M+E JOURNAL

The Future is Automated

The landscape ahead for M+E looks uncertain. Automation can ease the journey.

WORKFLOWS AND THE CLOUD
From cloud-based productions to unprecedented storage demands, the supply chain has never been more challenging

SMART CONTENT
The questions around AI, metadata, and analytics are endless. But we do have many of the answers already

SECURITY SOLUTIONS:
Cybersecurity and content protection in M&E is always on defense. Can automation can change that?

23.01

STRENGTHENING YOUR CONTENT'S PROTECTION: GO BEYOND DRM

The evolving nature of video security threats means an 'on your toes' approach

ABSTRACT: You might be surprised to learn DRM with token-based authentication can still be hacked. Breaches to delivery and device environments are outside the scope of what DRM can protect. To fully thwart hackers and pirates, additional tools are needed, and comprehensive best practices should be followed.

By Jon Samsel,
Global VP, Marketing,
Verimatrix

The protection of valuable video content clearly remains paramount — and even more so than yesteryear due to the vast media consumption choices demanded by viewers today. However, it's also now clear that digital rights management (DRM) no longer comes close to addressing today's ever-advancing threats that accompany these news ways of viewing and subscribing to content.

The fast rise in sophisticated piracy threats and cybersecurity breaches in streaming and broadcast means that the solitary use of DRM isn't even designed to take on non-DRM related threats. DRM technology is decades old, and the bad guys have become far cleverer and patient in their endeavors. They're finding ways to bypass DRM using exploits that were likely unimaginable just a few short years ago. Thus, DRM needs to be retrofitted with modern security approaches that come much closer to closing all of today's security gaps.

As a cautionary note, the need for newer technology is not meant to diminish DRM's role. Make no mistake that DRM is far from worthless. It still plays an essential role in protecting video content. It simply must now need to be paired with additional security solutions. Think of DRM as a lock on a door. It can deter burglars, but if they find a way to bypass it, it's no longer effective. A lock is an old technology that is still needed, but it cannot do it all. DRM is the same, it has an important role if used correctly.

Relying on numerous connected processes and devices, today's delivery of entertainment content demands an ecosystem type of approach. It's this interconnectedness that makes a comprehensive new set of countermeasure-like approaches so clearly needed to combat today's video security and piracy threats. Any video security solution that's largely just off-the-shelf DRM technology is far from adequate. Don't be fooled by DRM-only technologies that tout their simplicity as a reason for their deployment — quite the contrary.

In 2023, DRM has inherent complements. An obvious accompaniment for many might be forensic watermarking. Additionally, organizations can look to not only fortify the execution environment, but also ensure the keys and key-exchange process is properly obfuscated. Another simple yet often overlooked step is to be sure that technology providers deliver all relevant documentation needed to help make sure that everything is configured correctly and secured as it should be. That means a reliance on any default parameters or settings is a big red flag.

Persistence and focus play a big role for those tasked with ensuring video security. Although there may be a need, for example, to look to new chipsets and other hardware deployments, those efforts almost assuredly take more time than initially planned. It can be that time when a new threat can emerge, just as new hardware is being adopted. An example of the benefits associated with a comprehensive security approach then shines through — are tools that are already in place, such as forensic watermarking, which can identify and link specific services with specific devices and create a much-needed trail when it's thought that piracy either is or was underway.

RELYING ON NUMEROUS CONNECTED PROCESSES and devices, today's delivery of entertainment content demands an ecosystem type of approach.

Providers will benefit greatly from regularly scheduled surveys of their environment that take a continual look at technical requirements that typically spawn from perhaps ever-changing strategic business requirements and industry norms. By going back and looking at defenses in this way, it's often easier to map out what works and what doesn't in an infrastructure — including all types of flows as well as protection tools and general techniques that all come together to make their service possible in the first place.

By maintaining a heightened sense of familiarization surrounding one's current platform, it's that much easier to be sure that the technical teams align with executive management and their objectives and concerns. A thorough and diligent audit can greatly improve security over the long haul as well as during any smaller adjustments. Although a few of the below items could be construed as being rather obvious, it's not uncommon to find them unaddressed even among sizable institutions. Be sure to look at your:

■ ***Important documentation and tracking.*** Is the end-to-end platform documented adequately, and are current versions of every item in the platform and the versions of its software consistently tracked?

■ ***Examination.*** Does an adequate lab-like environment exist to allow for testing which is separate from the production environment? This way, challenges can be recreated and evaluated to fix them in a timely fashion. Are all documented services use case tested? And do qualified personnel test all software updates before implementation? Same with new hardware?

***Jon Samsel** is the global vice president of marketing for Verimatrix. The chief storyteller for the company, he has three decades of experience working with leading brands such as Bank of America, Apple, and Ford. He has also founded two startups that had successful exits, RoadLoans, a direct-to-consumer auto finance lender acquired by Banco Santander, and Heardable, a brand analytics platform acquired by Hatcher+. jsamsel@verimatrix.com @VerimatrixInc*

- ***Destination information.*** Are the platform's sources and destinations known, and are they comprehensively protected? Are the interchange points across the platform (APIs) properly implemented? When a session is opened, does the platform check whether the request is from a known or knowable source? And are sessions managed and ended in an efficient manner?

The evolving nature of video security threats means an "on your toes" approach is inevitable if an organization seeks to remain one step ahead of the bad guys. One step further would be to implement a more comprehensive video protection, as DRM alone is not enough. ⊞