RESOLVING COMPLEXITIES IN CONTENT LICENSING AND PROTECTION

Streamlined Approach to Deal Making Encompasses Solutions for Meeting Enhanced Protection Mandate
INTRODUCTION

Nothing better illustrates the premium video market’s need for the Verimatrix Viewthority connected content distribution platform than the costly, time-consuming processes content providers and their affiliates endure when transacting, communicating and enforcing licensing terms for premium video distribution.
As explained in Part One, the platform-as-a-service (PaaS) Viewthority workflow facilitates access to the combined benefits of Verimatrix content rights management and analytics solutions in engagements between content providers and video service operators. Leveraging the market-wide embrace of cloud technology, Viewthority also creates an environment for integration with other cloud services that automates interactions, strips away wasteful processing redundancies and facilitates monetization across a broad range of activities.

We then turn to an in-depth explanation of how the Viewthority cloud workflow supporting the Video Content Authority System (VCAS), RightsConnex, watermarking and other elements of the Verimatrix security portfolio allows content providers and operators to replace manually intensive, redundant security processes with a far more efficient, automated approach to rights management and distribution.

As the discussions here and in the ensuing Part Three exploration of the Verspective Analytics platform make clear, a cloud-based workflow that brings to bear all the mechanisms essential to rectifying the dysfunctions in rights management also establishes a function-rich foundation for meeting other challenges. This is why Viewthority, running as a PaaS on the Amazon Web Services (AWS) infrastructure, is well positioned to be the cloud hub for an expanding realm of collaborations on cost-saving and revenue-driving processes across the global media and entertainment ecosystem.
THE INEFFICIENT STATE OF AFFAIRS IN LICENSING AND RIGHTS MANAGEMENT

The fact that there is so much room for improvement in how premium video content is licensed and protected reflects how little time content providers and operators have had to react to the disruptions that have made the internet a primary distribution platform for their services. A new generation of OTT-optimized premium content security solutions has been instrumental to enabling this market transformation, but content providers and operators have had limited options to move beyond the old ways of doing things when it comes to negotiating contracts and managing all the steps from encryption to reporting that go into protecting content.

This is no longer the case. Capitalizing on pervasive use of cloud technology across the media and entertainment ecosystem, Verimatrix has been able to position Viewthority as a workflow for more advantageous, cooperative utilization of the multiple cloud-friendly content security and analytics solutions the company has been providing for many years.
The Impediments to Efficiency in Deal Making

The problems addressed by Viewthority start at the point of initial engagement between content providers and operators. As things stand now, the following conditions persist across much of the ecosystem:

**TOO MANY ACCESS POINTS**
Content titles and linear channel availabilities are exposed in locations specific to each content provider, sometimes in their own private B2B websites, sometimes in third-party locations where content is pooled for multiple providers. This makes it hard for operators to gain a full view of the options available for assembling service packages suited to any given location. And it reduces the exposure content providers need to ensure maximum reach for their assets.

**DIVERSE FORMATS**
Cataloging and exposure of content is further complicated by the need to convey whether assets are available for 4K UHD as well as HD delivery, and, if they are, what the formatting variations are with respect to HDR (High Dynamic Range), WCG (Wide Color Gamut) and bit coding parameters.

**LACK OF LICENSING REQUIREMENTS STANDARDS**
The same approach to documentation applies to conveying B2C licensing policies for each avail, including device access restrictions within and beyond the household, time-shifting constraints, formatting requirements, and mandated link protections between set-tops and TV sets and across the home networking complex.

**DISPARATE INTERNAL PROCESSES**
Content provider’s ability to compile all this information into avail notifications whether via documents or portals is slowed by reliance on multiple internal workflows relating to legal rights, title master parameters and other metadata and to terms imposed by marketing departments. For operators, the need to ingest all this information into back office systems further slows preparations for distribution.

**LACK OF REPORTING STANDARDS**
Content providers, with occasional exceptions where information is available through B2B portals, rely on spreadsheets, emails and other types of documentation, to convey content entitlements, including distribution windows, geographic constraints, duration of availability, and types of protection that are required with regard to conditional access (CA) and digital rights management (DRM) systems and, increasingly, forensic watermarking as well.

**NO STANDARD LEGAL LANGUAGE**
Matters are further complicated by lack of any means to transcend differences in terminology used with licensing terms, where the phrasing used by businesses for setting policies differs from verbiage common to legal contracts.
All of these complications are intrinsic to procedures that are repeated over and over again in content providers’ one-on-one contractual negotiations with operators, sometimes involving multiple linguistic and territorial contractual variations with just a single outlet. This imposes huge costs on all sides and frequently slows actual distribution of licensed content by weeks or even months beyond the date of initial contact.

For content providers, these costs limit their dealings to operators with market reach sufficient to make it worth their while, leaving them without the content exposure they would get were they able to contract with smaller operators. For smaller operators, the situation limits their ability to put together appealing content packages.

Inefficiencies in Encryption and Key Management

The Content Provider Perspective

Adding to all these complexities and duplications is the need to execute protection mechanisms at every tier of distribution in this manual-intensive environment. For content providers, unlike the days when it was possible to deliver in-the-clear programming in a single contribution format over secure links to MVPD partners, today’s market requires delivery of assets into a multitude of aggregation points for OTT distribution scenarios, including their own direct-to-consumer (DTC) operations centers, as well as the distribution platforms operated by MVPDs, vMVPDs and SVOD providers.

Industry-wide adoption of the MPEG Common Encryption (CENC) system for OTT content has eliminated the need to perform separate encryptions on a given asset going out to multiple affiliates. But content providers still must manage the distribution of decryption keys and digital rights policies for each piece of content transmitted to each affiliate.

Moreover, providers incur the risk of asset theft as each operator decrypts and re-encrypts the content in preparations for delivery. And, perhaps worst of all, content providers have no independent visibility into whether licensing policies are adhered to. Instead, they have to rely on periodic reports from operators, which may or may not convey an accurate picture of what is really happening.
Complications for Operators

For operators, including content providers who are engaging in DTC operations, the complications multiply with the need to match all their protection mechanisms to the requirements of each device, including, in the case of traditional pay-TV services, the CA requirements of operators’ set-top domains. While the market has consolidated around a handful of prominent connected-device operating systems, including iOS, Android and Microsoft Windows, frequently the details of how security is implemented on devices vary from one OS generation to the next, meaning that within any given OEM’s product line different models of smartphones or tablets can require different approaches to security.

These variations have to do with the types of DRMs used for protected content and the means by which operators interact with OEMs and DRM suppliers to authenticate the devices for subscriber’s access to premium content. In the case of DRMs, overseeing encryption key production, provisioning and life-cycle management for all the security applications intrinsic to different device types requires an ability to manage relationships with a wide variety of SoC manufacturers, OEMs, software system suppliers and licensing authorities.

With multiple DRMs in play, operators must ensure keys are generated and refreshed as required to enable playback on all authorized devices, including instances common to linear content where keys must be refreshed multiple times during a viewing session. Each step in the key provisioning and security upgrade processes associated with these interactions must be rigorously secured in accord with established industry practices.
The rising importance of forensic watermarking and the challenges it poses to content protection workloads were addressed in Part 1.

Here the discussion turns to the broader implications of other aspects of advanced security requirements as outlined in MovieLab’s Enhanced Content Protection (ECP) specifications.

Clearly, market conditions are changing the perspective on what needs to be done to secure premium video content. The combination of wider consumer participation in illicit consumption of purloined content and the surging role of high-profile linear content, especially live sports, in OTT services has broadened the application of ECP requirements beyond movies licensed for 4K-UHD and early release strategies.

Live streaming as reflected in the availability of bundled TV channels and high-profile sports events in and outside those channels is now crucial to content providers’ and sports organizations’ efforts to sustain revenue amid falling viewership on traditional TV outlets. Reporting on a 2017 survey of 500 industry executives worldwide, Unisphere Research and Level 3 Communications said that when respondents were asked when live-linear OTT viewing would exceed legacy broadcast TV viewing, more than 50% said the tipping point would come by 2020 while 70% said it would be reached by 2022.
These developments have raised the stakes and challenges respecting timely and effective execution of disruptive action against professional and casual acts of piracy.

Digital TV Research projects that over the period from 2016 to 2022 the losses to theft in subscription and advertising revenue will total $52 billion.

Coordinated, fast responses to pirate streams is vital to stemming the damaging impact caused by illicit re-streaming of live sports and other high-profile events. The ability to immediately identify offending individuals and implement remedial action in time to disrupt viewing experiences is critical to making users aware that the risk of relying on illegal sources is not worth taking. This requires coordinated efforts across the supply chains to collect, share and analyze forensics data.
Through the advances embodied in VCAS Ultra, RightsConnex, StreamMark, Verspective Analytics and other Verimatrix solutions, content providers and operators have the tools they need to address all the issues discussed so far within their individual spheres of operations. Viewthority takes these capabilities to a new level by enabling stakeholders to eliminate red tape and time-consuming manual processes in their licensing transactions, avoid redundancies and risk exposures in execution of content protection mechanisms and exploit new opportunities for collaboration in the use of the Verimatrix tools.

In other words, the Viewthority PaaS - running on the market-leading cloud infrastructure provided by AWS - provides the most effective means yet developed for minimizing the costs and complexities of conducting business in the premium video services marketplace.

The impact Viewthority has in maximizing the benefits of the Verimatrix rights management solutions can be seen in the integration of the Viewthority workflow with Mediamorph’s Content Value Management (CVM) cloud platform.
At the same time, it is important to note that, owing to the commonalities in cloud architectures and standardized approaches to virtualization, Viewthority is well positioned for additional integrations with other cloud platforms that serve to systematize entertainment business transactions. The cloud platform thus ensures the widest possible use of Verimatrix solutions for distribution of live as well as on-demand content in OTT, legacy pay-TV and hybrid pay-TV/OTT scenarios.

The Implications for Security in Viewthority-Mediamorph Workflow Integration

The Mediamorph CVM platform has become the market-leading arena for pursuing business dealings related to digital content distribution. It is used by entertainment companies worldwide to streamline contract management through systematized exposure of their content libraries, metadata files and licensing terms with real-time access to actionable data and analytics processes.

The integration with Viewthority further automates interactions across the supply chain by allowing the seamless flow of content rights and entitlements directly from content providers to operators. This eliminates time-consuming manual processes, while expanding content provider’s ability to ensure adherence to licensing policies. Operators can gain full visibility into content options available for their service strategies, and, once they have contracted with chosen suppliers, VCAS digitally formats the relevant terms and delivers them via the Verimatrix RightsConnex platform directly to their back offices.
Through the RightsConnex API, contract terms are translated for all the DRM modes used in distribution to optimally manage usage windows, playback policies (e.g., download/offline, output copy controls, required level of security, etc.) and the keys that deliver the right content to the right operator in a secure fashion. In turn, viewer and usage data derived from the Verspective Analytics solution are automatically sent back through the workflow, providing actionable viewership analytics that content providers can use to confirm policy enforcement.

The integration with Mediamorph also facilitates collaborative use of Verspective Analytics to help monetize content and services. Part 3 will explore the many ways Verspective Analytics contributes to achieving these goals.

One-Time Encryption and Other Attributes of RightsConnex

As indicated in the Mediamorph example, RightsConnex is central to the platform overcomes all the previously cited encumbrances associated with use of DRM technology.

Critically, RightsConnex makes it possible for content providers to encrypt each asset just once whether its configured as a stored file, a live event stream or linear broadcast channel without the need for decryption and re-encryption at any point between origin playout and end user playback. Decryption keys and playback policies used by operators to gain authorized access to the content are distributed separately and securely with each instance of engagement.
Similarly, at each instance of user playback, the platform supplies the key for decryption and deactivates it in accord with the rights policy. This includes accommodating the multiple key renewals imposed with licensing for live streaming of events and TV channels.

In three-tiered situations where the original content provider feeds assets to a TV network or other aggregator, which, in turn, sends the content to OTT distribution affiliates for delivery to end users, RightsConnex can be used by both the original provider for managing protection on the link to the aggregator and by the aggregator for managing key distribution to affiliates and their end users.

With modularization of its solutions in the cloud environment...

**Verimatrix has maximized the customer’s flexibility to mix CA, DRM or watermarking solutions from other vendors with those provided by Verimatrix.**

With integrations specific to the operating environments of each customer, Viewthority makes it possible to consolidate execution of policies related to all platforms through the RightsConnex pipeline.

For content providers, use of RightsConnex takes the uncertainties out of determining whether licensing policies are properly enforced. Rather than relying on operators to verify they have properly managed encryption and decryption, they retain control over key distribution end to end.

Elimination of multiple encryptions benefits operators as well, not only reducing processing costs, but also relieving them of manually intensive record keeping and reporting on conformance to licensing policies. Moreover, as a cloud-based platform, RightsConnex insulates all users from the costs incurred in legacy environments through unplanned equipment expenditures associated with scaling and load-balancing.
The Expanding Role of Cloud-Enabled VCAS

As mentioned earlier, RightsConnex relies on VCAS, which serves as the single revenue security authority at the heart of the mechanisms embodied in the Verimatrix product portfolio. For more than a decade, VCAS has served as the complete digital TV security solution for multi-screen services over multiple network types with support for:

- Fine-grain entitlement
- Authentication
- Dynamic copy control
- Local file cache and playback

Along with other essential functions across a variety of device categories, including PC/Macs, smartphones, tablets, set-top boxes and connected TVs.

Viewthority capitalizes on the cloud-optimized version of the technology, VCAS Ultra, where stakeholders can access all the benefits of the latest version of the platform, including its support for forensic watermarking, hardware root of trust, Trusted Execution Environment (TEE), and end-to-end link security that are essential to satisfying ECP specifications.

VCAS Ultra is specifically designed to continue to facilitate market evolution away from card-based security systems in the legacy pay-TV, as well as OTT, domains. Working in the virtualized cloud environment, VCAS Ultra ensures that encryption, key management and other content protection functions can be closely synchronized with cloud-virtualized encoding wherever it is physically located.

As noted in Part 1, these benefits are already realized in Viewthority integrations with the AWS Elemental Media Services and Harmonic VOS 360 advanced video processing platforms.

VCAS Ultra supports scalable deployment architectures in broadcast (DVB)-hybrid, IPTV and OTT network configurations, enabling use of HLS and DASH streaming modes with multiple codec and DRM options and harmonized security across video and multi-track audio. This includes support for CENC encryption of multiple DRMs in DASH and CMAF (Common Media Application Format) configurations.
The Verimatrix Viewthority cloud platform takes business dealings between content providers and video service operators to a new level of efficiency where players on all sides can work to mutual advantage streamlining everything from initial engagement to execution and enforcement of licensing policies.

Where traditional DRM and CA protection modes are concerned, Viewthority, running on the AWS infrastructure, enables content owners and their affiliates to leverage cloud-based interactions to eliminate many of the manual processes entailed in securing their assets across an ever-more complex ecosystem. Building on the flexibility of the VCAS Ultra cloud-based security suite, Viewthority automates the flow of content rights and entitlements from content providers to operators, aided by integrations with asset management systems like Mediamorph.

For content providers, it is now easier to structure and disseminate policies in accord with all the variations in formats, modes of distribution, usage parameters, targeted device profiles and local regulations that characterize today’s global marketplace. And with visibility into each affiliate’s use of protected assets, content providers have a direct means of overseeing policy enforcement, avoiding the uncertainties, delays and encumbrances associated with reliance on affiliates to report on their conformity with those policies.
Likewise, video service operators benefit from this Viewthority-enabled automation by making it easier to set up licensing terms and to eliminate the vulnerabilities and costs associated with decrypting and re-encrypting content as it enters their domains. Moreover, operators are unburdened of the costs of validating licensing policy enforcement while expanding access to high-value content in instances where providers might otherwise not want to risk an affiliation.

These Viewthority benefits also extend to execution of higher levels of content protection, including forensic watermarking, for Ultra HD-formatted content and other valuable assets streamed live or on demand. As protection requirements like those spelled out in MovieLab’s Enhanced Content Protection (ECP) specifications become more universally applied in an era of mounting piracy, Viewthority enables content providers and operators to take much of the pain out of the transition to what seems certain to be the new norm in premium content licensing.

Talk to one of our experts and discover how Verimatrix can help you resolve complexities in content licensing and security. Request a demo here.