BROADCAST
THE BRIDGE
Connecting IT to Broadcast

Protecting Premium Content OTT And VOD Distribution

Essential Guide

EG

ESSENTIAL GUIDES

Introduction

By Tony Orme, Editor at The Broadcast Bridge

The complexity of modern OTT and VOD distribution has increased massively in recent years. The adoption of internet streaming gives viewers unparalleled freedom to consume their favorite live and pre-recorded media when they want, where they want, and how they want. But these opportunities have also presented content owners with unfortunate challenges, typically piracy and overcoming illegal content copying.

Traditionally, it was very difficult for pirates to get hold of premium content as the high-quality video tape source material and edited masters could be physically kept under lock and key. Expensive custom electronic equipment in the way of broadcast VTR was needed to copy the video tape and few people had access to these devices making the possibility of illegal copying very difficult. It still went on but was relatively problematic to achieve and the quality of the reproductions was often very poor.

One of the challenges content owners experience in the digital world is that the quality of streamed video and audio is incredibly high meaning multiple duplications can be achieved with little loss of quality. Unlike the analog days when multiple generations of copying would quickly result in poor quality sound and vision, digital media, especially high-quality broadcast masters can be copied many times without noticeable degradation.

Source material no longer sits on a medium that can be easily tracked but instead resides in a soleless datacenter somewhere. Although storage and network security has improved massively in recent years, faceless malicious actors conspire to access media from anywhere in the world making their detection difficult, if not impossible, leaving content owners to find new and innovative mechanisms to protect their content.

All systems are only as secure as the weakest link and when the open media leaves the content owners fabulously well protected environment the possibility of unauthorized access increases significantly. Content owners must use strategies that extend their secure systems beyond the precincts of their facilities.

However, content owners see massive opportunities to monetize their media in OTT and VOD and so want unrestricted access to these viewers through the Wild West internet. Unfortunately, they also see equally massive opportunities for malicious actors who can access their content, steal it, and make it available on pirate web sites, thus forever devaluing their much sought after material.

Security is nothing new to broadcasting as television stations have been protecting high-value content since the first programs were broadcast. Access was controlled through tape libraries and source material could be tracked, and the physical size of the tape meant it was difficult to conceal. What has changed is the access now open to criminals who can download material without having to be anywhere near the locality of the broadcaster or content owner.

Tony Orme.

Protecting media is critical for content owners. Encryption and watermarking are two tools in the arsenal of the content owner, but the complexity of modern OTT and VOD distribution means maintaining high levels of protection is not as easy as it may first appear. The myriad of international affiliates and broadcasters whom they utilize to improve audience reach further draws in many new challenges that must be overcome.

Tony Orme
Editor, The Broadcast Bridge

Protecting Premium Content OTT And VOD Distribution

By Tony Orme, Editor at The Broadcast Bridge

OTT and VOD distribution over the internet has afforded content providers and viewers with unprecedented opportunities. Episodic program and movie makers are able to reach considerable audiences and viewers have more platforms than ever to consume both live and pre-recorded media. However, the internet was never designed to be secure and the multibillion-dollar content that traverses the globe must be protected.

Distribution chains from broadcasters and movie producers utilize a network of affiliate channels to take advantage of their audience reach, and this is where the challenges first start.

Not surprisingly, the content owners are protective of passing high-quality copies of their valuable content to affiliates and anybody else in the distribution chain.

Large legal documents ensue, and movie releases can easily become bogged down in tightly specified contracts, making them both difficult to sign, and even more difficult to enforce. Application of copyright law varies throughout the world and countries differ greatly in their attitudes towards enforcement.

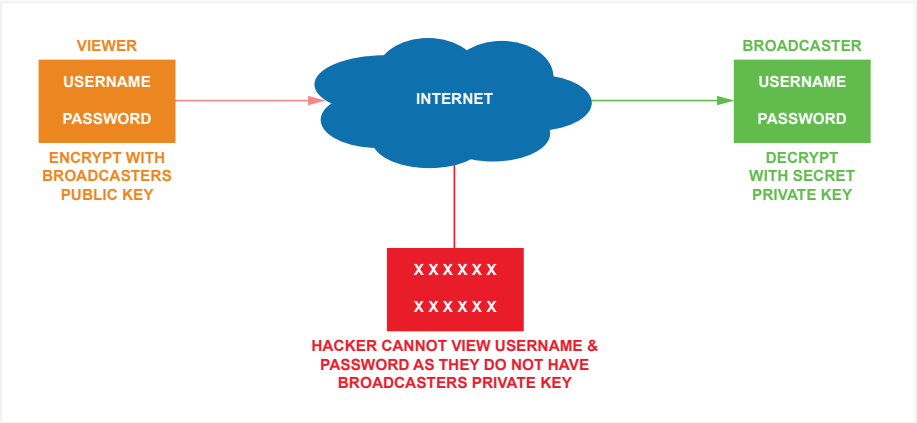


Diagram 1 – Cryptography is used to guarantee password and username protection during authentication. Anybody having access to the encrypted content will be able to receive the content, but not decrypt it or view it as they do not have the essential private key.

Maintaining Creative Intent

Another challenge is that of creative control. Media owners go to incredible efforts to maintain the look, feel and sound of their productions. Language localization may be provided with assistance from interpreters from the country in question, but the content owners will want full control over the dubbing process to maintain artistic control. Other technical constraints that impact the creative look also need to be considered such as the aspect ratio and resolution rates.

For small distributions to a handful of affiliates, maintaining these controls should be relatively straightforward. However, a high-value movie could easily be distributed to many thousands of affiliates throughout the world, rendering contractual agreement and enforcement almost impossible.

One method for dealing with this is to audit the affiliates IT security systems to make sure they are highly secure and cannot be breached. Not only does this include checking for hostile actors attacking the computer networks, but also includes verifying who has access to the media. Forensic audits are necessary to keep track of who has accessed the media, when, and where from.

Resource Consuming Audits

IT audits are a massive undertaking and their requirements are not always consistent across media publishing companies. This often leads to affiliates requiring every content owner to conduct their own specific tests resulting in thousands of hours of effort and potential disruption to their own services.

Audits are generally passive as the auditors will want to make sure correct processes are being followed and adequate records are being maintained. At some point systems need to be tested on-line. Penetration testing (pen testing) is a method of providing a scheduled and agreed check of the affiliates network by attempting to break into their systems. Everything should be fine and pen tests are now fairly common; if something goes wrong, then it can go wrong really quickly resulting in potential damage to the affiliates output. This may not necessarily be a fault with the affiliates systems but could be due to issues outside of their control such as anomalies with internet and leased line providers.

Clearly, nobody wants to enter into an IT audit unless they really need to. One audit could easily take six months to complete, that is from the time the auditor walks into the building to the time the affiliate has implemented all the requirements highlighted by the testers. This can be a real can of worms, especially if two auditors representing different media owners have contrasting interpretations of security, potentially providing the affiliate with contradictory requirements that may heavily impact their facilities.

A further challenge is that of monetizing the content by the affiliates. There are several models of charging consumers for content such as transactional viewing or monthly subscriptions, to name but two. Either way, the affiliate must know exactly who is watching the content, when and where. They will have a contract with the content owner that will specify how they are to pay for the content and this in turn requires highly accurate viewer reporting.

Under and over reporting is a key issue for both content owner and affiliate. If the affiliate under measures the media consumption by their viewers, then they run the risk of not charging the viewer adequately and losing income. More importantly, under reporting runs the risk of the affiliate not paying the content owner enough and effectively being in breach of copyright, or at the very least in breach of contract. Neither of which are very palatable.

Three Challenges

So, we have three challenges to overcome; firstly, the content owners must maintain quality standards, creative control and ownership of their media, secondly, affiliates must guarantee their systems are secure and the media will not find its way onto the internet where it can be downloaded free of charge or offered through a pirate site, and thirdly, accurate and timely viewing reporting must be maintained.

It's clear to see that there are multiple reasons why the content owner doesn't want to pass their high-quality and high-value media onto the affiliates, and why the affiliates don't want the risk and potential liability of storing the media within their systems. Although content owners can monetize their media by broadcasting directly to the viewer, working with affiliates reduces their costs and saves time.

This suggestion may have many technical challenges which can be overcome relatively easily, the real issue is that of localization, presentation and marketing. The affiliates specialize in understanding their audiences, advertising to them, and packaging programs for presentation so the viewers subscribe to the content. This is a massive challenge and not one that can be easily centralized.

All of these issues revolve around the same argument, that is, technically high-quality video and audio media is easy to copy, change, and re-distribute.

Staying Secure

Encryption has been a staple part of broadcasting for nearly 30 years. From the primitive analog systems that involved inverting line and field syncs, to the complex smart card systems that facilitate enabling of individual set-top boxes, to the rise of viewer-supplied devices and connected TV. One of the great advantages of encryption is that we can assume anybody can copy the encrypted content but cannot view it without authorization.

Encryption isn't new to the internet and has now become an established method of operation. To overcome password sniffing in TELNET connections a secure system was developed back in 1995. Later known as SSH, this is a cryptographic network protocol that stops any malicious parties from viewing data by sniffing and copying content between a user terminal and its associated server. This cryptographic method has stood the test of time and similar methods have found their way into modern HLS video streaming and HTTPS web site access.

The fundamental assumption is that anybody can see the data and copy it, however, the data is meaningless as it is encrypted and cannot be de-crypted as keys are needed to provide the necessary authentication.

Public key cryptography requires two keys; the public key, and the private key. The owner of the data creates the key pair, stores the private key and makes the public key readily available to other users. Anybody with the public key can encrypt their data, but only the holder of the private key can decrypt it. Therefore, the security of the system relies on the private key being kept secret.

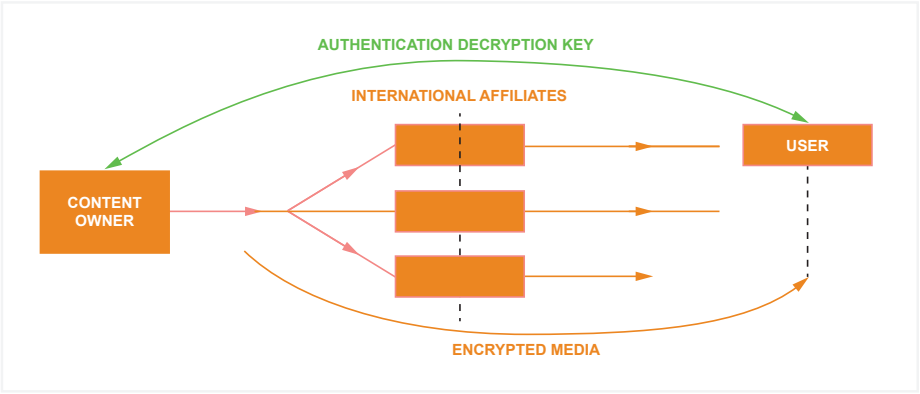


Diagram 2 – Media is encrypted before it leaves the content owner and users liaise directly with the content owner during authentication. This greatly reduces the risk for content owners and affiliates while giving the viewer a consistent and high quality of experience

This is useful if the broadcaster wants to validate the authenticity of the viewer when using insecure transport mechanisms such as the internet. When a viewer attempts to access the broadcaster's content it uses a well-known public key issued by the broadcaster to encrypt their logon credentials, such as username and password. Only the broadcaster can decrypt the message as they have the private key. If a malicious actor intercepts the message containing the viewers credentials, then they won't be able to view them. This gives the broadcaster a very high level of certainty that the user is who they say they are.

Maintaining Personal Security

There are some caveats here; firstly, it is assumed that the viewer has not allowed their username and password to be given to somebody else, and secondly, it is assumed that the broadcaster's private key is secure and has not been compromised in any way.

As part of this exchange, the viewer has their own private key independent of the broadcaster's key-pair and freely issues the corresponding public key. The viewer will often be oblivious to this process as it is an integral part of the security software running on their device. The broadcaster uses the viewers public key to encrypt messages back to the viewer. Again, as the viewer is the only person with their private key, only their device can decrypt the message from the broadcaster.

When the broadcaster is sure the viewer is who they say they are, a token is then issued to the viewers device to prove they have the right to view the specific content. The viewers device then presents this token to the license service when requesting the playback license. The license service then verifies the token's validity and issues a decryption key together with the playback policy for the content.

As hinted at earlier, the major flaw with this design is the security of the private keys held by the broadcasters. They have a massive responsibility to keep the private keys from being exposed or even being misused by disgruntled employees or anybody else.

Delivering Equitable Benefits

But there is an even better solution that provides a win-win for content owner, affiliate, and viewer. That is, the content owner both encrypts the content at source and manages the viewer authentication.

Giving content owners the power to encrypt their content at source removes much of the risk in the distribution chain. The content is encrypted before it is delivered to the affiliate and with the right design of playout system or streaming service, there is no need for them to decrypt it. It's possible they may want to view the content for compliance, but this can be achieved with the same method used for the viewers. This method solves a whole load of problems very quickly.

Assuming the content owner now encrypts the content then the viewer will have to contact them directly to receive their decryption license. This can be achieved using the private-public key system and when authenticated the content owner can issue the playback license to enable decryption of the content directly to the viewer. Again, all of this interaction is achieved without the viewers knowledge and provides them with a seamless quality of experience, or QoE. The main difference now is that the content owner is uniquely responsible for the protection of their content, thus providing them with greater control and security.

Encrypting content is a relatively straight forward task and can be automated with very little human intervention, and different encryption keys can be generated for geographical regions and timescales. Furthermore, the content owner knows exactly who is watching their content so they can provide much higher reporting accuracy so charging to affiliates can be better detailed.

Higher Level Visibility

Having this level of viewer visibility helps content owners spot any anomalies in viewing patterns allowing them to identify malicious activity earlier. Because they have global visibility instead of only the more dispersed data available to affiliates, any potentially fraudulent use such as sharing of login credentials can be easily detected.

Another level of security that is better applied centrally is that of watermarking. It can be enforced at a regional level so that any attempts at piracy can be chased through the supply chain. Pirates have many options to steal content these days including recording high-resolution copies on good quality cameras, but the illegal copies will still have undetectable watermarks embedded in the content that can be easily identified by the watermark vendor.

Not only is modern undetectable watermarking applied to the raw video, it can also be applied to the transport stream and encrypted media. This makes watermarking and encryption possible in one pass and reduces the overhead for multiregional delivery.

In the midst of all this, the affiliate is still broadcasting and delivering the media but does not get involved with the encryption process or viewer reporting. Ultimately, the affiliates may need only the smallest of IT audit, if any at all. As the content owner starts with the premise that the encrypted media can be copied but not viewed or changed, the centralization of encryption, viewer authentication and reporting virtually removes responsibility from the affiliate.

API Integration

From the viewers perspective, their authentication is happening in the backend of their viewing app giving them a consistent viewing experience. The affiliate will need to integrate their viewing software into the content owners' systems, but well-engineered APIs can make this relatively straight forward.

APIs provide a convenient gateway for the affiliates to be able to exchange information, such as reporting statistics and even QoE measure (quality of experience) to help them build a consistent and reliable business model without the increased risk of the system being compromised with the associated liability. It's bad enough having a security breach in a network, but then finding you're liable for the leaking of multiple high-value movies would be unbearable.

Furthermore, APIs speed up the integration process as the same interfaces will be used by multiple affiliates meaning they are consistent and well-supported. Content owners or their security partners can build monitoring systems into their API gateways to detect security anomalies and further improve detection. For the affiliates this is a fantastic opportunity as they only need to focus on the software integration to facilitate their business model, and not be too concerned about the security of the media.

Maintaining High Technical Quality

From a quality point of view, the content owners increase their control over the quality of the media. Multiple bit rate delivery systems such as DASH and HLS rely on generating many versions of the media with increasing bit rates. Although this implies smaller frame sizes, varying the bit rate has the potential to reduce the video and audio quality to the detriment of the content owner and the viewing experience. Using the centralized encryption model, the content owners use their own compression systems to optimize their content and deliver the multiple bit rates to the affiliate. Again, this removes more responsibility from the affiliate and further reduces their risk as well as maintaining high technical standards.

Protecting highly valuable media assets is critical for content owners and sending their media into the Wild West of the internet is a great concern for them. Using centralized encryption, authentication, and watermarking helps content owners, affiliates and viewers equally. This is truly a win-win outcome for everybody.

The Sponsors Perspective

Protecting Content Is A Never-Ending Battle

By Nikolai Keychenko, Senior Director of Product Management at Verimatrix

For content providers (studios, content owners, content aggregators, or other content licensors) and their licensees (affiliates) operating in a multiplatform world - and pirates looking to obtain illegal access to the most popular content - it's an unrelenting game of cat and mouse. While the internet has provided a cost-effective and easy way to deliver content to consumers, it also opens up new vulnerabilities that content pirates are eager to expose.

Piracy has become more sophisticated and it naturally changes constantly. Hackers and pirates continue to attempt new ways to attack different links in the supply chain. New threats are identified every few months.

In 2019 alone, digital piracy cost the U.S. film and TV industry at least an estimated $29.2 billion and as much as $71 billion, according to a study from the U.S. Chamber of Commerce's Global Innovation Policy Center.

Staying One Step Ahead

Security specialists are able to stay ahead of commercial piracy most of the time, but the war is never over. There are always numerous battles to fight, yet there is never a winner who can claim complete victory. Fighting piracy means constantly coming up with new ways to counter attacks, and a moving target is harder to hit.

Even the term "digital security," which has been redefined multiple times since the dawn of the digital age, carries new meaning these days. Today it implies not only implementing software-based security technology (encryption or authentication) and the algorithms themselves, but also how security processes and procedures around content protection work. It also means that different authentication elements are now added to the pure encryption methods, to create various types of multi-layered protection systems. This makes them harder for pirates to exploit.

For Verimatrix and its customers, the very process of how digital security is implemented and managed between the source and the recipient has been extended across the entire content delivery chain. Using state-of-the-art technology with cloud-based edge computing, the company is now automating that entire end-to-end process with security infrastructures that can be managed remotely and effectively.

Optimizing Standards In Secrecy

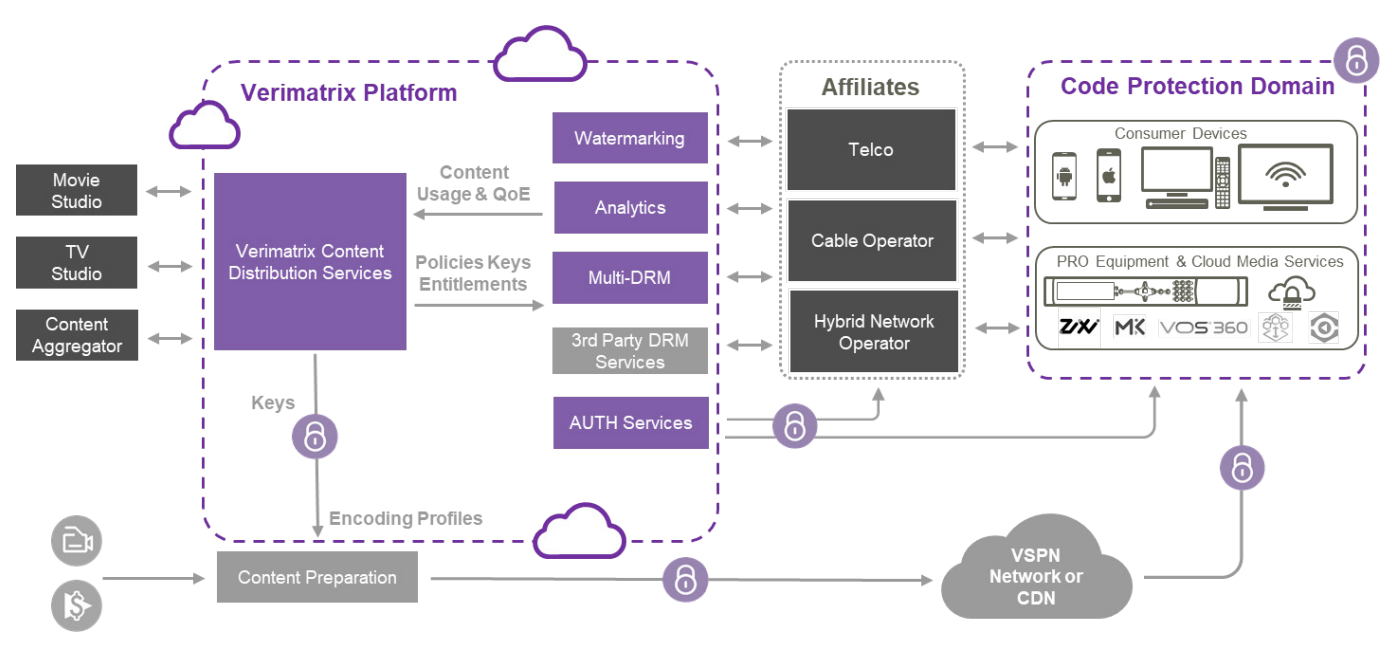
The cloud-based Verimatrix Content Monetizer solution is based on various industry standards and goes a step further to include redundant signal paths, effective authentication methods, and safeguarded workflows to prevent piracy.

There is always a place for implementing proprietary solutions to prioritize security. At the end of the day, a sound, cost-effective security system enables content providers to gain a leg up in today's highly competitive OTT environment. Standards define a general framework of how to implement security, but there is a need for specific implementation based on the user's requirements and value of the content, which is the task ideally suited for security providers. And those implementations have to be kept secret from the outside world, for obvious reasons.

Protecting Content Increases Monetization

Content Monetizer can be used for delivering content through an affiliate (telcos, cable operators, broadcasters, or hybrid network operators) or it can be employed for a direct-to-consumer (D2C) OTT delivery model. For a wide range of customers, the system provides a high level of trust and confidence.

It includes tools for translating licensing terms defined by content providers — to the rights an affiliate is entitled to and when they can offer that content to viewers (often called a "release window"). As content is ingested and processed, metadata is added to each piece of content. This metadata typically includes security and entitlement policies including a content key for decryption at the receive site, EPG data and information about the content licensor, and where it can be consumed.



Verimatrix Content Monetizer reimagines the existing model of content distribution through cloud-based workflows that provide "always-on' transparency, reporting accountability and revenue protection.

Supported by

verimatrix
DRIVING TRUST

The content provider assigns all of these attributes to a specific affiliate — each affiliate can have different rules and entitlements as described in its content license agreement — or it can assign the same rules to a group of affiliates. They can also be assigned to a single linear program, on-demand title, or a collection of those within an OTT service from companies like Apple TV, Amazon, Disney+, Hulu, and Netflix among others.

Content Monetizer also supports multiple availability zones and offers reliable region redundancy. The solution is built to automatically propagate all of the data across all of the regions where a media company's operations are supported. If one zone goes down, it automatically switches to a second signal path. Therefore, the subscriber is always assured availability of the service. Subscriber data has shown that if the quality of the experience (QoE) is high, the consumer will order more services and stay loyal.

Managing Security Across The Entire Chain

Once the system is configured, it generates entitlements for each piece of content. Each affiliate is authenticated when logging in and can access content automatically from a continually updated list of "avails."

The affiliate retrieves the content using the metadata they receive and passes on that access to the viewer. The viewer then accesses the content using a special authorization (software) token that gives access rights during a defined period of time. This token is issued for each piece of content and the device (or user) and used to track how the content is consumed. When the viewer requests playback of the content, it is automatically routed to an authentication end-point to get the playback license for this piece of content.

This is how affiliates manage the access of each specific device. The same workflow is employed for D2C services. And this all happens in real time or in advance as pre-authorization (for live events as an example).

DRM Strengthens Monetization

For those looking to monetize their assets while keeping content secure (and who isn't?), digital rights management (DRM) technology is applied by Verimatrix all along the way, from the content provider to the consumer's display device. All industry-standard DRMs are pre-integrated. Third-party multi-DRM solutions can be easily plugged-in and proprietary DRM services from traditional CA vendors can also be applied if a service provider has an existing security platform in place.

The ability to embed watermarking in every piece of content is key to not only deter piracy, but also to maximize monetization. The content can be marked for whichever affiliate is using a specific piece of content or it can be marked for the end user. This allows the content provider to trace distribution of each piece of content and to track piracy and leakage to the source.

During content processing, Verimatrix applies security tags as the content leaves the provider's facility (typically a cloud-based library) and it remains protected all the way to the DRM edges. This can be done on multiple levels to counter system attacks.

Verimatrix offers each customer a dashboard with real-time view behavior and QoE analysis tools to oversee the content lifecycle. This real-time usage data is essential to:

- Automate royalty reporting
- Accelerate revenue recognition
- Allow marketers to determine what content is most popular
- Help better decision making regarding infrastructure and business models

Among the most successful scenarios is one where the content goes from the software player to the hardware processing engine, where it is decrypted, decoded and rendered on the user's display screen using HDMI's High-bandwidth Digital Content Protection (HDCP) protocol. In this scenario, content never leaves the protected environment until it is displayed on the viewer's screen. Even then, if someone tried to illegally record the content with a video camera pointed at the screen, a watermark is embedded in the picture. Content providers can extract this watermark from the illegal recording and use it as forensic evidence in court proceedings against offending pirates.

The Battle Wages On

So, as the battle against content piracy wages on, new technologies will be refined and able to be deployed within minutes if required. When a security breach occurs, time is of the essence and must be addressed immediately.

There will always be points of potential failure in any content security system, and that's why Verimatrix has deployed its system in the cloud—to ensure high redundancy and high availability.

Protecting content is more important than ever in today's digitally connected world. With a SaaS model designed to ensure fast and secure on-boarding of content, full analytical monitoring, and 24/7 uptime, Verimatrix remains highly focused on providing rock-solid protection and high availability for any piece of content—no matter where it originally resides.

With content safeguards that travel with the asset, enforcement of license terms and a reliable and intuitive way of affiliate reporting, content providers have a great chance fighting against piracy.

BROADCAST
THE BRIDGE
Connecting IT to Broadcast

CI
CORE INSIGHTS

EG
ESSENTIAL GUIDES


MEDIA


ARTICLES

For hundreds more high quality original articles and Essential Guides like this please visit:

thebroadcastbridge.com

11/2020

Supported by

verimatrix
DRIVING TRUST