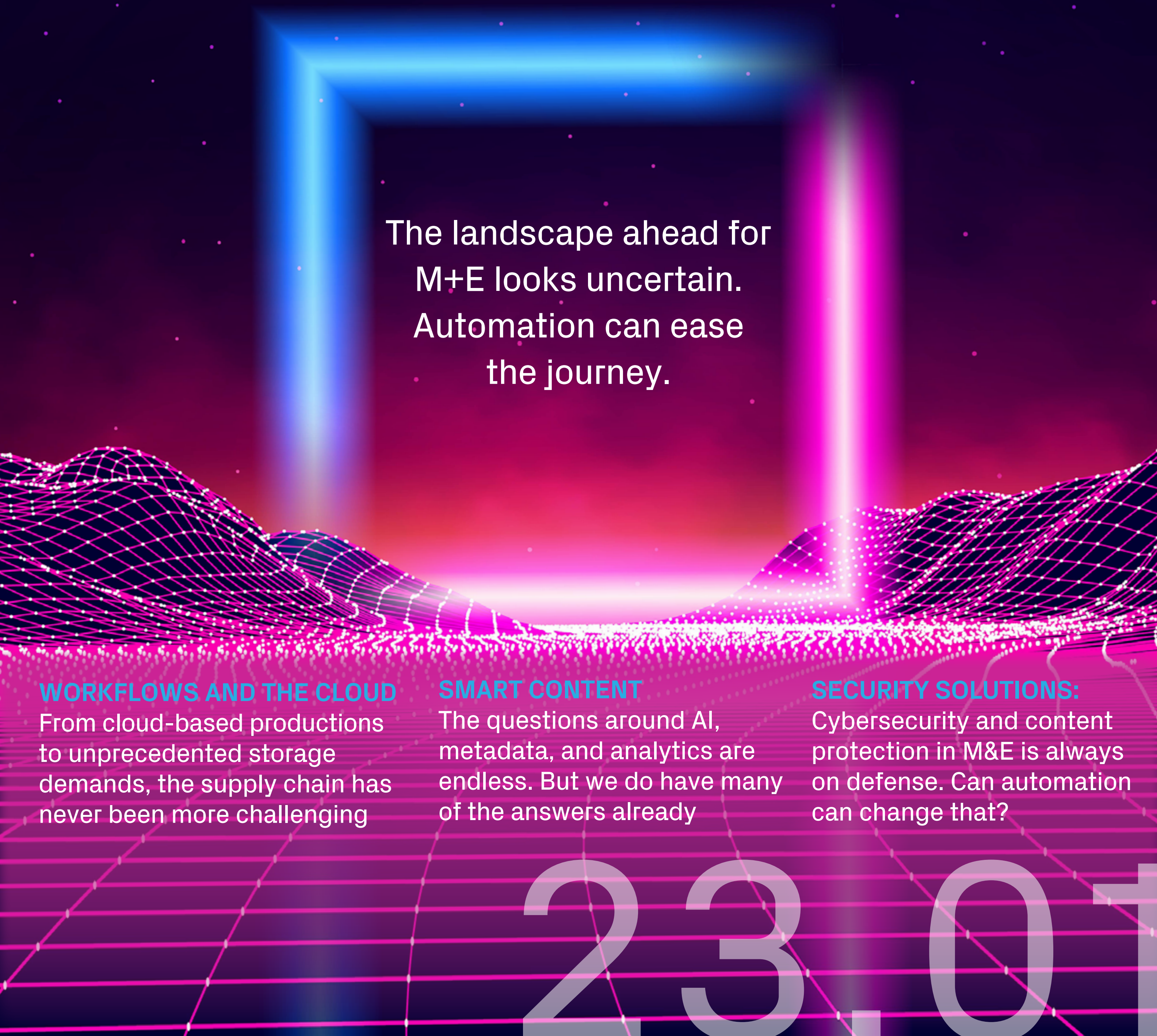
M+E JOURNAL

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

LEVERAGING AI TO FIGHT STREAMING PIRACY

Digging into the data can improve our protection efforts

ABSTRACT: In today's video streaming landscape, protecting our favorite TV shows and movies from piracy requires rigorous analysis of data. A daunting task considering that associated data grows by billions of records each month. This article explores how AI and ML can greatly improve the effectiveness of anti-piracy efforts in the industry.

By Werner Strydom, Head of Advanced Technology, Innovation;
Rodrigo Fernandes, Product Director, OTT;
and Jessica Alecci, Senior Data Scientist, Irdeto

The U.S. Defense Advanced Research Projects Agency (DARPA) informs us that we are currently experiencing the third wave of the evolution of artificial intelligence, which is characterized by the development of systems that can reason and learn in much the same way that humans do.

This wave is powered by several key technological advancements that create the perfect conditions needed for smarter, more contextually aware autonomous systems. Although there is much debate as to exactly which advancements have played the greatest role, we can at least agree that we now have access to more sophisticated AI algorithms, significantly more powerful, inexpensive, and ubiquitous computing resources, and large amounts of data that can be used for training AI systems.

The third wave of AI is also having a significant impact on cybersecurity, primarily by enhancing the speed and accuracy of threat detection and response. Cybersecurity solutions that make use of a combination of rule- and machine learning based algorithms have the potential to greatly improve the effectiveness of anti-piracy efforts in the video streaming industry. By automating

CYBERSECURITY SOLUTIONS THAT MAKE USE OF A COMBINATION OF RULE- and machine learning based algorithms have the potential to greatly improve the effectiveness of anti-piracy efforts in the video streaming industry.

repetitive tasks, providing new tools for identifying and tracking pirated content, and finding subtle patterns in complex data sets that indicate new forms of piracy, these technologies can help rights holders to better protect their content and ultimately benefit the entire streaming industry.

DRM LOG ANOMALY DETECTION

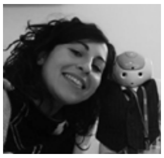
According to Grandview Research, the video streaming market size is expected to expand at a compound annual growth rate (CAGR) of 21.3 percent by 2030. To secure content and protect valuable revenue, the industry regularly uses a variety of technologies such as digital rights management (DRM). DRM is widely used within the pay media industry to ensure that video content is stored and transmitted in encrypted form, so that only authorized users and devices can play it back. When a user attempts to play back a protected video, the video player must first request a DRM license from a DRM server. The interaction between the DRM agent in the video player and the DRM backend — the DRM protocol — makes it possible to collect a host of valuable data about how the platform is being used.

But DRM systems are not entirely foolproof. Pirates continuously find ways to circumvent security technologies to steal and illegally rebroadcast licensed content. This is where artificial intelligence (AI) comes in. AI can be used to detect the difference between normal – and legitimate – use of a streaming platform, and abnormal usage that could indicate piracy. Traditionally, detecting this type of activity would require resource intensive and time-consuming manual analysis of the data. In particular for "big data" sets with multiple billions of records added to it each month. Although rule-based detection methods can go some way towards automating this process, it is less effective at detecting all threats. Especially if they are not encountered beforehand or if the abuse pattern is very subtle. The best solution is to complement the rule-based approach with an AI algorithm.

The exact nature of the data may differ slightly from one pay media operator to the next. But typically, it includes a timestamp of when the DRM interaction took place, the content that was being accessed, the data that identifies the device/player that was used in accessing the content, the IP address of the device, and often an identifier that can be traced back to the subscriber using information in other backend systems.

For an initial test of an AI solution, our team chose an auto-encoder architecture model, which makes semi-supervised learning possible despite lacking enough labeled data. Using cleansed data for training, the goal is for the encoder to learn how to interpret the input and compress it to an internal representation. This is done while the decoder attempts to recreate the original input from the output of the encoder.

***Werner Strydom** is the head of advanced technology and innovation and works for the office of the CTO at Irdeto, where he leads the advanced technology, enterprise architecture, and innovation teams. He has been with Irdeto for 30 years, having held prior roles in software engineering, architecture, product management, and technology management. Strydom has a background in computer science and applied cryptography, and a comprehensive understanding of the cybersecurity market. info@irdeto.com @Irdeto*



***Jessica Alecci** is a senior data scientist within Irdeto's advance technology team. She has a background in computer science and has worked in the data science field for the past six years. As part of the advance technology team, she collaborates with other teams, both within the company as well as with external clients, to brainstorm about, implement and validate new ideas that employ AI technologies. **info@irdeto.com** @Irdeto*

***Rodrigo Fernandes** is the product director for OTT products at Irdeto. He started at Irdeto in 2012 as product manager for Irdeto's multi-DRM solution. Prior to that, he worked for more than 14 years in the telecom industry in different roles. Currently, he is focused on growing and enhancing existing video streaming security capabilities, including multi-DRM cloud services, client security and the use of AI/ML for service abuse and piracy detection. info@irdeto.com @Irdeto*

The original input and the reconstructed input are compared through a distance measure. This allows a threshold to be set, whereby all inputs with a distance value higher than the set threshold are identified as anomalous data points.

The following workflow explains how the AI solution works in practice:

- ***Data are pre-processed and summarized to ensure that training and inference operations are cost and computationally effective.***

- ***The model ingests the data that represents "normal" activity, which is identified through a set of rules. It produces a binary prediction (anomaly vs not anomaly).***

- ***A report with detected anomalies is shared with the customer.***

- ***The customer validates the predicted anomalies and provides feedback. The model is re-trained based on the customer's feedback (e.g., confirmed anomalies are removed from the training set) to ensure that model's quality is up to date.***

This approach allows for customer-specific AI models, where the model only learns from the usage patterns of the target customer's platform. This ensures that one customer's data is not exposed to the models of other customers. It is also important that differences in business models are correctly reflected. Additionally, the AI model can also be specifically tailored for different DRM types such as Widevine, PlayReady, and FairPlay, to detect DRM specific anomalies.

The solution is currently being validated with targeted customers and has already yielded valuable results. Interestingly, it also flagged up anomalous behavior that, once investigated, proved to be a buggy DRM implementation. A combination of both rule- and machine learning-based detection of anomalous behavior yields much better results than one based only on rules.

Looking forward, the AI model must be continuously evaluated and improved upon based on content piracy evolution. We also plan to advance the current periodic anomaly detector to be a real-time alerting system to further mitigate piracy and fraud. ⊞

5 Steps to Establish an Anti-Piracy and Cybersecurity Management Program

By Mark Mulready, Vice President, Cyber Services, Irdeto

Cyberattacks have become increasingly sophisticated and frequent and the need to manage cyber risks to ensure business continuity has been consolidated on every leadership agenda. According to data from Microsoft's 2021 Digital Defense Report, 24 trillion threat signals had been identified by the company around the world, a significant increase from the three trillion signals from the 2019 report.

In the entertainment industry, it is no different. Content piracy is one of the biggest issues plaguing the video-streaming and the OTT (over-the-top) industry worldwide. By the end of 2022, piracy cost all industries a total of $51.6 billion, $6.7 billion for video entertainment alone.

There are multiple reasons for the rise of digital piracy. First, access to cheap (or free) content can appear lucrative to many. The advent of new technology has made pirated content readily available to those whose geographical locations otherwise restrict them from accessing it.

Piracy can impact the consumption of original content through password and credential sharing, sending files over the internet, and purchasing illegal streaming devices and services. These are available at just a fraction of the cost to the consumer but impose mounting revenue losses and reputational harm on the original creators.

As content consumption and digital access continue to grow, stakeholders must collaborate to form effective anti-piracy strategies as it is not enough to install anti-piracy software. An effective program requires not only the right tools but also the right mindset and awareness throughout the entire organization. It is also essential for companies to drive discussions in their local markets, promote campaigns and support government action to improve the piracy landscape and pave the way for a brighter future.

Based on our experience as a global leader in video security and beyond, from "lens to screen," and from "production to consumption," here are our recommended five steps to establish a successful anti-piracy and cybersecurity management program.

Prevent and protect

Using multi-DRM and conditional access, an industry standard, is the first step in preventing piracy and protecting valuable content. An effective multi-DRM system provides a frictionless viewing experience, while at the same time protecting and maximizing content revenue. It keeps infrastructure costs in check and helps untangle and simplify DRM deployments across various players, streaming formats, devices, and platforms.

Forensic watermarking should also be an industry standard. Fortunately, encoder, packager and CDN standards and integrations have made watermarking content significantly easier.

Concurrent stream management limits credential sharing and allows operators the ability to upsell additional streams. Finally, the final line of piracy defense involves code protection and obfuscation to protect software from unwanted attacks.

Platform hardening

The second step in fighting piracy involves hardening your platform to minimize the risks from hacking attempts targeting your content or back-end systems. The industry has seen countless examples where hackers have gained access to a platform and, through that vulnerability, wreaked havoc on other systems.

A good example of platform hardening is penetration testing — or pentest — an in-depth security assessment on a specific system or component within an OTT environment, OTT application or even an important server for the OTT platform. During this test, the security team simulates an attack by a malicious person on a selected (web) application, infrastructure, or device. For example, a pentest on an Android OTT application includes testing the app on a mobile device but also focuses on communication with the backend.

Monitor and detect

Our third important step in anti-piracy and cybersecurity management involves monitoring and detecting threats. The business strategy benefits from the recognition of the type of threats the business may encounter. Effective tools such as online piracy detection (OPD) and brand protection make it more difficult for pirates to find alternative sources, devices and subscriptions.

Tools that should be used include threat intelligence to monitor information gathered via proprietary web crawling, deep and dark web mining; live, VOD and P2P content discovery using crawlers built to discover where infringements happen on the internet; brand protection measures and anti-fraud management.

Investigate and analyze

Investigation and analysis is an important step in any anti-piracy program. This is where companies and cybersecurity vendors need to operate on the offensive, as opposed to the defensive stance of the previous steps. It is where you will find out exactly how pirate applications and devices work.

It should include threat investigation and reverse engineering service to be applied to customer applications to test the robustness of the application against a variety of attack types, intelligence analysis and forensic evidence collection.

Report and enforce

Finally, companies and cybersecurity vendors must report and enforce in collaboration with international partners. There is no silver bullet to piracy and the fight against piracy cannot be done alone. Collaboration with partners can include measures such as payment disruption, IP blocking and takedowns, but also insights, managed services, consultations, and training others in the anti-piracy/content protection community. We are in this together and can certainly learn from each other.

Whether it is movies, high-profile series or live sports events, video content continues to be one of the most valuable intellectual property forms in the world. Increased screen options for consumers (phones, tablets, smart TVs, etc.) have facilitated the growing consumption of video content over the years. It is crucial to ensure that these assets are adequately protected.

As mentioned, there is no magic cure for piracy. As video entertainment delivery and consumption evolve, pirates continuously find new ways to circumvent security technologies and steal valuable assets. Rights holders and content owners must use every tool at their disposal to continuously prevent these emerging threats and protect their revenue. An end-to-end approach combines state-of-the-art security technology with expert piracy oversight, cyber investigations, intelligence analysis and targeted enforcement. ⊞