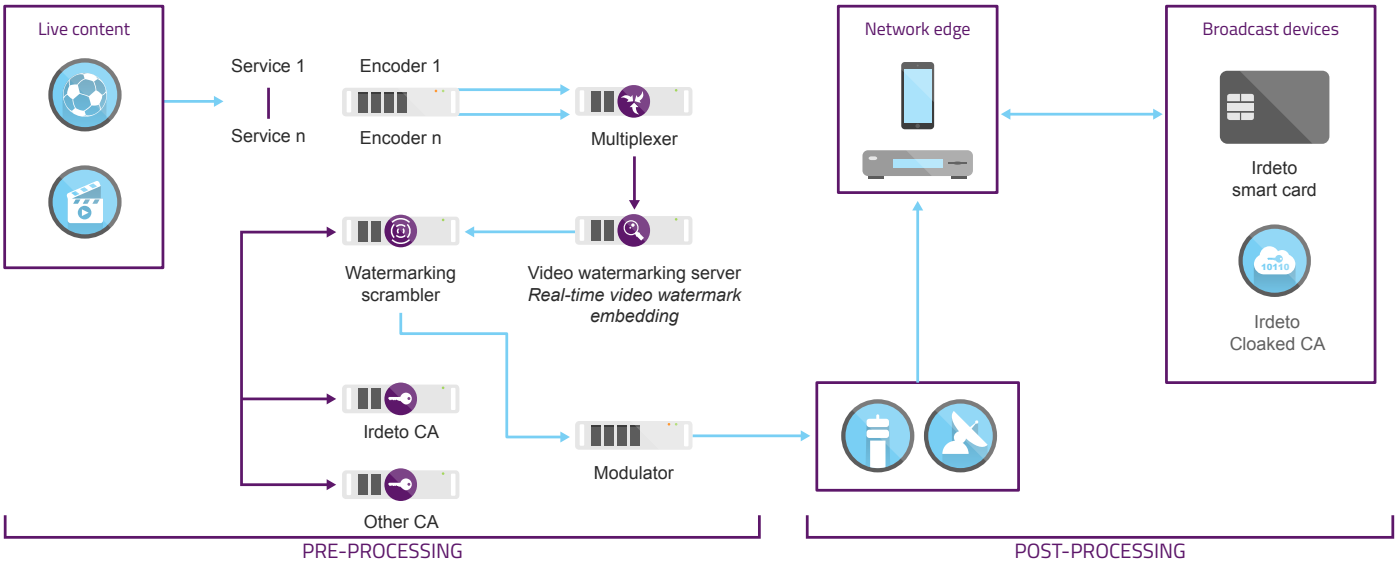

Figure 3: Watermarking in a broadband setting

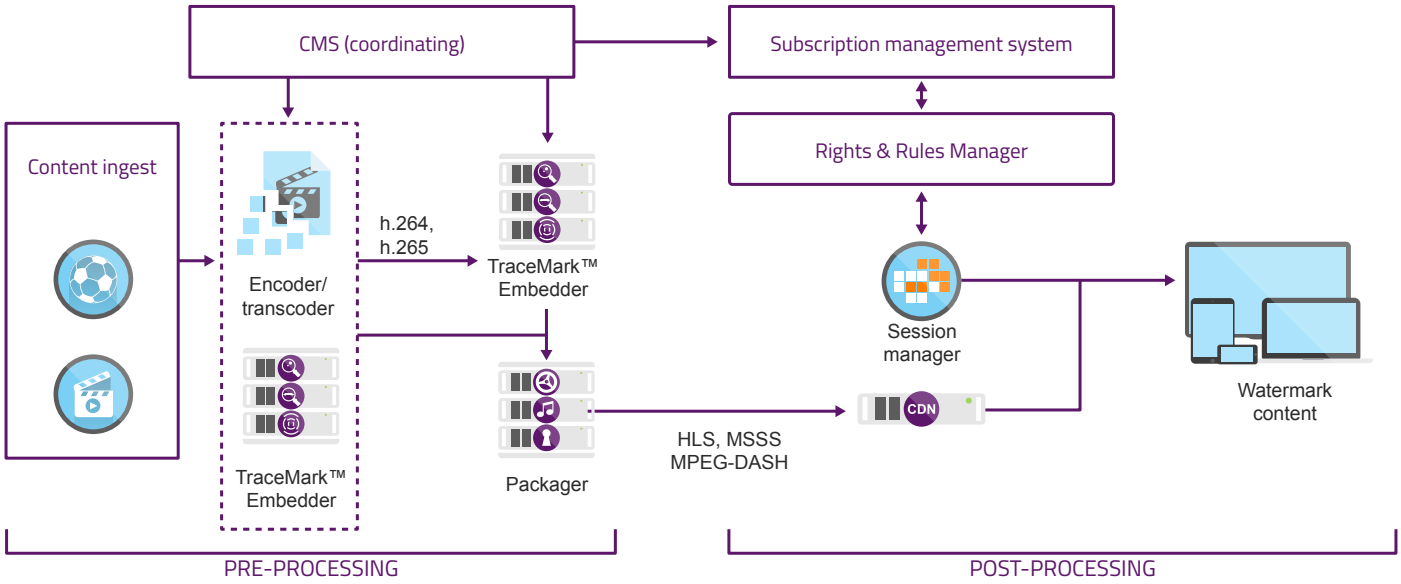

Figure 4: Watermarking in an OTT setting

Indirect distribution

For the content owner who provides their content via a distribution network (indirect), watermarking helps you identify where in your network the leak is coming from. Per individual distributor a unique, persistent, invisible watermark can be added to their individualized content. If leaked content is detected, then the individual distributor watermark will highlight where in your distribution network this has come from. This allows you to take the necessary measures to protect the value of that content. For instance, by using distributor watermarking a studio can proactively manage their distributors. Where needed, a studio can work with those parties whose security falls short of the studio's requirements by helping the distributor implement an improvement plan. By doing this, studios can extend the high value release window for their premium content, resulting in greater profit.

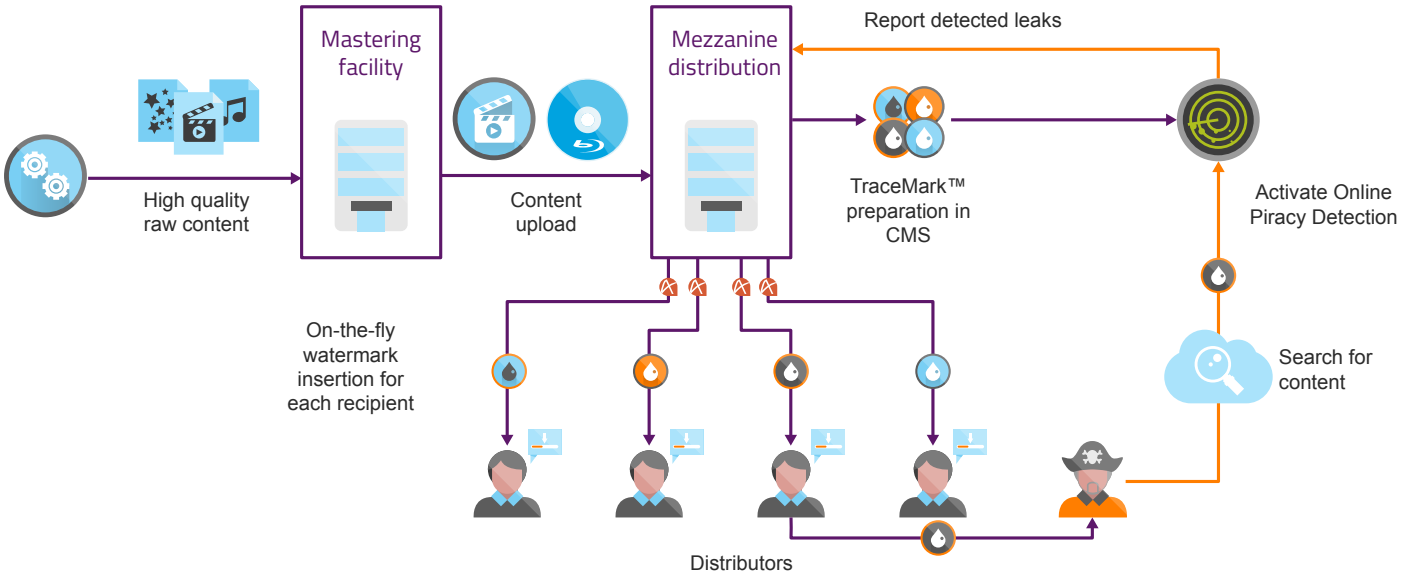

Figure 5: Distributor watermarking

It's worth highlighting that using distributor watermarking becomes easier when the solution integrates with the various high speed download services, e.g., Aspera.

Watermarking for physical content: Blu-ray discs

Watermarking technology isn't just for digital content. Physical content can also be protected. Just as with digital content, an invisible unique mark is embedded into the content feature during the authoring or BD+ application process.

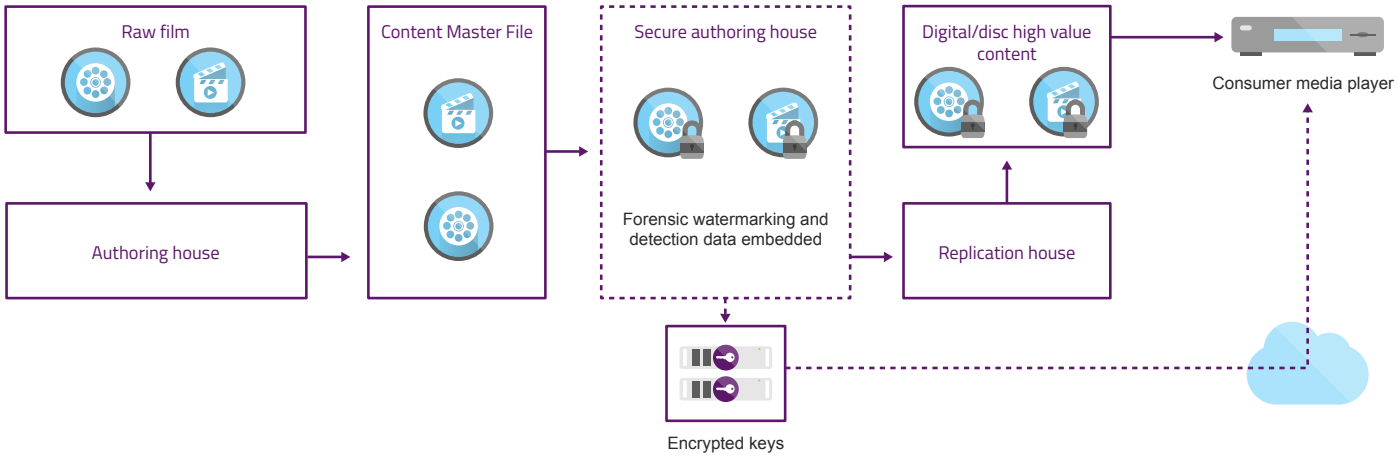

Figure 6: Physical disc watermarking

By combining watermarking on a disc with a security service such as BD+ or AACS2, content owners can see where the rip occurred – down to the individual player level in the case of UHD BD+. Previously it was only possible to identify the type of player. Any counter measures would impact any user with that machine. Combining watermarking with BD+, the actionable forensic information allows you to undertake counter measures against that individual player, without affecting the rest of the deployed machines.

UNLOCKING THE BUSINESS INTELLIGENCE

With consumers having a wider choice of content than ever before, the competition between the content owners is more pronounced. And it's not just legal competitors that you need to worry about. Pirates are the biggest threat to existing business models. They are a global competitor, who are not hindered by rules and regulations. Pirates supply content across the world and they are not concerned with regional or country specific deals.

The business value of watermarking is the forensic information it can provide. This intelligence enables you to protect your content and current revenue through enforcing contractual compliance. For instance, with live sports there is no long tail of content monetization. The value of the content is high before and during the event but diminishes once the game is over. Being able to shut down pirate accounts leaking that high value content quickly is critical. What's more, watermarking forensics can also unlock the possibility of introducing different business models to protect the overall value of your content and your bottom line.

Enforcing contractual compliance

The different flavors of watermarking ensure that content owners can use the watermarking intelligence for both indirect and direct distribution.

Distributor watermarking lets the content owner see weak links in the distribution network. Once leaked content is detected, you can work with that identified distributor to see how their anti-piracy measures can be improved and encourage them to adopt stronger security countermeasures. Protecting your content and revenue as well as their own.

For example, in Figure 7, the content owner can clearly see that remedial work is needed to improve the anti-piracy measures of Distributor 2 across 4 of the released formats.

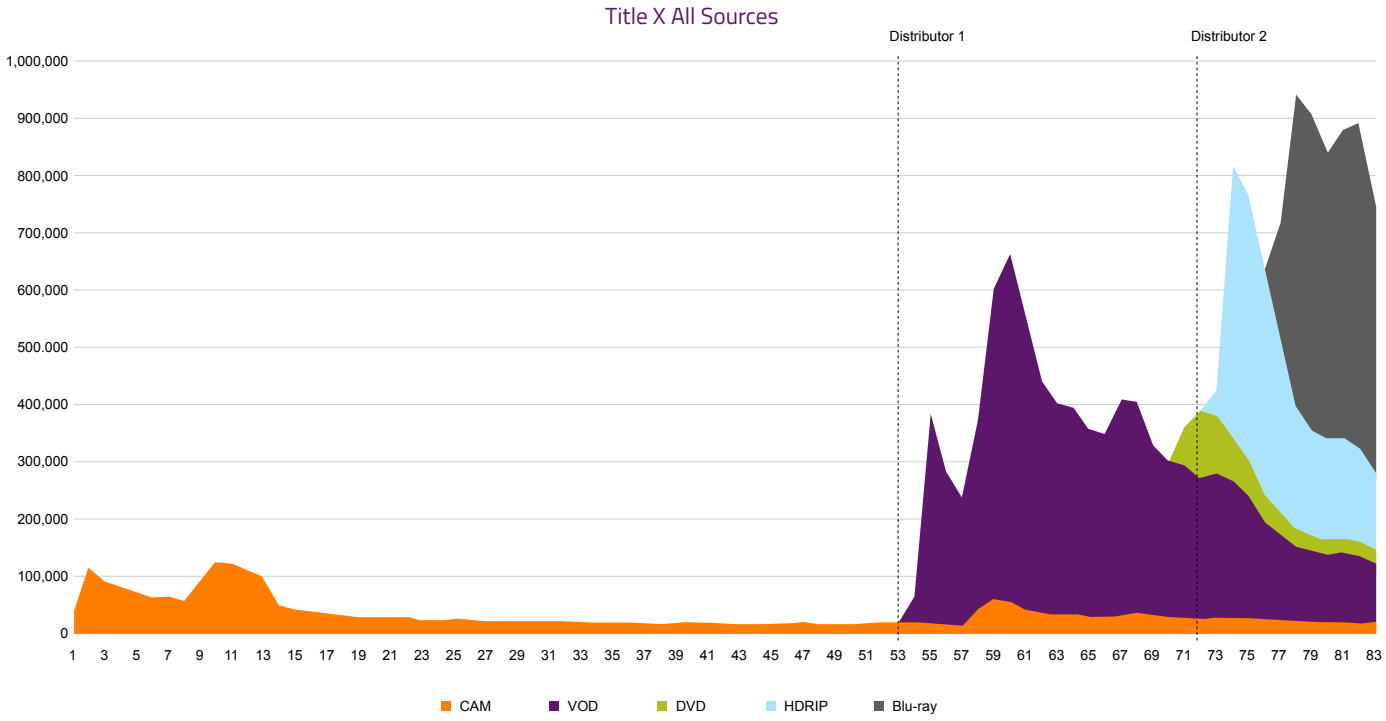

Figure 7: Distributor watermarking business intelligence

Having this level of insight ensures that you can guide and work with your distributor on specific areas of improvement. It also provides you with the intelligence that, should there be an ongoing problem, you can delay the release of premium content to that distribution channel, for instance, to protect the revenue stream. Or in the most extreme case, terminate their agreement if proactive actions are not adopted over an agreed period.

Ensuring that your distribution network is secure, means that any new deals are not undermined. For instance, you've been working for the last few months on finalizing an exclusive deal in China. Imagine, just before you sign the contract that distributor pulls out. Pirates are already supplying that so called exclusive content to consumers in the country. Why should they pay the premium rate you're asking? Revenue lost. Unfortunately, piracy is a global problem, pirates are not limited by geographic barriers and this can negatively impact your regional agreements. But having a watertight distribution network puts you in a stronger negotiation position.

For content owners going direct, session-based watermarking allows you to identify the platform or bad actors that are leaking your content. Having this insight enables you to enforce the user level clause of the contract for that specific account. Session-based watermarking is also a strong deterrent for any would-be pirates and often you will see a decrease in pirated content by making it known that a leak can be tracked back to a consumer. And it's not just consumers that this can be relevant for. Take the Oscars, for example. During the Oscars season the screeners can be watermarked before sending them to individual voting members of the Academy of Motion Pictures.

Different business models

The benefit of using watermarking intelligence is that it is accurate data. Before watermarking, content owners would need to rely on the purported sources and quality to find out the source of the pirated content – often this was inaccurate.

Now with watermarking forensics this information provides very clear intelligence: what quality resolution is the most popular along with what source format was used to propagate most of the leaked content as well as the number of copies downloaded.

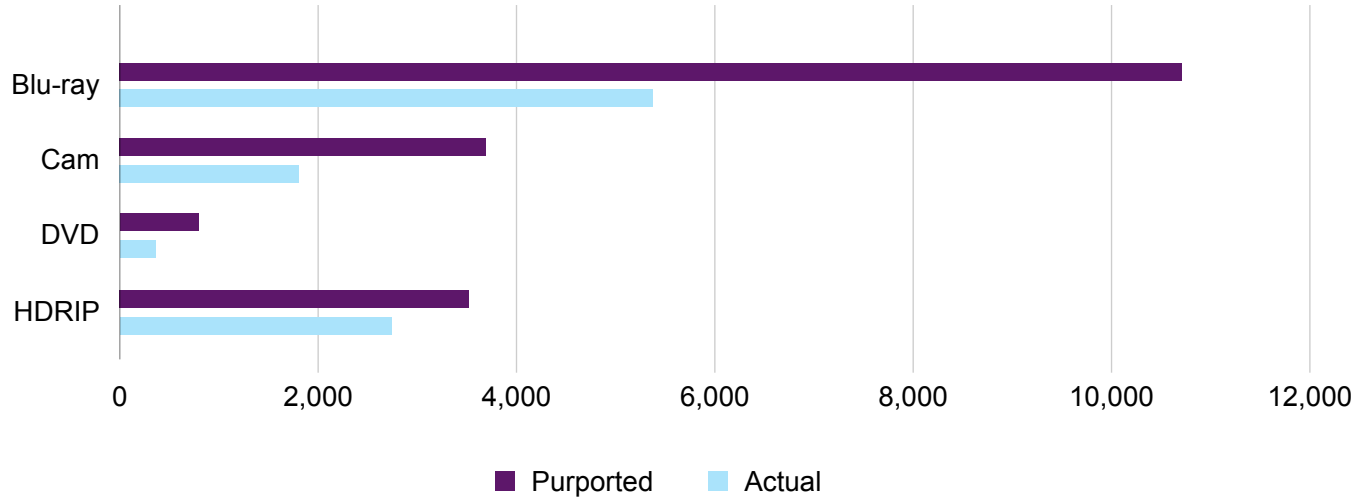

Figure 8: Purported vs. actual pirated files available for download

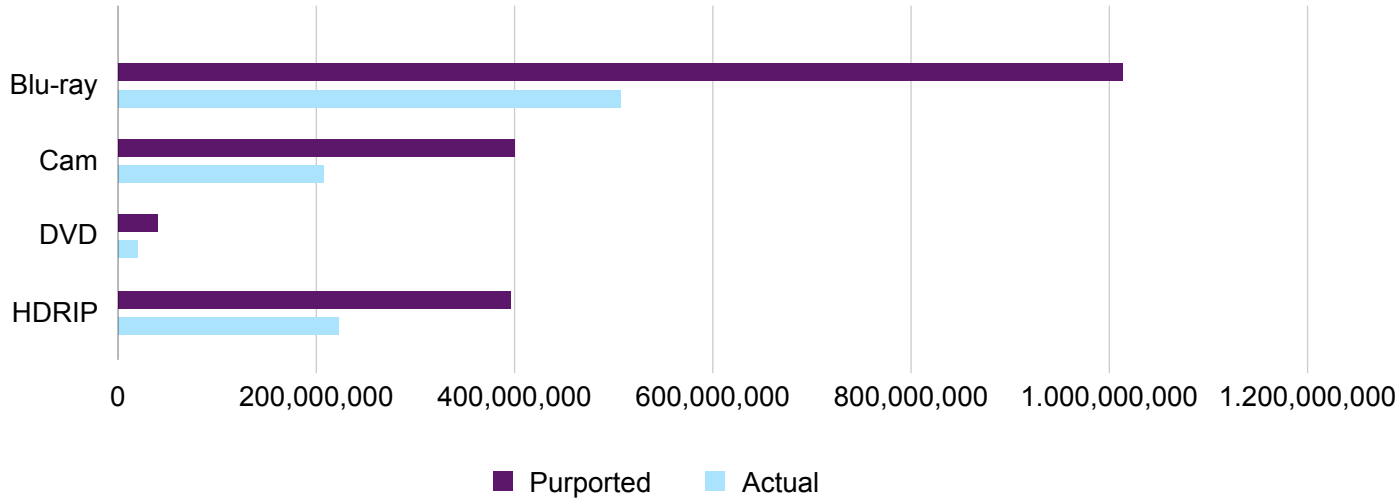

Figure 9: Purported vs. actual number of copies of pirated files downloaded

By providing a track and trace capability, watermarking provides you with the intelligence you need to act on. For instance, you could refine your distribution plans: delaying the release of content to a specific regional distributor could extend the high value Blu-ray window.

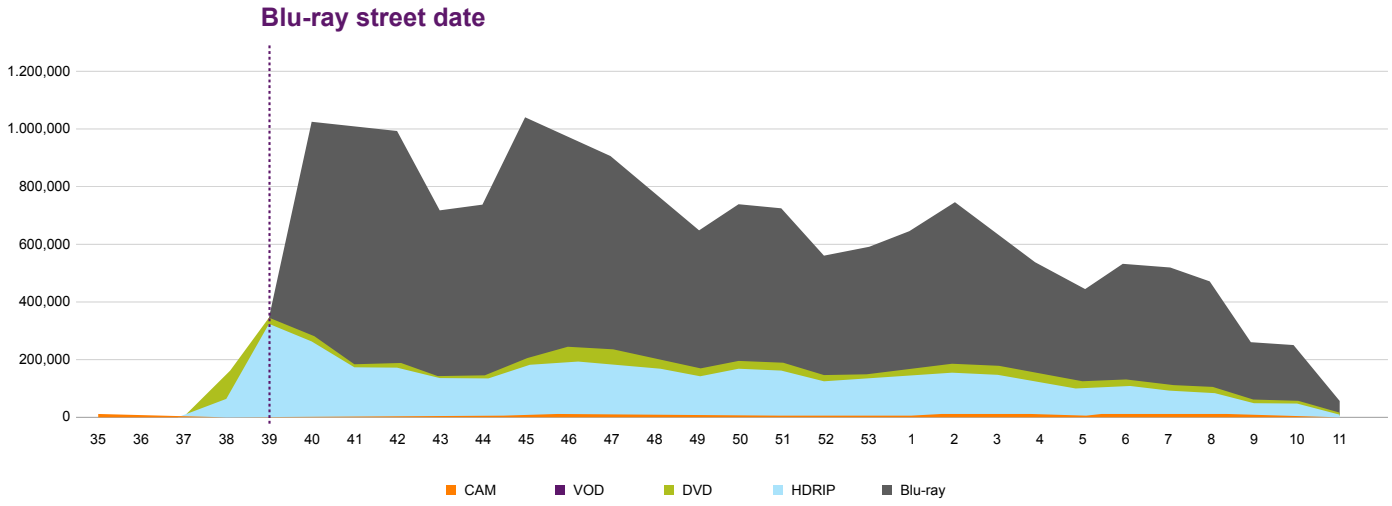

Figure 10: P2P piracy trends for a single content feature title

In Figure 10 above, the content owner can clearly see the power of combining watermarking with BD+. There were no Blu-ray rips prior to the street date.

What's more, the watermarking intelligence provides insight into the different formats and clearly shows when during the release cycle the pirate activities took place. This level of intelligence ensures that content owners can manage the business more effectively using accurate detailed and timely data. The intelligence helps you shape strategic goals as well as ensuring that day-to-day tactical decisions result in a positive outcome.

SUMMARY: MORE THAN AN ANTI-PIRACY TOOL

Forensic watermarking is more than an anti-piracy tool; it is a business tool that provides detailed analytics to help in the decision-making process. By watermarking live event and premium content you will have clear, actionable data that allows you to protect your high value content. Forensic watermarking gives you an understanding of where the leak came from and gives you the ability to take action without disrupting the ecosystem.

About Irdeto:
Irdeto 360 Security is an end-to-end, pre-integrated solution that meets even the most stringent security requirements, enabling operators and content owners to offer premium media services, such as 4K UHD VOD, live sports and early release window movies. It provides unparalleled breadth and depth to meet changing security needs, from content protection, to piracy control and cybercrime prevention, to key management by a trusted authority. Its proven success comes from the combined power of innovative technology, a diverse team of experts and a global network to deliver best security practices.

For more information about how the Irdeto Piracy Control and Cybercrime Prevention solutions can help you in the fight against online piracy, visit the website: www.irdeto.com.