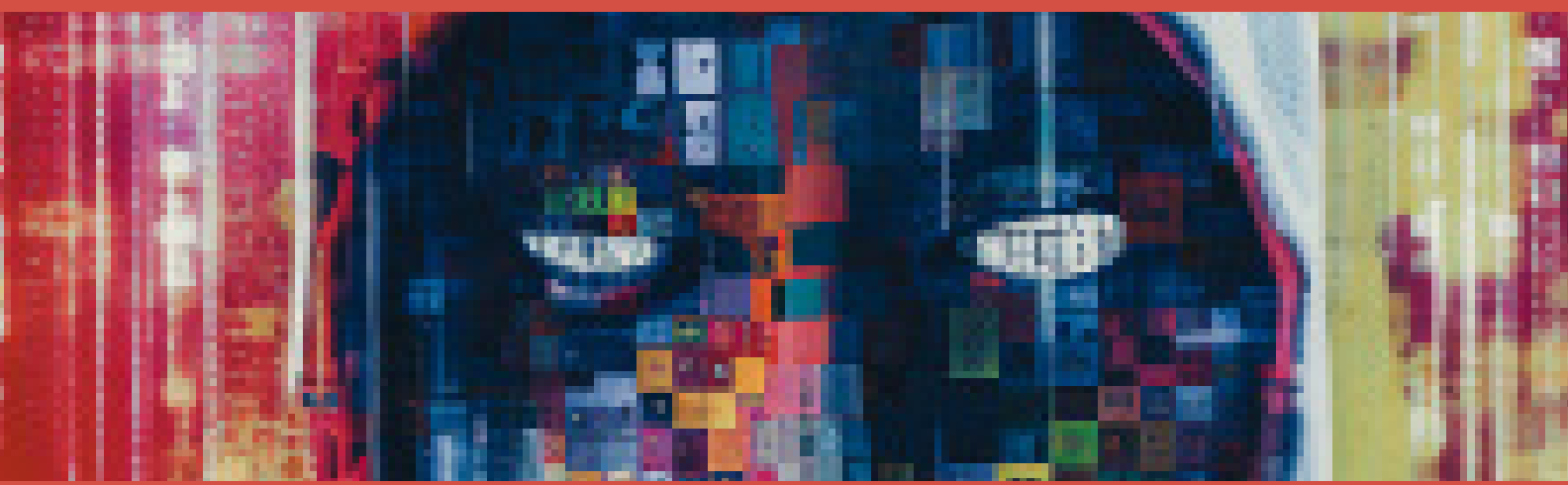
M+E JOURNAL

A SECURE AI WORLD?

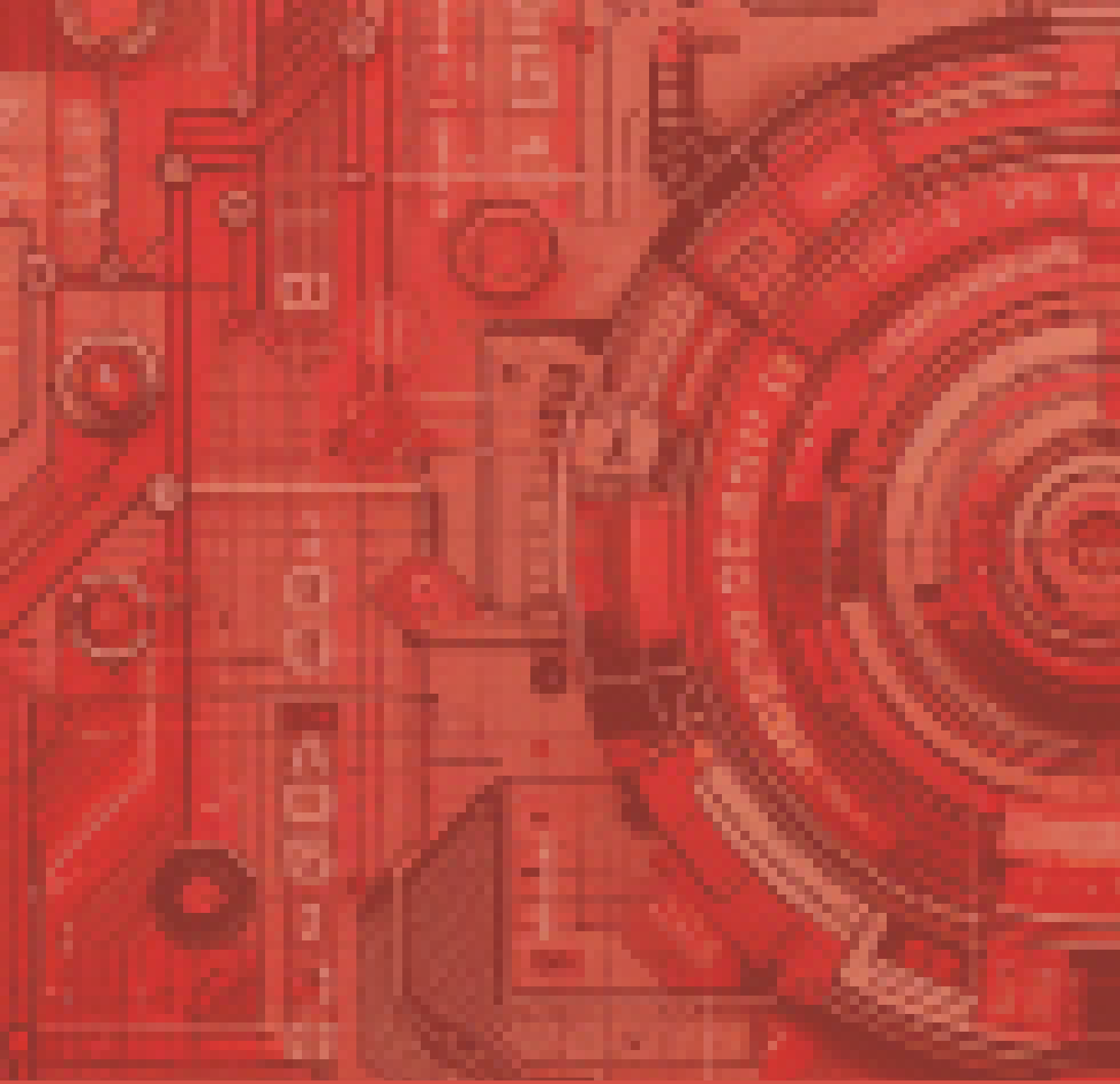


How AI is being used both by and against the industry

SECURITY SOLUTIONS
Where and how AI is being used to attack and protect M&E

SMART CONTENT
Massive amounts of data now required new tools, including AI

23.02



A SECURE AI WORLD?

Staying up to date with the latest cyberattacks and piracy and threats — and the defenses against them — means sometimes using the tools the enemy is using against you. Today that means embracing AI. While the bad actors are using AI for deepfakes and phishing attacks, media and entertainment is employing it for anomaly detection and watermarking.

THE STATE OF M&E SECURITY

From defending a streaming-centric industry to how AI can help in cyber defense

MESA spoke with several leaders in the content protection and cybersecurity space, asking for their thoughts on the pressing security needs of a streaming-first world, the impact AI technologies are having on security and content protection, and what's next for the industry.

By Chris Tribbey, Editorial Director, MESA

MESA: *What do you consider to be the most pressing content protection and cybersecurity threats facing media and entertainment today?*

JT Gaietto, chief security officer, Digital Silence: We are seeing the convergence of content protection and cybersecurity due to the growth of streaming, interactive companion apps, and metaverse content. As streaming apps expand to as many different platforms (e.g., Roku, Apple TV, PS5, etc.) as possible and the concerns around account sharing increase, this puts additional pressure on penetration testing applications and platforms where content is stored, streamed, and accessed.

The other major area of concern we're seeing is in the "physical" world of media and entertainment. Since the pandemic closures ended,

MEDIA AND ENTERTAINMENT COMPANIES THAT INVEST IN FINDING ways to stay ahead of or react to threats as quickly as possible will be the ones that most effectively minimize subscriber churn to pirated services.
— Alain Durand, senior director of business development, Synamedia

venue and live events have become a cornerstone of growth for many companies. The use of technology to enrich these events is becoming even more important, for example, the Sphere, or the use of RFID at music festivals to allow concert guests to easily enter different areas of the venue, pay for merchandise, and even buy food and drink. Misconfiguration of the underlying technology supporting these can result in public safety concerns, loss of content, disruption of the venue, and significant financial loss.

Alain Durand, senior director of business development, Synamedia: Identifying one threat is a challenge because pirates' approach to content theft is constantly evolving. The primary factors are that they will always opt for the simplest way to steal content, therefore keeping their operation costs as low as possible. Media and entertainment companies that invest in finding ways to stay ahead of or react to threats as quickly as possible will be the ones that most effectively minimize subscriber churn to pirated services.

Robin Boldon, head of product, Friend MTS: With an increasing number of SVOD services adding sports to their offerings, global protection of live sports is a real focus in the industry. For content owners and distributors to service and grow their business, it is critical that valuable content preserves its value. Our role at Friend MTS is to ensure that stolen streams are detected at scale thanks to sophisticated monitoring and to limit the spread across pirate networks by taking down stolen content in real time. This is the only way to preserve the ultimate value of the content and help media companies in being successful.

For both live and VOD content, we identify three key content protection and cybersecurity threats that content businesses need to focus on to prevent revenue losses: content leaks, either from production workflows or distribution channels (e.g. post-production, localization, broadcast, CDNs); platform design vulnerabilities, such as lack of DRM key rotation, session binding, deprecated CDM revocation, account fraud analysis. Pirates exploit a lack of priority given to security when designing streaming platforms; [and] cyber-attacks, attacks on an organization's IT infrastructure to obtain sensitive IP and other information for the purposes of extortion, reputational damage, political or blackmail.

Jon Samsel, SVP of global marketing, Verimatrix: The media and entertainment industry is currently facing serious challenges with content protection and cybersecurity, the most pressing of which is the exploitation of software-native Digital Rights Management (DRM). This technical vulnerability allows pirates to bypass DRM protections, leading to unauthorized access and distribution of content. This not only undermines revenue streams but also the integrity of content distribution.

Harish Bhat, product manager, forensic watermarking and anti-piracy, PallyCon: [The ability] to bypass DRM protection, illegal downloads, CDN leeching and re-streaming in non-authorized regions along with the ransomware attacks, deepfakes, supply chain and cloud security are the threats M&E facing today.

Stan Stahl, founder and president, SecureTheVillage: Any discussion of threat has to explore three dimensions. There's the obvious threat from miscreants and other cyber scum, coming both from cyber-cartels and nation states. AI will only make this worse. Then there's the legal/regulatory dimension. The SEC is coming down

***Chris Tribbey** is the editorial director of MESA. He's responsible for MESA's 13 newsletters published each week as well as the monthly EIDR Report. An award-winning journalist with 25-plus years working in newspapers, magazines, and online outlets, Tribbey's work has been published in Variety, The Hollywood Reporter, Home Media Magazine, Broadcasting & Cable, The Sporting News, the Miami Herald, the Florida Sun-Sentinel, USA Today and Sports Illustrated.*
chris.tribbey@MESAonline.org

hard here with its suit against Solar Winds and their CISO. The FTC, too, is strengthening its Safeguards Rule. And the states are passing their own privacy legislation. The threat from laws and regulations is the second dimension that management must consider. The third dimension is the human dimension; the cultural. It's the threat from poor "Tone at the Top," from a check-the-box mentality towards cybersecurity, and the failure to build cybersecurity knowledge, attitudes, and actions throughout the workforce, in IT and throughout the workforce. This third dimension is the most important because it amplifies the impact of the other two.

MESA: *With the studios increasingly focused on streaming first, what are the major content protection and piracy impacts, compared to those associated with theatrical and physical disc releases?*

Miguel Bielich, product marketing director of video entertainment, Irdeto: [There's a] larger attack surface. Discovering during our engagements, over 1000 systems exposed is no exception. Many different systems, administrative interfaces, risky ports exposed, unmanaged systems, legacy systems, etc.

Durand: Older business models relied heavily on content release windows with a particular focus on preventing any leakage before the physical disc release. With studios now shifting their focus to streaming releases first, end users expect their content to be delivered in shorter windows — the sooner the better — which causes additional challenges to reach the same level of protection. Studios will need to deploy multiple content protection techniques, including encryption and watermarking, to preserve their revenues or evaluate releasing content to a subset of users or one specific platform so that higher security and content protection can be guaranteed.

Boldon: Compared to traditional theatrical and physical disc releases, digital assets and streams are more easily copied, traded, and redistributed by pirates: a full movie in HD quality can now be downloaded in just under 15 minutes from the web. Current DRM schemes are no impediment to professional pirates that are highly motivated to circumvent protection for significant profits that can be made from illegal content redistribution. Content can be obtained directly from a streaming platform by exploiting a known vulnerability within its CDN or DRM solution - the threat known as "content leeching." When content leeching occurs, the platform foots the infrastructure bill for the pirate, i.e. pays to service the pirates' illegitimate audience.
With streaming first, the most valuable studio content requires enhanced end-to-end protection with a full suite of content protection and anti-piracy measures from forensic watermarking to digital fingerprinting, smart piracy detection systems and server blocking continually upgraded to stay ahead of the constantly evolving piracy threats.

Delivery server blocking enabled by large-scale automated content monitoring is one of the most effective methods to mitigate the threat of illegal live content redistribution today. Video capture and analysis monitoring is equally effective for all live content not just sports, and service providers can deploy the same monitoring solutions to protect their valuable content within early-release windows when rapid IP enforcement is of the essence.

Samsel: As Hollywood studios pivot towards a streaming-first strategy, the shift has exposed new vulnerabilities compared to traditional media distribution methods. The use of DRM exploits allows for content to be illegitimately accessed via CDNs of the legitimate distributors, effectively doubling the financial impact. This form of piracy is more accessible and cost-effective for pirates compared to the distribution of pirated physical discs or theatrical releases, which required more complex distribution systems and were less suitable for live streaming.

Gaietto: Steaming and the home content consumption model are clearly growth areas. While we continue to read about things slowing down, we've seen technologies demonstrated that can monitor who is in a room and make assumptions about their age, sex, and other demographic information. This introduces some interesting growth opportunities, enabling focused content and ads to be shared with the target audience. However, from a privacy perspective, monitoring what happens in a customer's home is very cutting-edge. We've already seen mobile device companies like Apple clamp down on the use of personal conversations.

MESA: *In what ways do you see AI impacting M&E security today (threat and piracy detection, network and physical security, predictive analysis, etc.)? Do you see AI working in tandem with other technologies, like DRM and blockchain?*

Gaietto: First, it's worth noting that there seems to always be a "hype cycle" with new technologies as they come to market. This is true with AI, just as it was with blockchain a couple of years ago. AI can disrupt, including predictive analytics and using generative AI to defraud users and companies. Specifically in the M&E space (an industry where there is plenty of content available from key executives), it would be very easy to feed a large language model (LLM) platform information from a target executive to learn their speech patterns and methods of communication. Attackers can then use content generated in this way to attempt to social engineer targets.

While there are threats of deepfakes and other content mis-generation, there is also an opportunity to utilize AI alongside DRM and blockchain to better protect content. It wouldn't be too far to reason that one could use machine learning to monitor known VPN and SMART DNS sources and map those content delivery requests to known blacklists feeding DRM and blockchain distribution platforms. However, like all security strategies, it's a cat-and-mouse game; as defenders improve their security, the attackers adapt, and thus the world continues.

Overall, it's easy to see how generative AI and ML both will help and change the overall threat landscape.

Bielich: Pirates are more adept at covering their tracks. There is so much more data available that can be cross analyzed. So, AI/ML helps in detecting patterns much faster. However, human analysis is key. Tech is one piece, but it can also fail. Having human analyst

AI IS GOING TO HAVE A HUGE IMPACT AND HELP ENHANCE SECURITY in several ways such as looking at the content played, license requested patterns, usage and suggest the possible threats with necessary action to be taken.

— Harish Bhat, product manager, forensic watermarking, and anti-piracy, PallyCon

vetting the data and then help transform the data into business intelligence for our customers based on our expertise and knowledge is highly valuable and appreciated by them, especially those that are highly protective of their brand and relationship with their customers.

Bhat: AI is going to have a huge impact and help enhance security in several ways such as looking at the content played, license requested patterns, usage and suggest the possible threats with necessary action to be taken. It would even help to trace the region of piracy and impact on the revenue as well. AI would be being used with almost all security components involved in the streaming be it CDN, DRM, watermarking, access control etc. and we already see each company announcing the adoption of AI from improving the video quality till delivery with ultra-low latency. As AI continues to develop, AI-powered security solutions are becoming more sophisticated and affordable, and they are being adopted by a growing number of M&E companies.

Boldon: AI can be used to assist with large-scale identification of infringing behavior and has the prospect of significantly increasing the ability to spot unauthorized activity before it can cause significant economic harm. One of the promising applications is data analysis to identify patterns within large amounts, particularly in the areas of subscriber fraud and pirate infrastructure mapping.

Samsel: AI has a dual impact on M&E security. On the one hand, it aids pirates through advanced tactics like deepfakes for stealing account credentials and malware development. On the other hand, AI, in conjunction with machine learning (ML), plays a critical role in the defense against such threats, enhancing threat detection, network security, and predictive analysis. Although blockchain has not seen widespread adoption in video security, AI is increasingly being integrated with DRM systems to fortify anti-piracy measures.

MESA: *What do you see as the top threats with AI and M&E (deepfakes, cyber-attacks, etc.)?*

Samsel: The utilization of AI in reverse engineering poses a significant threat to the M&E industry, facilitating more sophisticated cyber-attacks that can bypass traditional security measures. The development and use of deepfakes for malicious purposes further exacerbate these security concerns.

Durand: While AI can be a helpful resource to aid content protection efforts, alternatively, it can be leveraged by pirates to exploit and steal content. For example, AI may be used to find new cybersecurity attacks that can also be exploited to steal content.

Boldon: AI is already being used by hackers enabling them to deploy more sophisticated attacks. AI for hackers means more automation and bigger reach thereby risking increasing the level of distribution of unauthorized content. ChatGPT is all about scaling — so imagine hackers using the tool to write code leading to a quicker spread of illicit sites.

Ultimately AI has the capability to facilitate access to a variety of technologies. ChatGPT is a public tool that we can benefit from and so can hackers - it can lower barriers for technicalities (coding or technical issues) and increase the agility of the hackers who will be able to move super-fast. [And with] generative AI, being able to identify when a creative work has been generated by AI is increasingly important. Misinformation, propaganda, cyberbullying, fake news, memes often make use of manipulated video and audio content to convey alternative narratives. A signpost to the user that content is a derivative work and has been manipulated in some way could become part of "nutrition labels" shown during the viewing experience.

Bhat: The threats with AI and M&E would be related to distinguishing false, fake attacks versus the real. The content distortion, editing of content with deep fakes which makes it difficult to identify the real one. The trained bots which mimic human behavior to get early access and circulate it illegally. Identifying deepfake automatically and combating the cyber-attack with AI/ML based would be a tug of war and industry would witness interestingly new algorithms and concepts being developed and deployed. As we all know the notorious characteristic of deepfake is damage reputation, spread misinformation and even unrest among countries it is need of the hour to invest heavily in AI/ML powered security solution and adopting best security practices with constant upgrades.

MESA: *Overall, what is the media and entertainment industry doing well in terms of content protection and cybersecurity, and what could we be doing better?*

Continued on page 8

Durand: The media and entertainment industry is very effective in establishing efficient rules, guidelines, or standards to help content owners or video service providers to better protect their content. As we look to the future, the industry should focus on their ability to quickly adapt to new threats and evolving pirate techniques.

Bielich: In the last 18-24 months we have seen a higher level of focus on anti-piracy, not only in live sports but also in on-demand content. More watermarking, more detection analysis, usage of track keys, key rotation during live sports, etc. We see governance challenges. Media security and IT/cybersecurity are often different responsibilities. Different security measures per product (i.e., it's the team's responsibility, rather than a coordinated effort) Result: lack of cybersecurity maturity in many media platforms.

We believe the M&E industry should be asking itself these questions: How is our cybersecurity for media addressed in our company? Do we have an overall security strategy & what is our maturity (reactive, defined, proactive or advanced)? Do we have the basics right?

Boldon: We are seeing better industry collaboration, in particular better coordination between M&E organizations and law enforcement and other regulatory bodies to share data and approaches when tackling piracy threats. In terms of areas of improvement, first, it's solutions' design that needs to be addressed. Security should be given a more prominent consideration when designing new platforms. Mandatory minimum standards should be adopted to ensure the most widely exploited vulnerabilities are no longer available for pirates to exploit. In addition, sustained programs need to be in place to educate those working within the industry on security best practices as well as practical day-to-day actions that can be taken to minimize impact of pirate attacks.

Pirates are technically and business savvy and are always looking for vulnerabilities and ways to monetize stolen content. For example, AVOD is increasingly popular with subscribers today, but pirates negate the monetization model by restreaming AVOD content with no ads to their own paying subscribers. They effectively turn legitimate AVOD into pirate SVOD and steal revenues and subscribers from the legitimate offerings.

Bhat: M&E [is] aware of the threat and losses due to piracy, preventing it with all possible technology and innovation is at its peak. Already de-facto multi-DRM with its vulnerabilities being identified, patches regularly, experimenting with different business models, developing standards to combat piracy. But there is still room for improvement such as automating the whole process of once the content is released or streamed, identifying the leaked content, reporting it for take down, identifying the source of the leak and blocking it at CMS level or CDN, is the need of the hour to effectively prevent piracy. The M&E industry is working together to improve cybersecurity. This includes sharing intelligence and developing new technologies to protect against cyber-attacks. ⊞