

**M+E**

**JOURNAL**

Today's localization challenges are enormous. The opportunities are unprecedented. Is the industry ready for the mayhem?

# GIVING VOICE TO CHAOS

## **SECURITY SOLUTIONS**

The threats to our most valuable assets are many. M+E vendors are on top of it.

## **WORKFLOWS AND THE CLOUD**

Much has changed in the way we track, access, move and store everything we deal with.

## **SMART CONTENT**

The many ways the industry adopts new technologies to make content smarter.

22.02

# STAYING AHEAD OF THE CURVE

The options to secure content are vast.  
Make use of all of them



*Photo by Robin Pierre /unsplash.com*

**ABSTRACT:** The increasing demand for video content underlines the need for additional streaming flexibility. But with global piracy costs representing up to 24 percent of lost revenue, it is critical to focus on minimizing vulnerabilities. This article explores the secure workflows and protections content owners can employ to fully protect their titles.

**By Joanna Syiek,  
Senior Directing, Marketing,  
Vision Media**

Film and television content requires intense investment of time and funds. Once content is created, studios and content owners must contend with various market pressures (including shrinking windows, consumer demands, and the need for high quality playback and bandwidth) as they find the audience for their titles. These demands have led to an ever-increasing pressure to tighten security measures to protect high-value content.

As those in the media and entertainment industry know, video piracy is not a new trend. In recent years, increasing economic pressure and the COVID-19 pandemic amplified demands for both licensed and unlicensed content. According to NERA Economic Consulting and GIPC, digital video piracy amounts to at least \$29.2 billion and as much as \$71.0 billion annually in lost revenues, representing overall revenue reductions between 11 percent and 24 percent.

The increasing demand for video content underlines the need for additional

**WHEN IT COMES TO THE QUESTION** of what's next for screener security, it will be necessary to consider the modes in which audiences will be engaging with content. AR, VR, and MR technology continues to become more mainstream for consumers and the metaverse's development is clipping along at an accelerated pace.

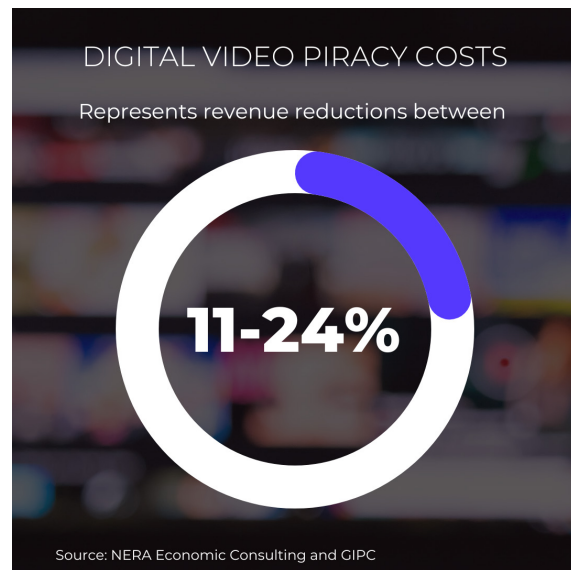
streaming flexibility. But with global piracy costs eating into content's revenue, it is critical to focus on minimizing vulnerabilities. Luckily, there are several secure workflows and protections content owners can employ in tandem to fully protect their titles.

### ROBUST DRM/CAS

One of the primary lines of defense against pirate attacks that video service providers need is either a strong layer of protection via either digital rights management (DRM) and/or a conditional access system (CAS). Both help prevent unauthorized access of video content from unauthorized users and hackers; CAS can be thought of as a transport protection mechanism while DRM is an asset protection mechanism. Many secure video solutions and OTT platforms are outfitted with protections that can perform both CAS and DRM functionality. Today, the differences between DRM and CAS are few, though it is likely that there will continue to be further advancements in CAS and DRM technology in the future.

### FORENSIC WATERMARKING

Session-based forensic watermarking helps protect content both before and after release. With this type of watermarking, each playback session features an embedded identifier which allows the content owner to establish a link between the playback session and the user. This level of additional forensic capabilities supplements security such as DRM or CAS by protecting decrypted content from escaping undetected, enabling identification and enforcement and makes it applicable to criminal proceedings should any illegal activity occur. And the appetite for watermarking has increased in



*The true costs of video piracy.*

recent years as well with more viewers watching at home and around the world, especially with the ripple effect from the pandemic. On Vision Media's platform, there was a 98 percent year on year growth in watermarking from 2020 to 2021 as studios adjusted to balancing viewer demands and security needs.

### RESTRICTED PLAYBACK WINDOWS

Another way to reduce unauthorized sharing is to establish strict playback rules when sending secure invitations to view content. This can include: 1. Limiting the viewing window during which a user can watch a title. 2. Establishing a set number of times a user can watch the title. 3. Restricting playback by device-type or IP address.



*Joanna Syiek is the senior director of marketing for Vision Media. She has worked in the media space for more than a decade, helping to develop global marketing strategies and grow businesses at the intersection of entertainment and technology. [info@visionmedia.com](mailto:info@visionmedia.com) @jwsyiek*

IP restriction is popular for being one of the more cost-effective ways of protecting content, but title owners must be aware of the risk of IP spoofing as a potential workaround to this level of security. Each of these restrictions allow content owners to control how users interact with a title, especially pre-release, and helps to deter viewers from sharing with additional users.

### **HTTPS VIDEO DELIVERY AND TRANSFER**

When it comes to data that needs to be kept private, HTTPS offers a level of web encryption that provides security by preventing tampering when the video file is in transit. While moving from file location to file location, encrypted data cannot be changed without destroying the data completely. It also offers authentication and peace of mind as data sent via HTTPS connections can verify their source location.

### **PASSWORD PROTECTION**

When sharing video internally or with external stakeholders, VIPs, or wider audiences, password protection still is a powerful and essential method for protecting content. As always, changing passwords every couple of months is recommended for additional security. Additionally, content owners can integrate with a SSO tool to help ensure additional protection on content invitations.

### **DETECT AND DETER CONCURRENT STREAMS**

While credential sharing can lead to simultaneous logins from multiple locations, programs that allow content owners to see and investigate any unusual password activity can be key to cracking down on illegal sharing. Content owners can benefit from tools that allow them full transparency into users logging in from various IPs. If a user logs in two locations that are thousands of miles apart from each other in less than 1 minute, they can review and restrict that user from access.

### **STAYING AHEAD OF THE CURVE**

When it comes to the question of what's next for screener security, it will be necessary to consider the modes in which audiences will be engaging with content. AR, VR, and MR technology continues to become more mainstream for consumers and the metaverse's development is clipping along at an accelerated pace. According to BCG and Mordor Intelligence, the current market value for AR/VR/MR is around \$30.7 billion, and the market size worldwide of the AR/VR/MR market is to rise to \$300 billion by 2024. Content owners will likely want to select screening partners who are ready for and adapting to the changes ahead. 