

**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



# You've got questions. **Box AI** has answers.


Unlock the value of your enterprise content  
Learn more at [box.com/ai](https://box.com/ai)



This report examines the current state of the media market and highlights key trends...







# A SECURE AI WORLD?

*Cover Photo by Maxim*

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 @ MESA

## SECURITY & CONTENT PROTECTION

- |   |  |
|---|--|
| <p><b>P. 24 What We Need for Better Security in M&amp;E</b><br/>By Mathew Gilliat-Smith @ Convergent Risks</p>  | <p><b>P. 40 Using Cloud-based Content Delivery to Keep Pace with Modern-Day Streaming</b><br/>By Chris Bardsley @ Vubiquity</p>    |
| <p><b>P. 26 Charting Legal, Security and Privacy Waters: AI's Role in Content Creation and Localization</b><br/>By Nicole Quilfen @ Mediartis, and Stephanie Iyayi @ Convergent Risks</p> | <p><b>P. 44 Cybersecurity and Content Protection: This is a Serious Issue!</b><br/>By Eutdel Garcia @ The Kitchen</p>              |
| <p><b>P. 28 Creating Secure Content in and Evolving Landscape</b><br/>By Pawan Anand @ Ascendion</p>  | <p><b>P. 48 AI: The Next Big M&amp;E Creative Adventure or a Fast-Approaching Security Headache</b><br/>By Tim Pearson @ NAGRA</p> |
| <p><b>P. 32 Protection the Supply Chain</b><br/>By Chris Williams @ Richey May Cyber</p>  | <p><b>P. 52 One Size Does Not Fit All. A Vendor Dilemma</b><br/>By Katie Pickrell @ Independent Security Evaluators</p>            |
| <p><b>P. 36 Securing Entertainment's Emerging Tech Stack</b><br/>By Derek Powell @ Altman Solon</p>   |  |



## CONTENTS

### THE VIEW FROM MESA

- P. 6 Automation and Integration:  
The Best Applications of AI**  
By Guy Finley @ MESA
- P. 8 AI and Security Converge**  
By Richard Atkinson @ CDSA
- P. 10 The Philosophy of Discovery**  
By Hollie Choi @ EIDR
- P. 12 Cloud Localization Blueprint:  
How to Make an Engaging Sequel**  
By Caroline Baines @ MESA
- P. 14 The Pillars of WiTH: A Year of Empowerment  
and Inclusion**  
By Christina Aquilera @ WiTH Foundation
- P. 16 The Worth of Data ... and the Cost**  
By Mary Yurkovic @ Smart Content Council
- P. 76 M&E Journal Ad Index**

### SMART CONTENT

- P. 58 AI Accelerating the M&E Content Supply Chain**  
By Dave Liu @ EPAM Systems
- P. 62 Change the (Custom) Script for Your Media  
Supply Chain with a No-Code Platform**  
By Dan Goman @ Ateliere Creative Technologies
- P. 64 Identity Forces**  
By Will Kreth @ HAND (Human & Digital)
- P. 66 The Psychology Behind Using Music in  
Video Games**  
By Emily E. Garcia @ RSG Media
- P. 70 Unlock the Value of Content with AI**  
By Jade McQueen @ Box



P. 66





gracenote  
a nielsen company

# *State of* **play**

*Insights on the future of  
streaming content discovery.*



*Read it here*

# TURNING TO COMMUNITY IN TIMES OF CRISIS

By Guy Finley, President, MESA



*Guy Finley is the founder, CEO, and president of MESA.*  
[guy.finley@MESAonline.org](mailto:guy.finley@MESAonline.org)  
[@MESAAlliance](https://www.instagram.com/MESAAlliance)

Whether you're down to scraping the muck at the bottom of the barrel — because you may have already scraped the bottom of the barrel mid-year — or you're off to the races and can't keep up with what's going on because you're so busy (maybe because one of your competitors bowed out), the industry challenges this year have been varied and nonstop.

A common phrase repeated over 2023 (frankly, since March 2020) is that “all bets are off” and “everything's on the table.” Everybody is running hard, and everybody is stressed. There's anxiety in the marketplace, no doubt about it, and we can't ignore it as a society. Where do you turn when you have that type of stress? You turn to your community, you turn to your family, you turn to your friends. Ultimately, that's what MESA is all about. Yes, we're a trade association or a group of trade associations, but we do things with a little bit more heart and/or emotion than others. I started MESA on a foundation of authentic community (when community wasn't as fashionable as it is these days ...) and when I look at the day-to-day work that Team MESA produces I am proud of our performance for these communities along with their natural engagement within the industry.

Again, the strength of our communities is what carries us through tough times. We have a passion about what we do, evidenced by those leading our communities: Content Delivery & Security Association (CDSA), Hollywood IT Society (HITS), Smart Content and Content Localisation Councils, Entertainment ID Registry (EIDR), and Women in Technology Hollywood (WiTH).

And MESA is the service provider um-

*IT'S THE STRENGTH OF OUR  
communities that carry us  
through the toughest times.*

brella that continues to serve our industry where we started with the Entertainment Supply Chain Academy (ESCA) events that kicked off in 2005. However our supply chain has only become increasingly complex and streaming only makes global delivery more complicated. But never has it been so important to drill down and get to these nitty gritty pieces that are redundant, inefficient, and can be supplemented with emerging technologies like AI. We famously stated over 10 years ago that what we do moved together by platform and API rather than by telephone, email, and spreadsheet. And, ultimately, when you think about that 15-year arc of where MESA began (MESA launched in February of 2009) and what we're all in the middle of now, it's exactly as we've predicted. Our industry is exactly as we've discussed within our communities, our working groups, our events, media, and casual conversation because our members have been at the forefront of transforming the supply chain from its home entertainment beginnings. Just like platform integration, MESA was the first to mention “data journey” a decade ago when nobody had their eye on the streaming ball, when FAST was still just AVOD. When we could still count unit pricings and measure our profit based on a title rather than on a subscription. When you think about what our member companies have done, who's

*Continued on page 77*



## **PUBLISHER**

**Guy Finley**

[guy.finley@MESAonline.org](mailto:guy.finley@MESAonline.org)

## **EDITORIAL**

### **EDITORIAL DIRECTOR**

**Chris Tribbey**

[chris.tribbey@MESAonline.org](mailto:chris.tribbey@MESAonline.org)

### **NEWSLETTER EDITOR**

**Jeff Hyatt**

[jeff.hyatt@MESAonline.org](mailto:jeff.hyatt@MESAonline.org)

### **TECHNOLOGY REPORTER**

**Jeff Berman**

[jeff.berman@MESAonline.org](mailto:jeff.berman@MESAonline.org)

## **DESIGN**

### **CREATIVE DIRECTOR**

**Heidi Antman**

[heidi.antman@MESAonline.org](mailto:heidi.antman@MESAonline.org)

### **DIGITAL DIRECTOR**

**Stanley Felix**

[stanley.felix@MESAonline.org](mailto:stanley.felix@MESAonline.org)

## **MEMBERSHIP**

### **SENIOR DIRECTOR, CLIENT SERVICES**

**Caroline Baines**

[caroline.baines@MESAonline.org](mailto:caroline.baines@MESAonline.org)

### **DIRECTOR, CLIENT SERVICES**

**Teresa Austerberry**

[teresa.austerberry@MESAonline.org](mailto:teresa.austerberry@MESAonline.org)

## **CONTACTS**

### **Sponsorships**

[sales@MESAonline.org](mailto:sales@MESAonline.org)

### **Logistics**

[operations@MESAonline.org](mailto:operations@MESAonline.org)

### **Association Management**

[management@MESAonline.org](mailto:management@MESAonline.org)

MESA is a community dedicated to shaping the media and entertainment industry's future. MESA's 150-plus members and content advisors collaborate to advance change management, new workflow solutions, and production/supply chain efficiencies. Launched in 2008 as Media & Entertainment Services Alliance, MESA produces quarterly events (in-person and hybrid), daily email newsletters, webinars, and the M&E Journal on behalf of its members. MESA is the management company responsible for the community efforts of Media & Entertainment Data Center Alliance (MEDCA), Hollywood IT Society (HITS), Smart Content Council, and Women in Technology: Hollywood (WiTH), as well as the business operations of the Content Delivery & Security Association (CDSA), the Entertainment ID Registry (EIDR) and the WiTH Foundation.

For more information, visit [mesaonline.org](http://mesaonline.org)

▣ Bringing Ideas Into Action

# AI AND SECURITY CONVERGE

By Richard Atkinson, President, CDSA



*Richard Atkinson is president of CDSA, and his experience covers more than 15 years in classified defense and 23 years in M&E senior leadership positions, driving profound business revenue and change for Northrop Grumman, Disney, EA, and Adobe.*

[ratkinson@CDSAonline.org](mailto:ratkinson@CDSAonline.org)

“AI and Security Converge” is not just the theme of the Content Delivery & Security Association’s (CDSA) Content Protection Summit. Artificial intelligence is also increasingly impacting every one of us in a multitude of ways. It is making things better and easier than was ever possible before.

When you can take large components of the world’s information, index it and be able to assemble it in amazing ways, and link that with very simple and easy to use interfaces to access all this in seconds it’s simply amazing. I don’t mean doing things faster. I’m saying most things that AI is now enabling were literally not possible outside a lab and at scale before, and now it is not just possible, it is easy and almost instant.

When we then look at how AI is impacting security and aspects of fraud (in a broad context), there are both positive and negative aspects emerging, and here is a list of just a few categorical areas we were seeing AI impact today:

## Cybersecurity:

■ **Threat detection:** AI is used to detect and prevent cyber threats. Machine learning models can analyze large datasets to identify patterns and anomalies indicative of malicious activity.

■ **Anomaly detection:** AI can identify unusual network or user behavior that might be a sign of a security breach.

■ **Predictive analysis:** Machine learning models can predict future threats based on historical data and trends.

■ **Malware detection:** AI-powered anti-virus and anti-malware tools can quickly identify and mitigate new and evolving malware strains.

*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.*

## Network security:

■ **Intrusion detection and prevention:** AI helps in identifying and responding to network intrusions in real-time, protecting sensitive data.

■ **Firewall management:** AI can optimize firewall rules and configurations, reducing vulnerabilities.

## Physical security:

■ **Facial recognition:** AI-driven facial recognition systems are used for access control, video surveillance, and identifying individuals in real-time.

■ **Object detection:** AI can be used to identify objects or anomalies in security camera footage.

## Biometric security:

■ AI plays a crucial role in biometric security, such as fingerprint recognition and voice authentication.

## Fraud detection:

■ AI algorithms can analyze financial and transaction data to detect fraudulent activities in banking and e-commerce.

*Continued on page 81*



# ACCELERATING THE NEW ERA OF ENTERTAINMENT

End-to-end services for all content types;  
we can deliver anywhere, anytime



Your #1 Partner for  
all Content Services

---

[WWW.BYDELUXE.COM](http://WWW.BYDELUXE.COM)

@DELUXE1915

Localization

Cinema

Distribution

Mastering

Packaging & More

# THE PHILOSOPHY OF DISCOVERABILITY

By Hollie Choi, Managing Director, EIDR



*Hollie Choi is the executive director of the Entertainment ID Registry (EIDR). During her 15-plus years in media and entertainment she's become an expert in supply chain automation, metadata governance and workflows, and digital and media asset management systems.*  
[hchoi@EIDR.org](mailto:hchoi@EIDR.org)  
[@eidrdotorg](https://twitter.com/eidrdotorg)

Years ago, it was common to hear studio executives talk about their visions for an automated digital supply chain that would result in an individualized experience. They would reference a not so far-off future where the need for a content super-supply-chain (nobody ever called it that, I'm just illustrating a point) would be needed. In this vision, they foresaw the need to deliver to a growing consumer market around the world. The individual experience of the consumer was of the utmost importance. The ability to intuit (with predictive analytics and data science) what each and every one of the billions of people on Earth would want to watch would be the distinguishing factor between the studios' survival or it's impending death.

It sounds dramatic, but if there's one thing that has stayed the same in this industry, it's that everybody loves a good dramatic story with a major plot twist. During the early days of quarantine, while our customers were home learning a second language or taking up a musical instrument, they were also watching more content than ever. Intriguingly, mobile consumption skyrocketed. Even though people were in their homes with their huge beautiful flat screen televisions, they were choosing to watch content on their phones.

Quarantine also saw an explosion in the number of streaming services available so individuals could watch any content, anytime, anyplace, and apparently on tiny screens they held in their hands. The demand for new content increased even though the studios were not producing new content because production was also halted. What is a studio to do when they need to stream enormous amounts of content and they can't make new content? They dug through their catalogs to see what they had that could be redistributed. Knowing where the content is kept and knowing if they have the rights to distribute in any given territory is only part of the battle. There are any number of accompanying assets that go

*THESE DAYS, A LOT OF conversations about the future are centered around content discoverability. How can we help viewers to navigate the streaming landscape, anyplace, anytime, on any device? How can we ensure that the content they want is available? How can we improve the overall experience that streaming customers are having?*

along with the payout files. The process for delivering old content can be as complex as delivering new content. It relies on the quality of the metadata that people in the past associated with the files.

Archiving and metadata-tagging media files is practically an art form, and it is often done in bulk and a lot of times it is done by vendors. Imagine determining which content you have the rights to distribute, then sifting through millions of files to find the specific episodes and versions of a television show that was made before the turn of the century and then going through all the motions to authorize it for distribution either to your platform or to the platform of a distribution partner. Asset level metadata (including the EIDR ID) needs to be clean for the supply chain to function properly.

All of this is to say, it can be terribly difficult to find content that you control while it is still

*Continued on page 72*



# RETHINK EVERYTHING YOU KNOW ABOUT LOCALIZATION



## TRUSTED BY THOUSANDS OF USERS IN OVER 100 COUNTRIES



### OOONA MANAGER

A cloud-based management system  
for localization companies



### OOONA API

Enterprise integrations  
into your management platform,  
so the functionality you require becomes  
a seamless part of your workflow



### OOONA TOOLS

Professional production tools  
for the media localization industry



### OOONA EDU

A cloud-based platform  
specifically designed for media  
localization training purposes



### OOONA INTEGRATED

An online management platform integrated with a complete set of tools  
for an end-to-end media localization experience



OOONA.NET

# CLOUD LOCALIZATION BLUEPRINT TAKE 2: HOW TO MAKE AN ENGAGING SEQUEL

By Caroline Baines, Senior Director, Client Services, MESA



*Caroline Baines is the senior director of client services for MESA. She joined MESA Europe in 2018, as director of operations following a 20-year career in research and consulting within the media, entertainment, and technology sector. In her current role she oversees the European community, helping to raise the profile of members by providing various platforms for collaboration, networking and thought leadership. She is also director of the Content Localisation Council and secretariat for the Content Delivery & Security Association (CDSA). [caroline.baines@MESAonline.org](mailto:caroline.baines@MESAonline.org) @MESAAlliance*

Since its inception in 2016, MESA's Content Localisation Council has been pivotal in helping to raise the profile of audio-visual translation and dubbing across the industry. Through council meetings, events, workshops and taking part in third party conferences such as Languages and The Media and Media For All we continue to bring this vibrant community together to share learnings and best practices.

And in line with its mission statement, the Content Localisation Council continues to set a high bar by working on initiatives which will bring benefit to the entire industry.

One such initiative which holds enormous potential is the Cloud Localization Blueprint (CLB). Originally showcased during IBC 2022 as part of its Accelerator Programme, this project brought together supply chain software companies to create a definitive blueprint for distributing entertainment content globally.

By looking at the entire supply chain from licensing through to localization and final delivery, the blueprint seeks to build a global, cloud-based media supply chain for content localization. The resulting proof of concept was a resounding success and proved what could be achieved when like-minded companies with a shared vision worked together. MESA's sister organizations EIDR and the Language Metadata Table (LMT) played a key role in the original project and their expertise will prove vital for this next chapter.

When Fabric, a major data solutions provider in the M&E industry, approached us in the summer to ask if MESA would like to become the custodians of the CLB website, we leapt at the opportunity. Here at MESA, we recognize the need for this work to continue and we have the community that can

*SO, WHAT'S THE NEXT STEP? We are just getting started on this new journey and want to encourage our localization community to get behind the initiative and help us to drive it forward.*

make it a reality. Helping drive the project alongside the Content Localisation Council is Hollie Choi, managing director of EIDR and Mary Yurkovic, director of MESA's Smart Content Council. Choi was pivotal in driving the first CLB and will once again bring her significant industry knowledge and experience to this next iteration, while Yurkovic, a highly regarded technology strategist, has worked with many major media companies using her in-depth understanding of technology, content, and digital workflows to implement successful solutions.

In this next project the Cloud Localization Blueprint II will engage with the industry to continue to discuss a range of challenges and suggest solutions and offer guidance on best practices. For example, the use of AI in localization will touch and integrate across all players, be they large or small. However, if the sector is to take advantage of the benefits of AI it needs to fully embrace and prepare for greater workflow automation. And this workflow will have to begin further upstream as localization, due to collapsing windows and global day and date across streaming platforms, moves into production.

Audio-visual translation will continue to

*Continued on page 72*



EMPOWERING ACCESS TO GLOBAL MEDIA

---

Cut.  
Print.  
Wrap.  
Store.



When Legendary Studios  
assembles films quickly and  
cost effectively, Wasabi  
plays a starring role.



LEGENDARY



**wasabi**  
hot cloud storage

# THE PILLARS OF WITH: A YEAR OF EMPOWERMENT AND INCLUSION

By Christina Aguilera, President, WiTH Foundation



*Christina Aguilera is president of the WiTH Foundation.  
[hello@WiTHollywood.org](mailto:hello@WiTHollywood.org)  
[@WiTHollywood](https://twitter.com/WiTHollywood)*

In the world of media and entertainment technology, where innovation creates magic on screen, there's an even more enchanting story behind the scenes – a story of empowerment, equity, and inclusion. Women in Technology: Hollywood (WiTH) Foundation is at the forefront of this transformative narrative, and as we look ahead to the year to come, we are excited to share our accomplishments from the past year and the path we are forging towards a brighter future.

## *WiTH's Pillars of Action*

At the heart of WiTH's mission are three pillars of action that drive our efforts:

**Professional development:** WiTH is committed to leveraging our resources to broaden the collective expertise of women in technology. Through various initiatives, we empower our members to continually expand their skills and knowledge.

**Mentoring and networking:** Connection, inspiration, and encouragement are the cornerstones of WiTH's mentoring and networking initiatives. We believe in fostering growth in our professional network and providing mentorship opportunities to support the careers of women in technology.

**Community engagement:** WiTH members are avid ambassadors of technology, and we are dedicated to encouraging youth, particularly girls and women, to pursue careers in our field. Through community outreach and partnerships with non-profit organizations, we are making a difference in the lives of aspiring technologists.

## *Making a difference: Lifting all aspirations*

At WiTH, we firmly believe that lifting the

aspirations and careers of one raises all. Our organization stands for:

**Curiosity:** We encourage exploring paths to fuel learning and growth, constantly pushing the boundaries of what is possible.

**Belonging:** WiTH celebrates and respects our differences while making space where we can unleash our unique genius. We believe that every voice matters, every identity is celebrated, and we create an inclusive environment where everyone can thrive.

**Leadership:** WiTH is about blazing new trails to confidence, courage, vision, and joy. We empower women to become bold leaders in the world of technology.

## WITH EVENTS: CONNECTING AND INSPIRING

Throughout the year, WiTH members gather at various events to connect, inspire, and drive our mission forward. Here are some of our key events:

■ **WiTH Leadership Awards:** These awards honor contributors who serve as role models and mentors, empowering women to be bold leaders in technology.

■ **SoCal Women's Leadership Summit:** This event is designed to inform and inspire members around issues vital to the community, creating a platform for discussion and action.

■ **WiTH Workshops:** We host periodic educational and interactive events featuring keynote speakers and round table discussions with industry leaders, both in-person and online.

*Continued on page 72*



# STREAMING AT SCALE REQUIRES ZIXI

Amplify your video streaming potential with Zixi's revolutionary **Software Defined Video Platform (SDVP®)** powered by the **Zixi Protocol** and the **ZEN Master** control plane.

In the dynamic world of video streaming, media organizations are constantly seeking efficient and cost-effective solutions to manage their large-scale implementations. Solutions that utilize an Open-Source Protocol are assumed to be the most cost effective, but when fully analyzed are very expensive and inefficient. Zixi's SDVP features breakthrough innovations in both bandwidth optimization and compute requirements that significantly reduce your egress cost and cloud instances resulting in exponential savings especially at large scale implementation making Zixi the most cost effective and lowest total cost of ownership in the industry. This enables media companies the ability to allocate their resources more efficiently, redirecting budgetary allocations to other areas including new content acquisition for new business and opportunities to generate revenue.

Zixi's SDVP is your only choice when deploying large scale IP workflows over any IP network, any protocol, any cloud provider, and any edge device.



Learn more at [www.zixi.com](http://www.zixi.com)



# THE WORTH OF DATA ... AND THE COST

By Mary Yurkovic, Director, Smart Content Council



*Mary Yurkovic is the director of MESA's Smart Content Council. She has more than 15 years' experience in the publishing, entertainment, and technology sectors. [mary.yurkovic@MESAonline.org](mailto:mary.yurkovic@MESAonline.org) @chicagoMY*

In the dynamic landscape of the M&E industry, data is the modern-day goldmine. As technology and innovation continue to reshape the way content is produced, distributed, and consumed, the value of data has never been more apparent. From content recommendation algorithms to audience insights, data has become the driving force behind innovation and success for M&E companies or any organization for that matter.

However, what is the worth of data? Why does it matter? How can it empower the studios to stay ahead in the industry? But most importantly, are organizations being responsible with the data?

The benefits of data are obvious and worth a rundown:

**Personalized content delivery.** In the era of on-demand streaming services, one size no longer fits all. Data enables companies to understand their audience on a granular level. By analyzing user preferences, viewing history, and demographic data, companies can offer personalized content recommendations. This not only enhances the user experience but also keeps subscribers engaged and loyal. By effectively delivering personalized content, you can keep their viewers coming back for more and more, leading to higher subscription rates and increased revenue.

**Content creation and curation.** Data-driven insights are invaluable when it comes to content creation and curation. Studios can use data to identify trending topics, understand what type of content resonates with specific audiences, and even predict future trends. This information empowers them to make data-informed decisions about what content to produce and how to position it in the market. By effectively using data for content creation and curation, companies can minimize the risk associated with

*M&E COMPANIES MUST handle data with care, respecting privacy, security, ethical considerations, and data quality. As technology continues to evolve, the worth of data will only grow, making it a valuable asset in an ever-evolving industry.*

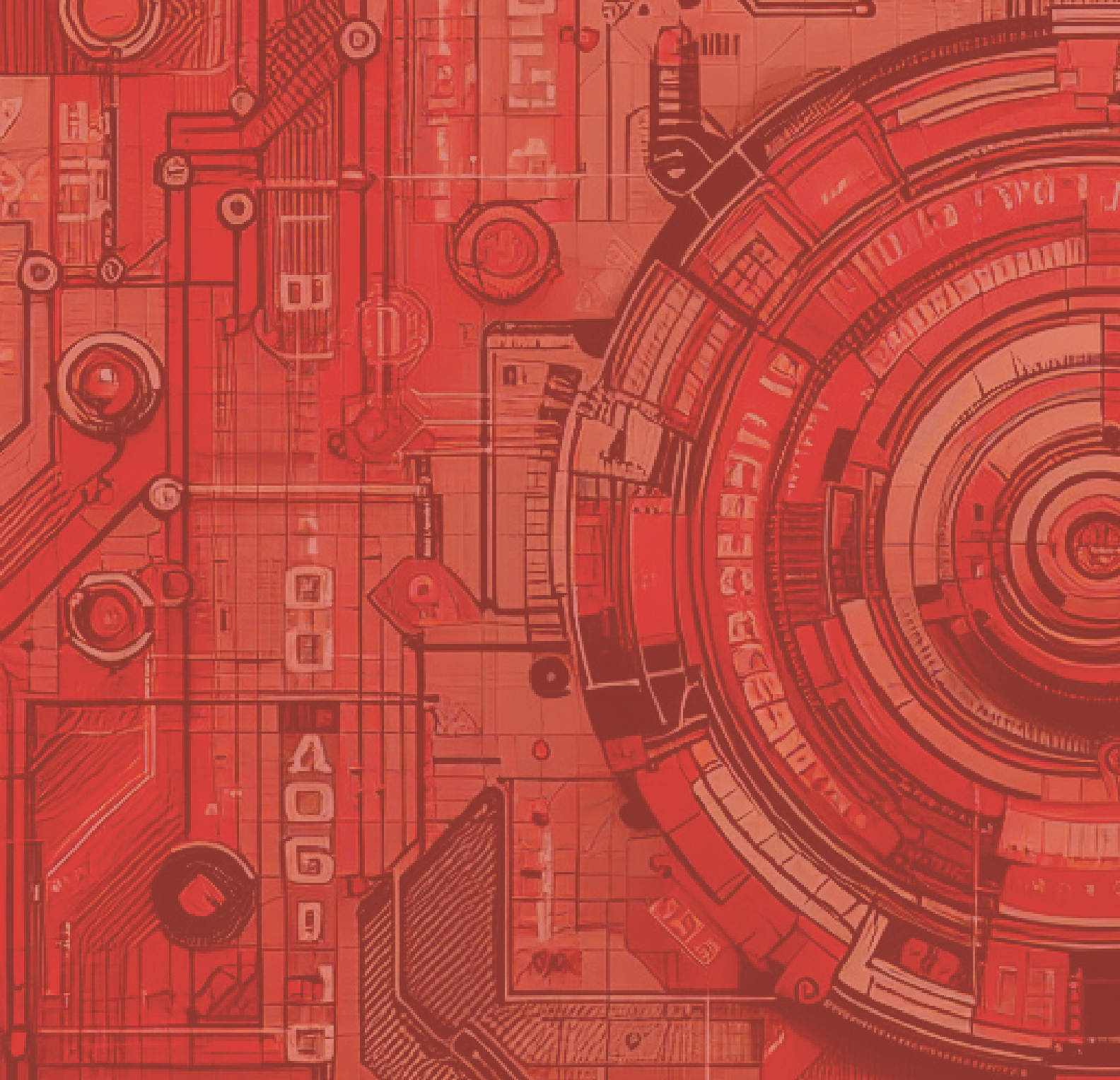
producing content that might not resonate with viewers, ensuring a higher return on investment. That's the very definition of Smart Content.

**Improved advertising.** Advertisers and marketers are increasingly relying on data to target their campaigns effectively. All companies have access to a wealth of user data, which can be leveraged to provide highly targeted and relevant advertising. This benefits both advertisers, who reach their ideal audience, and consumers, who see ads that align with their interests. By effectively utilizing data for advertising, companies can attract more advertisers and generate higher ad revenue, contributing to their bottom line.

**Content optimization.** Companies can use data to optimize their content libraries. By tracking viewer engagement and feedback, they can make data-driven decisions about which content to invest in, renew, or retire (maybe to be used later!). This approach minimizes the risk of producing content that doesn't resonate with the audience and allows companies to allocate their resources more effectively. Again, when data and con-

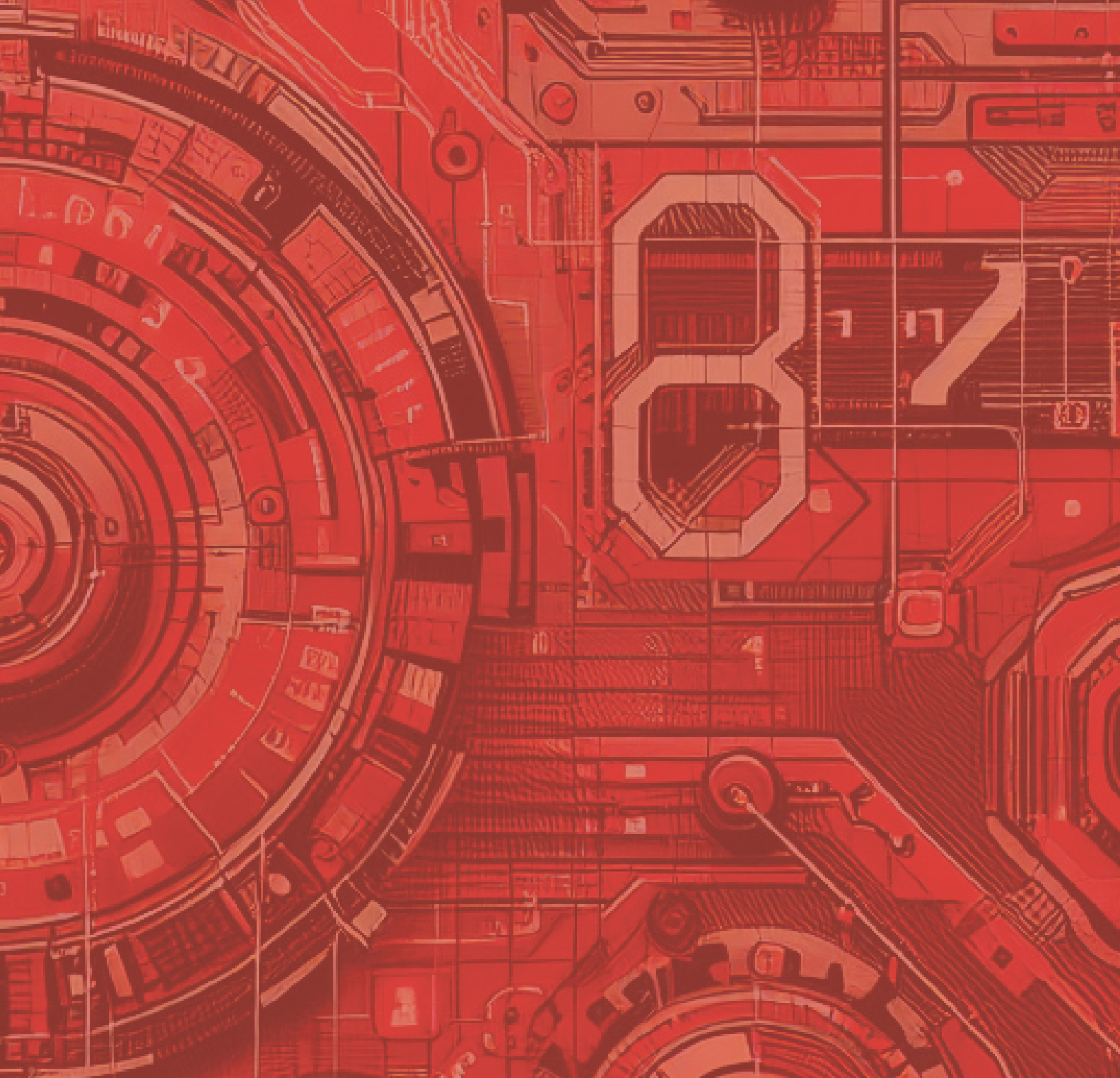
*Continued on page 82*

**MAKING LIFE  
EASIER FOR THE  
PEOPLE WHO  
ENTERTAIN THE  
WORLD.**



# 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](mailto: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 solu-

tions 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:** Streaming 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 (deep-fakes, 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 79*



# WHAT WE NEED FOR BETTER SECURITY IN M&E

Employ a holistic approach,  
instead of relying solely on one  
defensive measure



**ABSTRACT:** General security posture in the M&E supply chain is the highest it has ever been, but is it good enough? Leaks still happen and cyberattacks are becoming more prevalent. There's more to be done beyond meeting the minimum best practice. Being proactive and vigilant will save time and cost in the long run.

**By Mathew Gilliat-Smith, EVP, CRO,  
Convergent Risks**

We are at least now preaching to a converted audience. Gone are the days when security was an afterthought or was not a line item in the annual budget. It helps that a key driver for vendor security in M&E is the requirement by content owners for industry compliance, such as the TPN, SOC2, ISO and testing. Increasingly this is the hurdle to win and maintain business.

The threat landscape is continually evolving and becoming more complex and expensive to manage. It's therefore crucial that our knowledge is current and that we are in tune with the latest threats. The challenge will always be that attackers only need to find one vulnerability, while their targets must protect against all. In addition to following best practice, the best way to do this is by implementation of cybersecurity tools testing and information sharing.



Aside from attackers, human error is often the cause of an unintended leak or breach. Either way continuous education with regular training sessions on security awareness can significantly reduce the risk, for example on the latest phishing and social engineering tactics.

A holistic approach is beneficial and instead of relying solely on one defensive measure. We should adopt a layered approach to security that encompasses various tools and practices, including the obvious ones, such as endpoint security, network monitoring, stronger access control, advanced encryption in transit and at rest, secure collaboration platforms, correctly configured cloud storage, plus a meaningful incident response strategy.

There are hundreds of vendors and thousands of individuals working on each new production with an increasing use of SaaS applications. When a solutions provider detects a potentially exploitable vulnerability and issues a software patch, it's incumbent upon their customers to install it. Patch alerts signpost attackers to find exploitable wins. Tightening obvious gaps in all areas is crucial to ensure better security during on-set production and during post-production.

One size does not fit all however, and different content owners will have different security requirements depending on the vendor and the content. The MPA Best Practice Guidelines provide a sound security baseline upon which a delta set of checks and balances can be added. An iterative rather than a duplicative approach to the security assessment process must be much more productive and time efficient for all parties. It was encouraging to see a united front in the approach to the security assessment process at the IBC 2023 TPN panel, which was represented by most of the studios and watched by a good cross section of vendors and assessors.

There has been a lot of concern recently in the media about AI and how we might lose control of it. Apart from the fact that AI has been around for a while in various forms, it is beneficial to both offensive and defensive security strategies. For example, AI where it helps with anti-piracy by recognizing copyrighted material and alerting rights holders for take down. Forensic

**TIGHTENING OBVIOUS GAPS  
in all areas is crucial to  
ensure better security during  
on-set production and during  
post-production**

watermarking tools use AI for tracing back content to its original source. Natural language processing can read the web for references to pirated or unreleased content, acting as an early warning system.

In cybersecurity, AI can be used in anomaly detection indicating potential threats. Use of AI in behavioral analysis can help with malware detection. AI can recognize the characteristics of phishing emails and identify previously known threats. Deepfakes are increasingly hard to spot, and detection is made easier through AI.

On the downside AI can also be used for all the above to empower bad actors to generate deepfake videos, more sophisticated phishing and malware attacks, circumvention of passwords and so on. This is all on top of privacy concerns, the loss of jobs and all the rest.

In terms of what more we do to protect our businesses from cyber criminals, we can make more effort to stay current with the new or improved technologies out there. For example, ZDA (zero trust architecture) forces the concept of never trust and always verify on every access request. XDR (extended detection and response) which provides a suite of security products that automates threat detection and response across endpoints, networks, servers, and cloud environments. Improved MFA and password manager technology that both strengthens and simplifies the authentication for end users.

All of the above however is contingent on proper implementation, continuous updates, vulnerability management, security assurance and testing, and as importantly it has a holistic understanding of the security posture of your business.

Sapiens qui prospicit. Wise is he who looks ahead. ■



*Mathew Gilliat-Smith is the EVP and CRO of Convergent Risks. He has 20-plus years of experience in the media and entertainment sector with strong relationships at many levels within studios, broadcasters, and supply chain vendors. He is responsible for developing Convergent's initiatives in cloud and application security, threat assessment penetration testing and general consultancy. He also manages many of Convergent's corporate and business growth strategies, including the promotion of the TPN initiative. He was previously founder and CEO of a software development business focusing on video encryption solutions. [mathew.gilliat-smith@convergentrisks.com](mailto:mathew.gilliat-smith@convergentrisks.com) @ConvergentRisks*

# CHARTING LEGAL, SECURITY AND PRIVACY WATERS: AI'S ROLE IN CONTENT CREATION AND LOCALIZATION



**Achieving a balance between automation and safeguarding sensitive information is crucial**

**ABSTRACT:** The adoption of AI in content creation and localization operations poses significant legal, security and data privacy risks. Concerns center around copyright infringement, mishandling of personal data, and vulnerabilities to cyber threats. Achieving a balance between automation and safeguarding sensitive information is crucial for ethical and legal compliance in AI-driven processes.

**By Nicole Quilfen, COO, Mediartis,  
and Stephanie Iyayi, SVP,  
Legal, Privacy, Convergent Risks**

The media and entertainment industry is witnessing a revolution with the integration of artificial intelligence in content creation and localization. AI-powered algorithms can now generate written content, translate languages, and even voice-act in multiple languages. The appeal lies in speed, consistency, and cost-efficiency, but the transition is not without its share of challenges.

The adoption of AI in content creation and localization operations poses significant legal, security and data privacy risks. Concerns center around copyright infringement, mishandling of person-

**THE ADOPTION OF AI IN CONTENT creation and localization offers transformative benefits but carries a profound responsibility to address legal, security, and data privacy risks. Concerns surrounding copyright infringement, data mishandling, and vulnerabilities to cyber threats demand meticulous attention.**

al data, and vulnerabilities to cyber threats. Achieving a balance between automation and safeguarding sensitive information is crucial for ethical and legal compliance in AI-driven processes.

### REGULATORY LANDSCAPE

AI has given governments and policy makers a lot to grapple with. Several high-level questions are now being debated:

- *What interests should AI regulations protect?*
- *Should existing regulatory structures be adapted or new ones put in place?*
- *How should regulatory burdens be kept proportionate?*
- *What role should central government play?*

The EU is taking a leading role in the development of AI-specific regulations with a proposal for harmonized rules on artificial intelligence and amending certain Union legislative acts (the “AI Act”). The AI Act proposes broad-brush rules designed to ensure AI systems are sufficiently safe and robust before they enter the EU market. This includes banning certain prohibited AI practices outright and defining a new category of high-risk AI systems to which granular responsibilities, obligations and duties apply.

In contrast to developments in Europe, the UK has decided against creating a single regulatory function to govern AI, stating that AI is a general-purpose technol-

ogy having applications in many industry sectors. Instead, the UK issued a white paper setting out principles to support existing regulators, such as the Information Commissioner’s Office (ICO, the UK’s privacy regulator) and the Financial Conduct Authority (FCA), to develop a bespoke approach for AI development and use within their sectors.

The regulatory framework for AI in the United States involves multiple federal and state agencies, and there isn’t a single comprehensive law dedicated solely to AI regulation. Instead, AI is subject to a patchwork of existing laws and regulations that may apply depending on the specific use and impact of the technology.

### LEGAL CONSIDERATIONS

Perhaps the most prominent legal concern in AI-driven content creation is copyright infringement. AI algorithms trained on vast databases may inadvertently generate content that closely resembles copyrighted material. This poses a risk to both creators and organizations that utilize AI-generated content. To mitigate this risk, organizations should implement robust copyright checks and educate their AI models on intellectual property rights, emphasizing the importance of original content creation.

AI systems also encounter complexities in navigating licensing agreements and fair use policies. While AI can assist in content creation, it must operate within the

*Continued on page 78*



*Nicole Quilfen is the chief operating officer of Mediartis. She comes from a business development background specializing in international strategy, personal data protection, and accompanying media and entertainment professionals with their operational privacy strategies. [nicole@mediartis.com](mailto:nicole@mediartis.com) @Mediartis\_*



*Stephanie Iyayi is the senior vice president of legal and privacy for Convergent Risks. She comes from a legal background specializing in privacy and data protection and advises clients on all areas of UK, EU, and international data protection law, from general privacy compliance to risk management issues, including compliance implementation, privacy impact assessments, data breach incidents, cross-border data transfers, employee monitoring and data subject access requests. [info@convergentrisks.com](mailto:info@convergentrisks.com) @ConvergentRisks*



# CREATING SECURE CONTENT IN AN EVOLVING LANDSCAPE

**Blockchain, DRM, and AI form a  
robust trio in content protection  
for the industry**

**ABSTRACT:** We are streaming content on the fly. Content consumption has become synonymous with videos in most cases. All of these lead to one main challenge for the media and entertainment industry: cybersecurity. In 2022, a minimum of one data breach per month was reported by over 80 percent of the organizations globally. Digital technologies are transforming the M&E industry, redefining content production, distribution, and consumption. This fundamental change requires renewed focus on cybersecurity and content protection.

**By Pawan Anand,  
Engagement Partner,  
Communications,  
Media and Entertainment  
(CME), Ascendion**

Amidst a dynamic and ever-changing landscape, the media and entertainment industry is experiencing significant transformation. This shift is primarily driven by the profound impact of digital technologies, which have not only redefined but also completely revolutionized content production, distribution, and consumption. These extensive changes are reshaping how the industry functions and placing a renewed focus on the crucial areas of cybersecurity and content protection. As the M&E industry undergoes a fundamental change in how content is created, delivered, and consumed, it becomes essential to assess the tools and strategies in use to safeguard the industry's core.

## **CONTENT PROTECTION: SECURING DIGITAL ASSETS**

Protecting creative assets, intellectual property, and confidential pre-release content in the entertainment industry is challenging in the digital age.

**THE RAPID GROWTH OF ONLINE CONTENT DISTRIBUTION** and consumption has ushered in a new era of convenience and accessibility, but it has also opened the floodgates to rampant piracy and cybersecurity threats. The M&E industry is increasingly relying on AI as a powerful weapon in its arsenal to counter these challenges. AI's ability to detect piracy, protect digital assets, and fortify cybersecurity measures has become a cornerstone in safeguarding creative content and intellectual property.

*Why?*

Because digital piracy is constantly evolving.

*What can be done?*

Enterprises can invest in cutting-edge technologies like AI and blockchain. These technologies can help to monitor and defend against anomalies in real time, reinforcing the industry's commitment to safeguarding creative assets.

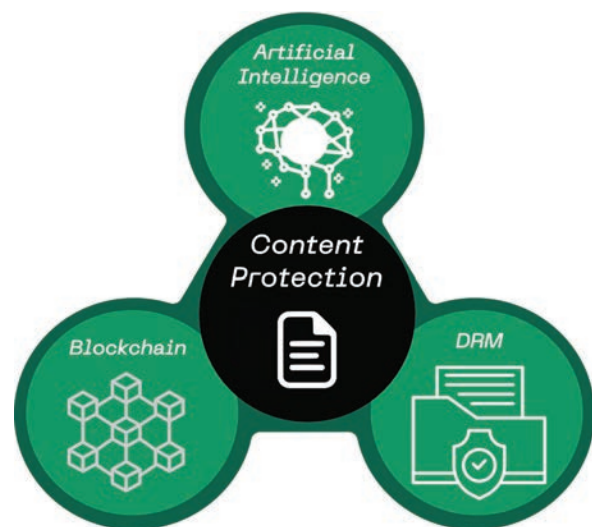
Blockchain, DRM, and AI form a robust trio in content protection for the M&E industry as they enhance security and control over digital assets.

Enhancements in digital rights management (DRM) solutions grant content creators and distributors better control over content access and distribution, safeguarding their intellectual property. While progress has been made, there is still room for improvement in vital areas.

Continued investment in cutting-edge technologies is essential to protect content in the ever-evolving content distribution landscape.

Blockchain plays a central role in DRM by creating an immutable ledger of content ownership and rights. It transparently records content creation and rights assignments, reducing ownership disputes. Smart contracts, powered by blockchain, automate DRM rules for efficient content access and sharing control, reducing violations. This decentralized approach minimizes vulnerabilities associated with centralized DRM systems.

AI strengthens content protection by enabling ad-



*The combination of AI, DRM and blockchain technologies results in a robust content protection solution.*

vanced threat detection, piracy pattern recognition, and predictive analysis to anticipate future vulnerabilities. AI also monitors user behavior for insider threats and enhances user authentication with multi-factor verification and biometrics. This blend offers a comprehensive approach to content protection. It safeguards intellectual property rights, reduces piracy risks, and reinforces cybersecurity, ensuring a thriving future for content creators, distributors, and consumers alike.

Collaborative efforts among stakeholders are crucial for a stronger ecosystem against piracy. Securing the entire content creation and distribution chain, including



*Pawan Anand is the engagement partner for Ascendion's Communications, Media and Entertainment (CME) division. His role as a technology leader at Ascendion includes overseeing client relationships, engagements, business development, and sales. His deep understanding of the industry and its evolving landscape enables him to introduce cutting-edge technology solutions that have a transformative impact on clients' outcomes. He is responsible for bringing technology offerings to provide transformational experience to drive business results for CME clients. [pawan.anand@ascendion.com](mailto:pawan.anand@ascendion.com) [linkedin.com/in/pawan-anand/](https://www.linkedin.com/in/pawan-anand/)*

third-party vendors, is essential. Reinforcing cybersecurity is vital. User education, awareness, and training programs are imperative. Regulatory compliance is essential to safeguard content and mitigate legal issues in the dynamic digital landscape.

### EMBRACING THE AGE OF OTT AND STREAMING: TRANSFORMATION IN THE M&E INDUSTRY

Across the world, over 3.5 billion people use video OTT services. That's a little less than half of the world's population. This OTT evolution revolutionizes content delivery, consumption, and industry dynamics. The convenience of accessing content on streaming platforms has heightened piracy risks, enabling the effortless capture and distribution of content, while the global reach of these platforms complicates the enforcement of copyright and content protection across multiple jurisdictions.

Efforts to combat piracy should be fortified through the deployment of advanced technology to detect and counter illegal content distribution, coupled with global cooperation involving governments and law enforcement agencies to effectively address cross-border piracy. Investments in secure streaming technologies create formidable barriers that make it increasingly challenging for pirates to capture and redistribute content. Alongside these technical measures, raising awareness among consumers about the detrimental effects of piracy on the industry and the creative community is an essential component in the battle against this pervasive issue.

### CYBERSECURITY IN THE M&E INDUSTRY

Cybersecurity plays a vital role in protecting content in the M&E industry. The evolution of technology introduces new threats and vulnerabilities, necessitating constant vigilance and adaptation.

Improving cybersecurity in the M&E industry involves several key strategies:

■ **Advanced threat detection:** Utilize AI and machine learning for advanced threat detection, identifying patterns and anomalies in network traffic and user behavior.

■ **Cloud security:** Secure cloud-based storage and distribution platforms with strong encryption, access controls, and continuous monitoring.

■ **End-to-end encryption:** Implement end-to-end encryption to protect content throughout its journey, from creation to consumption.

■ **Regular security audits:** Conduct regular security audits to identify vulnerabilities and address them promptly.

■ **Incident response planning:** Develop comprehensive incident response plans to minimize the impact of security breaches and ensure an effective response.

■ **Zero-trust architecture:** Implement a zero-trust security model, where trust is never assumed, and every device and each user is thor-

oughly authenticated before gaining access to resources.

In navigating the dynamic cybersecurity landscape, a culture of continuous adaptation is vital.

Collaborative efforts with experts, technology providers, and government agencies are critical for sharing threat intelligence. Investment in cutting-edge cybersecurity technology is vital for proactive defense. User education plays a pivotal role, as informed users and employees are the first line of defense. Compliance with data protection regulations is essential, avoiding legal consequences and reinforcing cybersecurity practices. Together, these strategies enhance the industry's proactive cybersecurity stance.

### THE SIGNIFICANCE OF AI IN COMBATING PIRACY AND ENHANCING CYBERSECURITY

The rapid growth of online content distribution and consumption has ushered in a new era of convenience and accessibility, but it has also opened the floodgates to rampant piracy and cybersecurity threats. The M&E industry is increasingly relying on AI as a powerful weapon in its arsenal to counter these challenges. AI's ability to detect piracy, protect digital assets, and fortify cybersecurity measures has become a cornerstone in safeguarding creative content and intellectual property.

■ **Content and pattern recognition:** AI plays a crucial role in content protection by analyzing and recognizing copyrighted content, facilitating the detection and prevention of unauthorized distribution. Additionally, AI algorithms are proficient in identifying piracy patterns like watermark removal or screen capture, allowing for swift and decisive actions against infringement.

■ **Automated takedown:** AI-driven systems can efficiently and automatically issue takedown notices to infringing platforms, significantly reducing response time, and improving content protection.

■ **Predictive behavior analysis:** AI offers two significant capabilities in cybersecurity. Firstly, it monitors user behavior to detect anomalies, aiding in the identification of potential pirates and insider threats. Secondly, AI employs predictive analysis, utilizing historical data and emerging trends to anticipate future cybersecurity threats and vulnerabilities.

■ **Threat and anomaly detection:** AI, specifically machine learning, excels at swift threat detection in cybersecurity. It analyzes massive real-time data volumes, enabling quicker responses compared to traditional methods. Machine learning models excel at identifying abnormal patterns and behaviors across networks and systems, serving as an early warning system for potential security breaches.

In conclusion, the state of cybersecurity and content protection in the M&E industry is at a critical juncture. While progress has been made, new challenges brought about by streaming-first distribution and rapidly evolving technology demand continuous vigilance and innovation. The industry must embrace integration of blockchain,

*Continued on page 72*



# Localize to Globalize

Unleash your content and **connect**  
with **global audiences** through  
**high-quality localization**

[www.vsi.tv](http://www.vsi.tv)



# PROTECTING THE CONTENT SUPPLY CHAIN



**By following best practices, any organization can be prepared to fend against cyberattacks**

**ABSTRACT:** Every day, the world depends on the supply chain of products and services for everyday tasks. How can organizations ensure that content shared with third parties stays safe? What is the impact of having a weak cybersecurity posture in your content supply chain, and how can these risks be mitigated? This article will examine the risks inherent in the content supply chain and identify best practices to defend your supply chain against potential risks.

**By Chris Williams,  
Senior Cybersecurity Consultant,  
Richey May Cyber**

The content supply chain involves creating, managing, and distributing digital content across various platforms and channels. Content can include documents, images, videos, audio, software, data, and more. Third parties, such as suppliers, customers, partners, or contractors, interact with this content for various purposes, such as collaboration, marketing, or outsourcing.

However, sharing content with third parties exposes it to potential threats such as theft, tampering, corruption, or unauthorized access. These threats can compromise the confidentiality, integrity, and avail-



IS NOW



Store, edit, share and manage your content on-prem,  
in the cloud or with a hybrid of both.

Learn more at [editshare.com](https://editshare.com)



CREATE AMAZING TOGETHER

(c) EditShare LLC | [sales@editshare.com](mailto:sales@editshare.com)



**BY FOLLOWING THESE BEST PRACTICES, you can protect your content supply chain from cybersecurity risks and ensure that your content stays safe and secure throughout its lifecycle.**

ability of the content, as well as the reputation and trust of the organization. Moreover, these threats can have severe consequences for organizations that must comply with GDPR, PCI DSS regulations, and others.

Therefore, organizations need to protect their content supply chain from cybersecurity risks. Some of the best practices to do so are:

***Conduct a risk assessment of your content supply chain.***

This assessment will identify the types of content you share, the third parties you share it with, and the platforms and channels you use to gather a complete understanding of your organization's threat landscape and the potential threats and vulnerabilities you may face. Prioritize the most critical and sensitive content and third parties and implement appropriate security measures accordingly. Review the past internal security risk assessments performed to meet TPN requirements.

***Encrypt your content before sharing it with third parties.*** Encryption transforms data into an unreadable format, usable only after an authorized party uses a key to decrypt it. Encryption protects your content from unauthorized access, modification, or disclosure. You can use encryption tools such as BitLocker, FileVault, VeraCrypt, or others to encrypt your content on your devices or storage media.

***Use secure methods of sharing your content with third parties.*** Avoid using insecure methods such as email attachments, USB drives, or public links that can be easily intercepted or compromised. Instead, use secure methods such as VPNs, secure file transfer protocols (SFTP), or secure cloud services that offer end-to-end encryption and authentication. You can use tools such as Tresorit, MEGA, or others that encrypt data on the

client side before uploading to the cloud.

***Monitor and review your content supply chain.*** Keep track of who accesses your content, when they access it, where they access it from, and what they do with it. You can use tools such as Splunk, Arctic Wolf, or others to collect and analyze logs and events from your devices, platforms, and channels.

***Respond to alerts from the monitoring systems.*** When alerts come from the monitoring feeds that are in place, it is crucial to be able to respond quickly. You can use tools that assist in the response process, such as Arctic Wolf, CrowdStrike, or others, to alert you to the actions to take.

***Educate and train your employees and third parties on good cybersecurity hygiene.*** Human error is one of the leading causes of cybersecurity breaches in the content supply chain. Therefore, raising awareness and educating your employees and third parties on handling content securely and responsibly is essential. You can use tools such as Arctic Wolf, KnowBe4, or others to deliver online training courses and simulations on phishing, ransomware, password management, data protection, and more.

Review all the steps above regularly to ensure that security gaps are remediated in alignment with evolving cybersecurity threats.

By following these best practices, you can protect your content supply chain from cybersecurity risks and ensure that your content stays safe and secure throughout its lifecycle. Questions about how to secure your content supply chain? Contact [info@richeymay.com](mailto:info@richeymay.com) to learn more about strengthening your content's defense shields. ■



*Chris Williams is the senior cybersecurity consultant for Richey May Cyber. He has more than 14 years of IT and cybersecurity experience. In his role at Richey May, he works with organizations to bring a better understanding of their security and helps align security with business objectives. Williams has provided assessments and advisory services for clients in the financial, media and entertainment, manufacturing, professional and business services, healthcare, educational, retail, and energy sectors. [cwilliams@richeymay.com](mailto:cwilliams@richeymay.com) @RicheyMay*



## Expect more than what you asked for.

Tools, security and workflows are important, but above that we understand the meaning of partnership.

- ✔ Trustworthy
- ✔ Organized
- ✔ Communicative
- ✔ Intelligent
- ✔ Effective
- ✔ Determined to do it right

SUBTITLING | DUBBING | SDH | AUDIO DESCRIPTION

# SECURING ENTERTAINMENT'S EMERGING TECH STACK

## Learnings from Altman Solon's 2023 Video Production Survey

**ABSTRACT:** The media and entertainment industry has continued to evolve over the last three years, accelerating the development of new processes and capabilities. In parallel, data security concerns grew for product teams and media companies expanding their tech stack. Findings from Altman Solon's latest emerging technology study shed light on adoption trends, strengths, and potential challenges with new media solutions, including virtual production, IP-based workflows, and artificial intelligence. How should media executives toe the line of managing security concerns with the increasing need to foster growth and innovation?

By Derek Powell, Director, Altman Solon

The media and entertainment industry has undergone massive changes over the past three years. The global pandemic upended legacy production methods and mainstreamed digital tools that cut costs, facilitate remote collaboration, and speed up deadlines. As Virtual Production (VP) processes, IP-based workflows, and generative AI tools take their place in the entertainment industry's tech stack, concerns about data security are growing. This past summer, we spoke to more than 300 production executives across the U.S., Canada, the EU, and the UK, to better understand the state of adoption of these cutting-edge production technologies.

Our findings, which are part of our third annual Emerging Media Tech Survey, show that even though these tools are understood to be innovative and potentially game-changing for the industry, data security is the elephant in the room. Ultimately, widespread implementation of these tools will hinge upon accommodating security directly into the product.

### **VIRTUAL PRODUCTION AND AI: FEARS AROUND DATA SECURITY, COPYRIGHT, AND PIRACY ARE MAJOR HURDLES**

While VP tools can eliminate the need for location shots, allow for borderless collaboration, and save money on post-production, they can increase security risks across the video production process. That's why over half of survey respondents say data security is "very important" when using the technology. Nearly 60 percent of



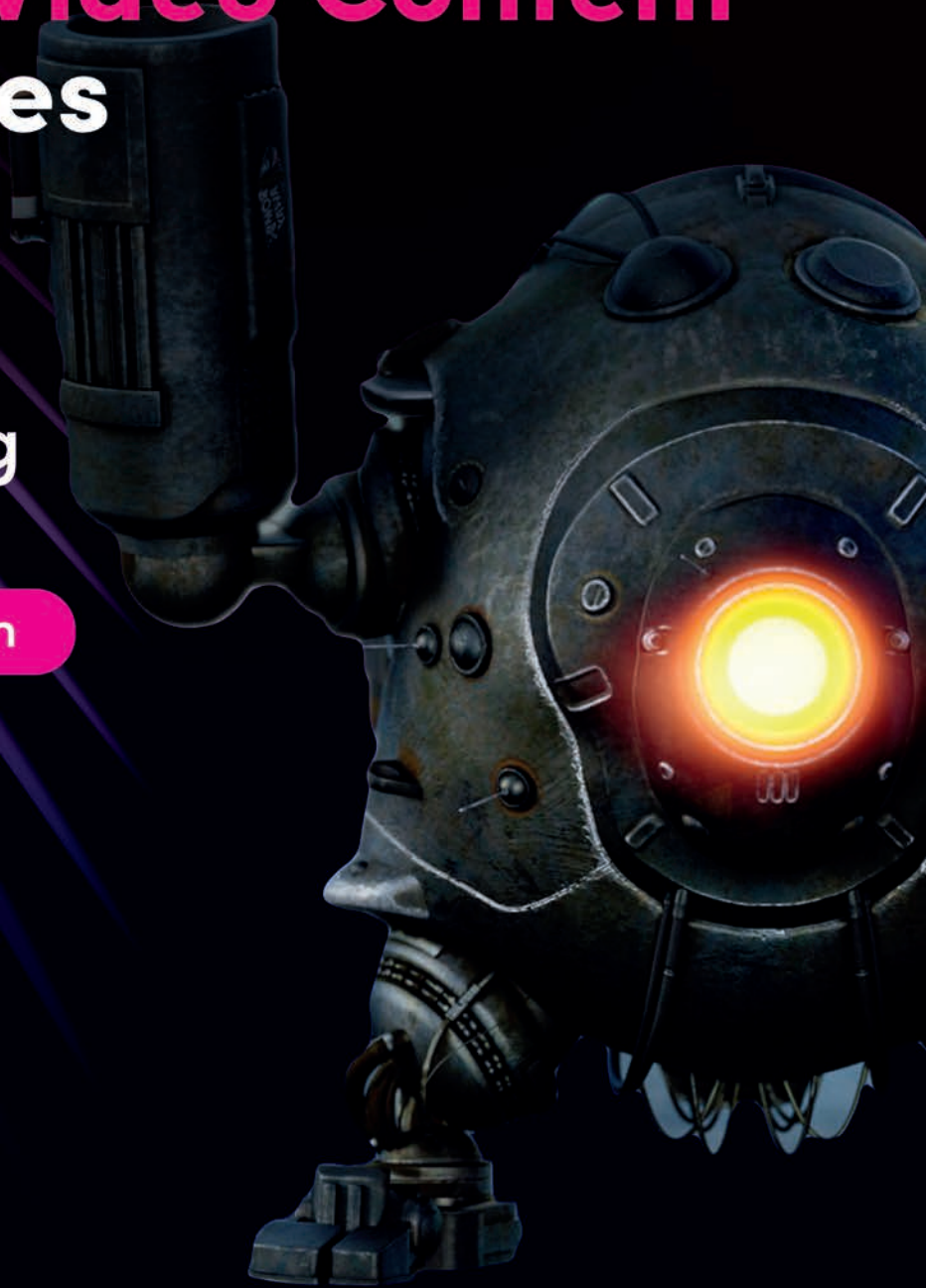


Verimatrix  
Streamkeeper<sup>SM</sup>

# The Ultimate Solution to **Secure Video Content** from Pirates

- Multi-DRM
- Counterspy
- Watermarking

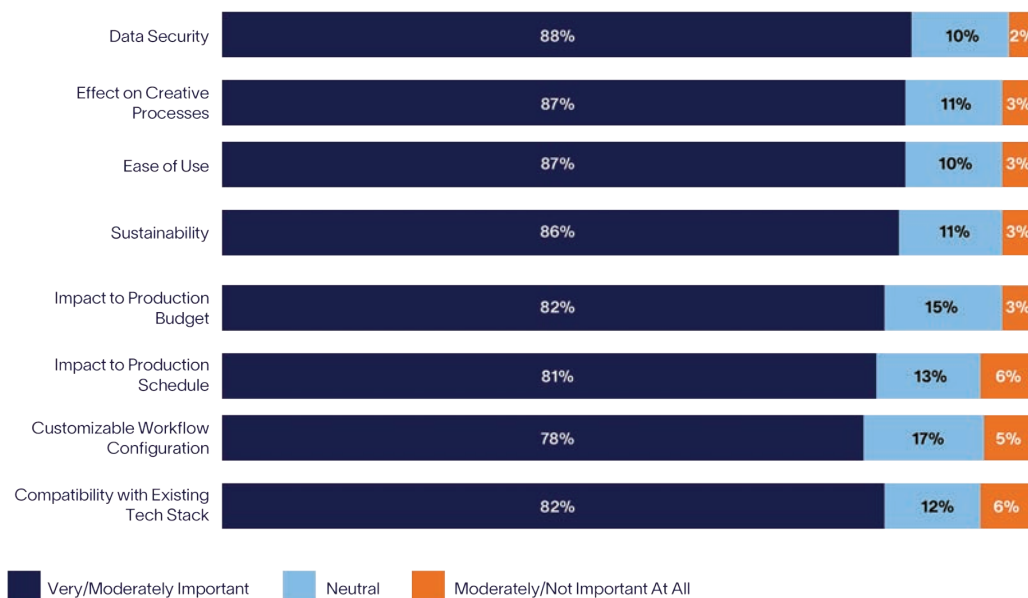
[www.verimatrix.com](http://www.verimatrix.com)



||| verimatrix™

## How important are the following aspects when considering and/or using virtual production technology capabilities ?

% of respondents selecting importance of tools, n = 145



*Altman Solon sought insight into the top industry concerns and desires around virtual production capabilities and found data security topped the list.*

respondents consider data security moderately or very challenging when implementing VP technologies.

Despite facilitating remote collaboration, projects across multiple worksites are exposed to greater risks. Moreover, VP tools depend on cloud-based off-premises workflows, which can, in turn, create security vulnerabilities. At a time when streamers spend record sums developing and producing original content, any vulnerabilities that might enable content theft undergo heavy scrutiny. While VP is still in the early stages of maturity, poor data security could slow or stop implementation.

The rise of AI in the entertainment industry is subject to fierce debate and was at the center of both the Writer's Guild of America strike and the Screen Actors Guild strike. Despite this, AI tools are already being used by studios for caption and transcription generation, narration, editing, and show-stopping special effects — including “de-aging” stars like Harrison Ford for *Indiana Jones and the Dial of Destiny*. More than 60 percent of survey respondents cited “cost savings” as the main motivator for adoption; however, most indicated

that their AI tech stack — including data, models, and deployment capabilities — is stored on-premises or in colocation facilities. The total control over hardware, security, and set-up offered by these on-premises solutions is preferred by production executives.

Anxieties over potential security breaches, data quality, content piracy, and DRM bypass were cited as concerns by respondents when it comes to adopting AI tools. These tools, which are still in their infancy, also raise questions about copyright infringement and authorship. Upcoming rulings on court cases, like the one brought by Getty Images against Stable Diffusion for copyright infringement, are certain to provide a framework for legal boundaries on AI use, but today, media and entertainment companies remain in the dark.

Media and entertainment companies' awareness of the inherent security risks in new production technologies means they can develop and adapt cybersecurity protocols for maximum data and content protection. Investing in data security tools and technologies to prevent future

*Continued on page 39*



*Derek Powell is director at Altman Solon and an expert in the global media and entertainment industry, with 15 years of experience in the production, distribution, and marketing of media content. At Altman Solon, Powell works in designing and developing new operating models, improving operational excellence, and implementing strategic planning and development for clients in film, television, music, and gaming. [derek.powell@altmansolon.com](mailto:derek.powell@altmansolon.com) @altmansolon*

***“THERE HAS ALWAYS BEEN THIS VIEWPOINT – if we move to a more modern stack with more consolidation will that expose us to more attacks like DDOS or DNS hijacking?” — VP of IT, major TV station***

breaches is a priority for the industry and essential for successful implementation of virtual production protocols and AI tooling.

### **MOVING FAST AND STAYING SAFE**

The streaming bubble has burst, with media and entertainment companies facing multiple challenges. While many are turning to innovative technologies to speed up production and cut costs, they are not immune to the risks of data breaches and copyright infringement.

Digitally native companies- including streamers and Free Ad-Supported Streaming (FAST) television networks – are already working to protect consumer data (thanks to GDPR and CCPA regulations) and their digital assets. As such, they are well positioned to apply these best practices as they expand their tech stack. There is no one-size-fits-all solution to ensuring growth and innovation while maintaining strict data security. However, production and distribution professionals should keep the following guidelines in mind:

■ *Minimize the chain of custody and double down on security protocols: As production teams embrace collaborative, digital tools, studios need to keep the people who have access to proprietary data at a bare minimum. Service providers should be subject to strict access control. Solutions like zero-trust security protocols should be*

*developed and influenced in addition to quantum-safe encryption.*

■ *Embrace the hybrid cloud: While on-premises infrastructure may be cheaper in the short-term and easier for studios to set up, AI infrastructure will certainly involve high-performance computing, and will force entertainment companies to expand to a hybrid public/private cloud set-up. Decision-makers should weigh each type of infrastructure model based on their needs for security, capacity, cost, flexibility, and choose accordingly.*

■ *Standardize ethical guidelines for AI tools: While regulations on AI are still being written, media and entertainment companies should develop internal guidelines that ensure AI use is done ethically. This can include disclosing AI use in products and establishing internal AI review bodies. Any AI tools in use should be subject to strict scrutiny.*

Gone are the days when a stern FBI warning at the beginning of cassette tapes and DVDs was sufficient protection from pirating. In a time when Universal Pictures' Super Mario Brothers was leaked in full on Twitter ahead of its theatrical release, data security for valuable intellectual property has never been more highly prized. Embracing a new digital tech stack means integrating security within the tools, the processes, and the storage facilities. ■

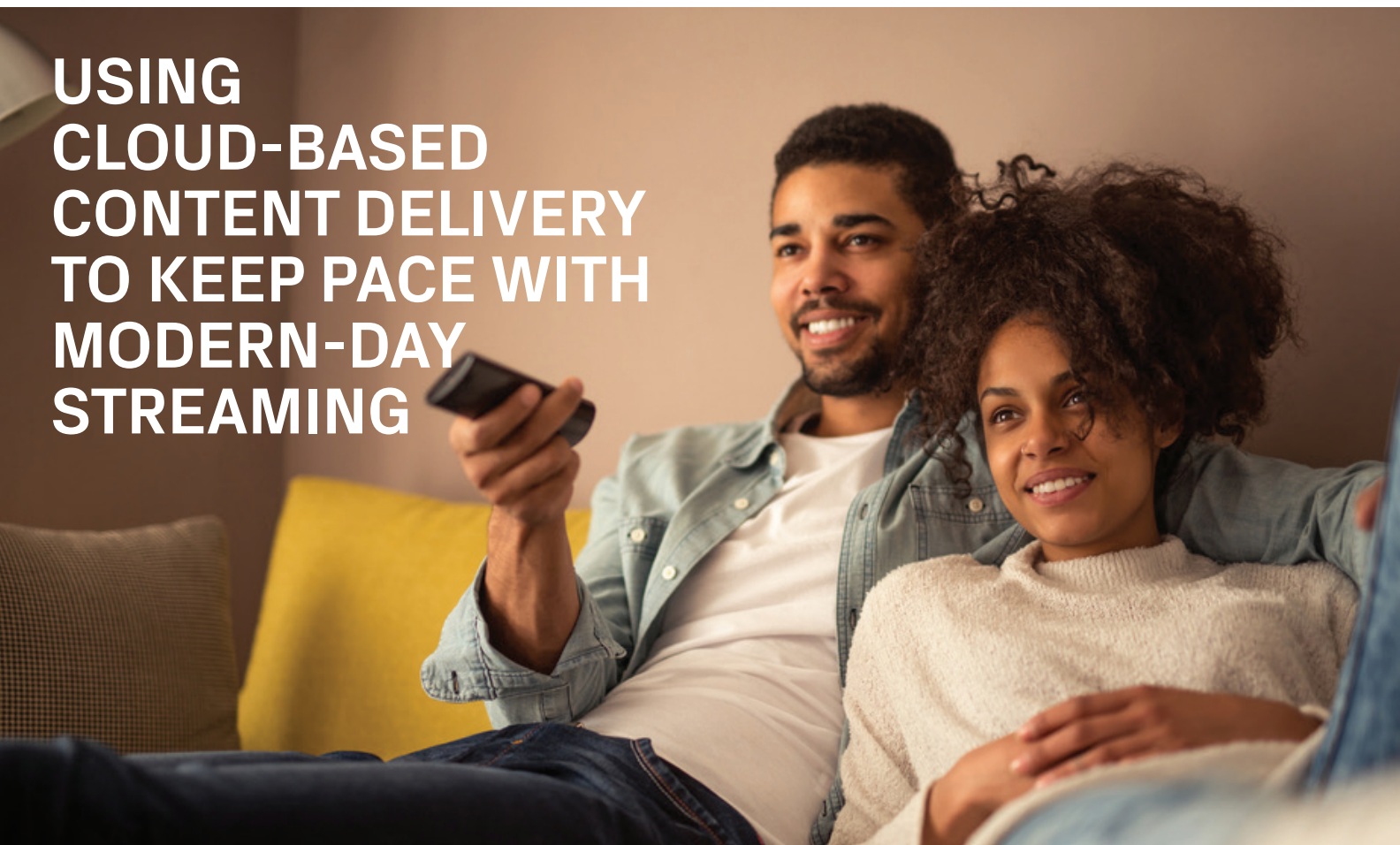
**Check out what we've been working on for our licensees!**



**Learn more at:**  
**[CDSAonline.org/spoileralert](https://CDSAonline.org/spoileralert)**



# USING CLOUD-BASED CONTENT DELIVERY TO KEEP PACE WITH MODERN-DAY STREAMING



**ABSTRACT:** Streaming content has increased in recent years as a general trend, accelerated with the pandemic. Some content is now available in line with theaters or very soon after. This brings additional challenges for the studios and operators to keep up with the demands of content protection and appropriate usage.

**By Chris Bardsley, Solution Designer, Vubiquity**

For many years, OTT streaming services have been growing in popularity, a trend that accelerated with the onset of COVID-19. During the pandemic, the studios experimented with releasing content to streaming platforms more quickly or as an alternative to a theater release altogether. Now, post-pandemic, release windows to streaming services are shorter than ever and look to stay that way.

This doesn't really come as a surprise because the convenience of watching movie and TV content on demand in your own home, shortly after its release, is very appealing to consumers. Plus, studios can earn higher revenues and gain more customer engagement, as well as charge higher price points for early access premium video on demand (PVOD) content. The net effect is

that what used to be simply regarded as a positive additional revenue stream is now considered a major way of monetizing content, which in turn has fragmented the streaming industry into multiple services.

However, these benefits come with additional risks. Whilst consumers have become accustomed to easy access to content via OTT services, economic conditions have made subscribing to the many fragmented OTT services less attractive. Increasingly consumers are either canceling services or worse case turning to pirated content. Since studios make most of their revenue in the first few weeks of a title's release, a pirated title in this period creates substantial revenue loss. Yet, studios must continue to make their content as widely available as possible to combat subscription fatigue and pressures



# Deliver video with confidence

The most secure and versatile platform for teams to manage video in the cloud.



## Theatrical

DCP eDelivery  
Live Event Cinema  
Film Festival Services



## Airline

IFE Encoding  
Metadata  
Lounge Streaming



## Streaming

Secure Screeners  
Video Libraries  
White-label OTT

Trusted by over 100 M&E industry leaders

**cinesend.com**

**IT'S THE SIMPLE FACT THAT THE MORE COPIES OF A TITLE THAT EXIST exist in circulation the greater the risk of a security breach. This risk triggers the studios to "up the [security] ante" regularly which consequently requires operators to increase their own security spending.**

from the current economic conditions.

For many years, the major studios have maintained technical security requirements that all streaming platforms must adhere to. With the acceleration of titles to streaming platforms and the potential loss of revenue from piracy, these security requirements are more important than ever.

### THE DILEMMA

Distributing content to third-party streaming services is typically achieved by titles being prepared and then physically sent to video operators who host these titles on their infrastructure, ready to be streamed by consumers. This scenario poses three primary areas of vulnerability:

- Transit of the title to the operator headend
- Storage of the title on the operator's infrastructure
- Streaming of the content to consumer devices

For transit, the studios specify secure, encrypted, trackable distribution methods which are straightforward to implement. Storage is a combination of encryption at rest and authorized access control processes. Lastly, streaming of content is a combination of encrypted DRM controls, combined with authorized access control, device management, and geo-location limitations. In all cases, the studios are entirely reliant upon operators observing their security requirements for the items noted above, which studios enforce by having operators complete a questionnaire. It's essentially a trust-based system. The point is not that operators are untrustworthy. Rather, it's the simple fact that the more copies of a title that exist in circulation the greater the risk of a security breach. This risk triggers the studios to "up the [security] ante" regularly which consequently requires operators to increase their own security spending to minimize the risk of breaches.

For example, the next expected security measure is to require session-based forensic watermarking which

would allow the unique identification of each stream of a title to the individual watching it. This would make it easy to precisely identify where a title was pirated from and perhaps become the ultimate deterrent for pirates.

However, this and other security improvements have a cost and it's rapidly increasing. An arms race that no one necessarily benefits from; but is a level playing field for ALL operators.

### CLOUD TO THE RESCUE

A shared cloud-based delivery solution, where titles are centrally held and access is given to operators' customers on a stream-only basis, can address many of the aforementioned issues.

Studio content can be uploaded to a cloud storage system that is centrally managed, thereby reducing the number of copies of a title in transit. Also, a cloud-based storage system has limited physical access, and with encryption at rest any physical access risk is further reduced. A shared cloud-based repository means that content access can be centrally controlled rather than relying upon each operator to provide such controls. This reduces the number of parties responsible for controlling authorized access, which of course reduces the risk of unauthorized access.

Notwithstanding the security benefits, a shared cloud-based repository also reduces the cost of storage for the operators as well as optimizes their operational costs. With licensing deals, content often moves in and out of its available license windows which tempts operators to retain content in between such windows. Studios prohibit this, partially due to the same security concerns, but it is difficult to enforce. A centrally controlled, shared cloud-based content repository makes re-acquiring content an inexpensive, legal, and secure way of satisfying both studios and operators.

Finally, streaming directly from a shared repository has further benefits for both studios and operators. For studios, they can build a successful and trusting relationship with the streaming cloud provider and ensure

*Continued on page 79*



*Chris Bardsley is the solution designer for Vubiquity. A seasoned solution designer and product manager, Bardsley has nearly 25 years of experience in the definition, development, and delivery of IPTV/OTT media systems. He was also a key team member behind the deployment of one of the UK's first VOD platforms for Yes Television in 1998. [chris.bardsley@vubiquity.co.uk](mailto:chris.bardsley@vubiquity.co.uk) @vubiquity*





# The largest global strategy consulting firm exclusively working in the telecommunications, media, and technology (TMT) sectors

**13** Offices    **25+** Years of Client Service    **600+** Consultants Globally

Altman Solon combines decades of world-class industry expertise and sophisticated data analysis to deliver prescriptive strategies to accelerate growth for Fortune 200 firms and leading TMT investors.



Sports



Video



Audio



Publishing  
& Content  
Commerce



Gaming



Advertising  
& AdTech

---

Connect with our team at [insights@altmansolon.com](mailto:insights@altmansolon.com).



**ABSTRACT:** Keeping vendor facilities secure has become more important than ever. But there are no concrete answers (yet) around what security will be needed with AI applications.

**By Eutdel Garcia, VP Engineering,  
Facilities, The Kitchen**

The Kitchen International is extremely active within the area of cybersecurity and content protection, from receiving of clients' assets, to completion and delivery. The Kitchen has been a trusted language services institution for more than 22 years, and this year we are thrilled to have received the coveted Gold Trusted Partner Network (TPN) Badge, a nod that we are very proud of, ensuring our clients of 100 percent protection from receiving of assets to final deliveries.

It is important to understand that TPN is granted when it is proven that the particular facility has met the requirements necessary to secure the clients' content, the physical facility, that staff are vetted, visitors are badged, and vendors sign appropriate NDA's if necessary.

We are soon expanding our Gold certification to our new Madrid, Spain studio (our European hub) as well, with our cloud secure infrastructure in place to manage and distribute content produced in our facilities throughout LATAM, North America, Europe and the Middle East.

Several of our global language studios are currently in the TPN badging process, and we expect to name these by the end of the year.

We are all aware of AI, however there are no concrete answers, or signifi-



# It's Only Artificial If It's Not Intelligent: Maximizing Content Revenue

## Smart Avails in the Age of AI

Recent innovations in the world of Artificial Intelligence have taught us all that large data can be queried using natural language.

From the world's leading rights and royalties expert, the Vistex Smart Avails solution helps you change the narrative from "What can I?" to "What should I?". Now, you can re-invent your media and entertainment business with a single source of truth to determine how to monetize the rights you control. Extend your avails query to leverage external data sets using a Natural Language Interface (NLI) rather than a form to run the query.

*With Vistex Smart Avails, the only limit is your imagination.*

### Let Vistex Smart Avails help you:



Elevate your queries from ordinary to extraordinary



Access and exploit your content's true potential



Uncover hidden gems in your content library



Scan the QR code or visit  
the page at [vistex.link/avails](https://vistex.link/avails)  
to learn more



cant directions to fully determine how this will affect our industry moving forward. As is always the case, if AI becomes a part of our receivables or deliverables, the same strict and detailed protection will be given to the new technology. Currently, we are already testing and evaluating AI technology in our language department, specifically to assist on text translation. The results to this point have been amazing. AI is a promising technology that will allow our industry to growth in multiple fronts by bringing flexibility, scalability, efficiency, time, and cost savings while maintaining the same security protocols.

Our global operational infrastructure has been designed to inspect, digest, and fully integrate new technology into our existing systems, as needed. Of course, all our rigid tests and standards must be met by any new sources for us to agree to offer a broader opportunity for our clients.

We do believe that it is necessary for the industry to create an AI protection authority to use as a guideline and for our overall protection. This must include an on-going testing committee when AI is used in new areas, or for new applications. Committee results should be made known, and much like what has been successfully created for TPN approval, studios must be guided through new processes.

One note of importance. As an international language provider, with studios throughout the globe, it is vital for The Kitchen to be ready to undertake and resolve any issues that may occur. This year

**AI IS A PROMISING TECHNOLOGY THAT WILL ALLOW our industry to growth in multiple fronts by bringing flexibility, scalability, efficiency, time, and cost savings while maintaining the same security protocols.**

alone, The Kitchen Turkey was hit by a devastating earthquake; the war between Russia and Ukraine, caused our staff in Moscow to immediately relocate to Uzbekistan, and the Israeli war now has found all our Kitchen Israel personnel safe, but in a highly unstable situation.

We have learned that it is necessary to keep on our toes, to remain instantly available to work and change direction at a moment's notice, always keeping security of content and deadlines for delivery in mind. Our global network of studios, led by our Emmy Award-winning U.S.-based headquarters, has been successful in providing all that is required to maintain a smooth flow for all our projects. ■



*Eutdel Garcia is the VP of engineering and facilities for The Kitchen. He was first introduced to The Kitchen as a client, having served as director of engineering for Discovery Networks for more than seven years. Eutdel is responsible for implementing support for overall technical standards and procedures throughout The Kitchen's 14 international studio locations on a day-to-day basis. [egarcia@thekitchen.tv](mailto:egarcia@thekitchen.tv) @thekitchenmiami*

**M&EDCA**

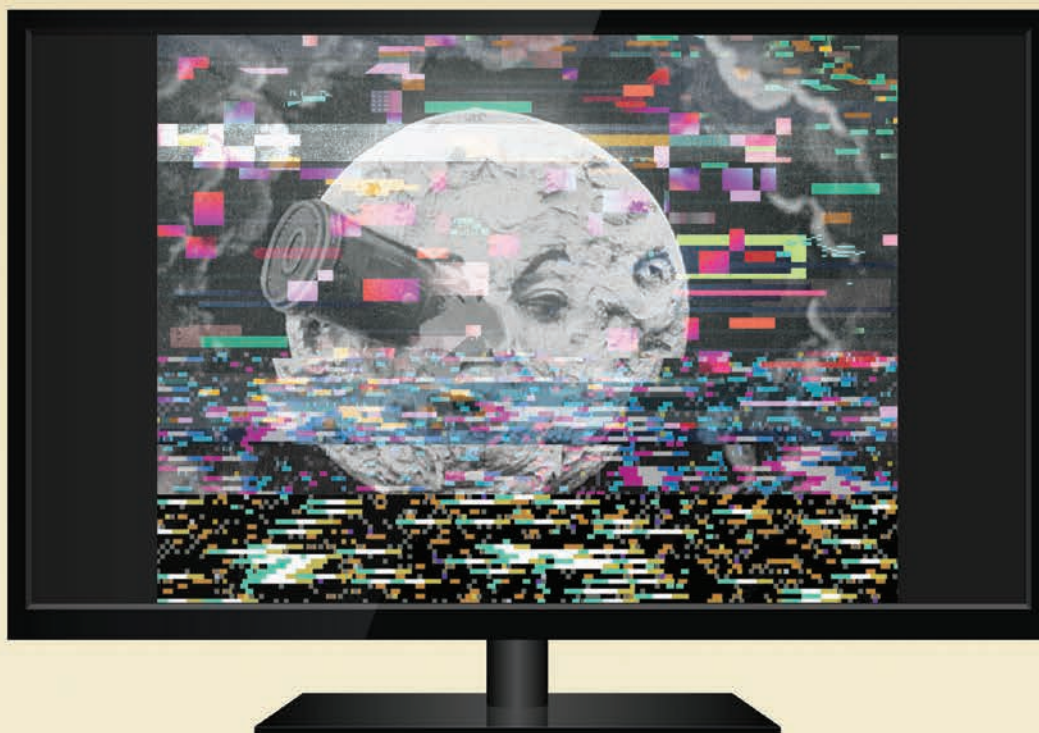
MEDIA & ENTERTAINMENT  
DATA CENTER ALLIANCE

**Bringing Data Industry  
Standards to the Land of  
Make Believe**

**[www.medcaonline.org](http://www.medcaonline.org)**

# Preserving digital masters is complicated – it's more than just storage.

Digital Bedrock preserves your valuable production assets and masters  
so the content can be monetized in the future.



Our detailed preservation actions include:

- Analyzing and organizing the data to ensure you are preserving the correct assets, and nothing is missing or corrupted
- Creating exact, immutable copies for disaster recovery, and storing the copies offline in secure, geographically dispersed vaults
- Monitoring the digital content's file health over time

Digital Bedrock was developed from years of experience and familiarity with what the Entertainment Industry needs. We understand the content, and your security requirements.

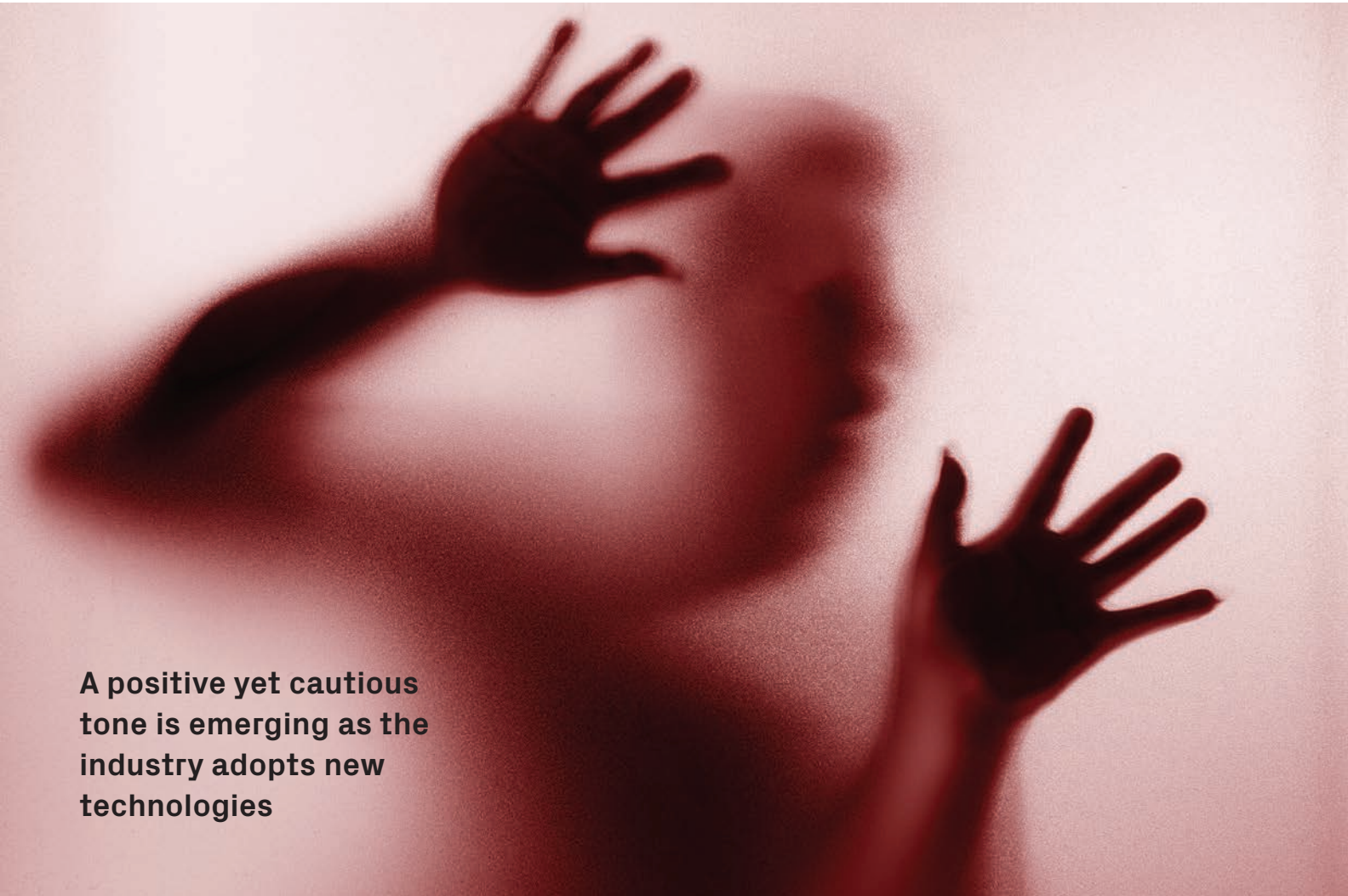
Our clients include media production companies, producers, artists, and Academy Award-winning directors.

**Digital Bedrock is your trusted digital preservation partner and data insurance policy.**

**DIGITAL BEDROCK**  
SECURE OFF-LINE DIGITAL PRESERVATION



# AI: THE NEXT BIG M&E CREATIVE ADVENTURE OR A FAST-APPROACHING SECURITY HEADACHE?



A positive yet cautious tone is emerging as the industry adopts new technologies

**ABSTRACT:** This article explores how AI is being used to create content that is realistic and easily blended with live-captured video. But aside from likeness protection, what about the wider security aspects and how could such technology be used for illicit gain?

**By Tim Pearson, VP, Global Solution Partner Marketing, NAGRA**

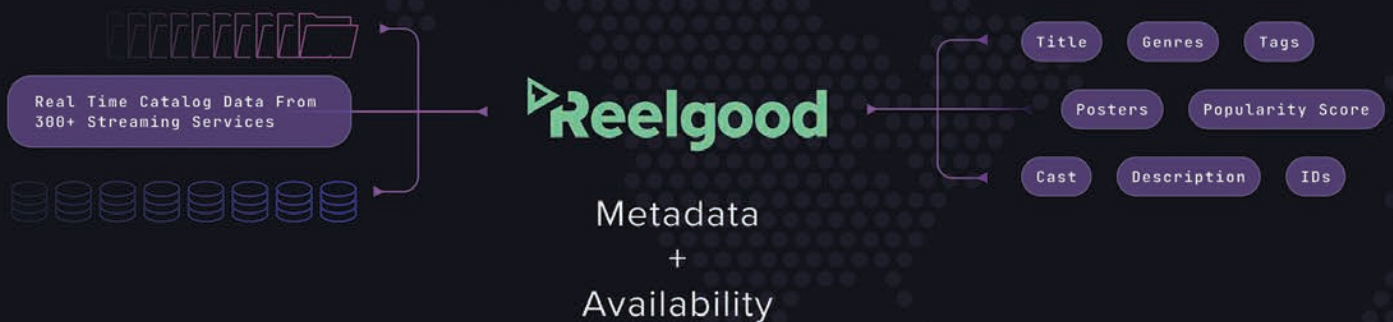
The M&E industry has been using AI in various forms for several years. Largely focused on data interpretation that detects anomalies and patterns around everything from security analytics to customer retention, its use is well documented. In the last year, however, its

use and application has left the labs to become more mainstream. One area in particular, generative AI, has caused a tempest of debate across the industry. Spearheaded by today's "go to" engines for tricky questions, such as ChatGPT and AI content creators such as



# World's **Most Accurate** Streaming TV Data

Powered by AI



**278K+**

TV & Movie Listings

**300+**

Streaming Channels

**100M+**

Users optimizing our data



Contact us at

[sales@reelgood.com](mailto:sales@reelgood.com)

## *WHETHER GENERATIVE AI WILL FORM the next content revolution and change established industry practices and business models remains to be seen.*

Midjourney, broader tools are also being used to create content that is realistic and easily blended into existing live-captured video.

At a recent NAGRA customer event, strategic partner AWS showed us how some of this technology is being used across the M&E industry — from sports telematics to creating new inserts for content production. Aside from likeness protection demanded by the recently striking actors, what about the wider security aspects and how could such technology be used for illicit gain and how does machine learning accelerate this adoption further?

### PROTECTING THE PROTECTED

In a world where computer generated moviemaking doesn't involve writers, crew, or talent, will today's structured production processes continue? Key to that production process is the protection of IP against illicit distribution. NAGRA is an industry leader in this charge by advocating solutions such as NexGuard Forensic Watermarking applied from the moment content leaves the camera to the point it is watched on a consumer's device. Along the distribution chain, further tools from the NAGRA Active Streaming Protection toolset are used to protect valuable content investments. This includes illicit activities such as pirate re-distribution, extended access through credential sharing or addressing broader cyber threats. Incorporated into production and distribution workflows, security is a firm fixture meaning it is protecting both studio revenues alongside the reputations, identities, and talents of those involved.

But how would this work in a pure generative AI landscape? For now, there is clearly a blend of both live and AI content working together as it passes through the existing secure workflows and processes. But with a pure AI landscape, where established processes, regulation and approaches are either in their infancy or

non-existent, innovation can spawn both new content genres and new content production approaches — and arguably quicker than their more traditional cousins. The adoption of machine learning technology can accelerate post-production through tools too. Examples include face ageing, changing clothing appearance and motion diffusion. But even before we get to that stage in the process, machine learning could also be used for concept ideation and reducing time spent on more time-consuming tasks such as animation, compositing, lighting, and optimizing localization.

But is that day already here? I recently came across an article on LinkedIn that discussed a new Netflix show where contestants guess whether their partners' actions are real or fake based on both live and deepfake content they review in the "chair of truth." Equally, Marvel Studios' new "Secret Invasion" TV series that has recently launched on Disney+ includes opening credits created with AI. Perhaps innocuous but creatives have reacted strongly about generative AI's role. In particular, the impact it could have on artists' careers going forward.

Evidently, this topic is generating much discussion across industry groups, regulators, and vendors.

### GENERATIVE AI AND PIRACY

Teams across NAGRA and the wider Kudelski Group have been hot-housing technologies that can identify bogus media or unauthorized representation of individuals' likenesses created through AI-generated content. The aim being to ensure our solutions protect our customers' interests. In the same way conventional content and service piracy is outwitted by developments in technology, a new era is dawning where piracy is about both stealing content and creating content that to the unaware, is a "genuine fake." The ramifications of this are vast. With consumers already showing a voracious appetite for online content across both streaming

*Continued on page 81*



*Tim Pearson is VP of global solution and partner marketing at NAGRA. He drives various market development, solution, and partner marketing activities for the company. His areas of focus include next generation content protection, OTT streaming, watermarking, anti-piracy, broadcast, consumer engagement and user experience. marcom@nagra.com @NAGRAKUDELSKI*

VERIFYING  
**PROVENANCE & AUTHENTICITY**  
DELIVERING  
**INTEROPERABILITY**  
FOR THE  
**REAL & VIRTUAL**

**HUMAN**  **DIGITAL**  
**BOTH IS BETTER.**

[handidentity.com](https://handidentity.com)



**UNIQUE TALENT IDENTIFIERS BUILT FOR:**  
Television • Film • Music • Sports • Gaming



# ONE SIZE DOES NOT FIT ALL. A VENDOR RISK DILEMMA.

No company is alike, and each has its own policies, procedures and values that make it different

**ABSTRACT:** When building or operating a vendor risk program, you know that using third party vendors comes with some level of risk to your business. How do we properly secure these vendors and ensure that we don't have a business operations impact?

**By Katie Pickrell, Senior Product, Operations Manager, Independent Security Evaluators, Senior Manager, Software Development Operations, Start**

Vendor risk management is an interesting space. Everyone does it differently, there is no right or wrong framework and vendors exist in a wide range of services. When building or operating a vendor risk program, it at least means you have identified one thing: using third party vendors comes with some level of risk to your business.

An early 2023 survey conducted by Gartner found that out of 100 executives surveyed, 84 percent indicated that a third-party risk “miss” resulted in operations disruptions. Despite this, reliance on third party vendors remains at a high, with work being shared and collaboration being essential to the business’ success. So how do we properly secure these vendors and ensure that we do not have a business operations impact when the vendor landscape is so vast?

Third party vendors come in many shapes and sizes. Some are niche and only provide one specific service. They



# Helping You Achieve a TPN Gold Shield



**TRUSTED  
PARTNER  
NETWORK**

We are the principal provider of security assessments for the major content owners and their M&E vendor supply chain. Our assessor team offers the widest experience and guidance for your environment. We work with pre-production, production, post-production and distribution vendors across the globe through our offices in the Americas, EMEA and APAC.

In addition to helping you achieve TPN Gold assessment status, our services include cloud and application security consulting, web app and infrastructure penetration testing; internal vulnerability scanning as a managed service (cloud configuration & infrastructure), management policies; incident response; SOC2/ISO/NIST readiness; and privacy compliance.



convergent

## **Contact Us**

**For more information or general enquiries:**

**e:** [info@convergentrisks.com](mailto:info@convergentrisks.com)

**w:** [www.convergentrisks.com](http://www.convergentrisks.com)

**US Office:** +1 (818) 452 9544

**UK Office:** +44 (0) 1276 415 725



may have a small number of employees and a small facility or be totally remote. Other vendors are quite large and have hundreds to thousands of employees, offer a wide range of services and work across many industries. No company is alike, and each has its own policies, procedures and values that make it different.

### SO WHERE DO WE START WITH OUR RISK PROGRAM?

#### *Step 1: Identify what is high risk*

The first step comes with figuring out what is considered high risk to your company. Is it financial assets? Is it content that is being created? Is it blueprints? Every company has risk but what that risk is will vary. Risk is often tied to financial impacts; products that create revenue, ideas that generate buzz, etc. However, they can also often be reputation focused; personally identifiable information (PII) that could cause a lawsuit, a movie getting leaked and posted online, private emails getting released. Risk comes in many different forms and levels. But starting by understanding what is considered high risk to your company will help you lay the right foundation for your program.

#### *Step 2: Who handles high risk content?*

According to the Deloitte Global third-party risk management survey 2022, 55 percent of survey respondents indicated they segment their third parties based on those that present the highest risk to their company. Understanding what type of vendors handle your high-risk content is crucial to any vendor risk program. This is the stage where you evaluate the service offerings of your various vendors in the pool and determine which services may require more attention than others. If you do not know where your highest risk lies, then you do not know where to focus your assessment efforts.

#### *Step 3: Control mapping*

Once you know which types of vendors present the biggest security risks to your company, step three is where the rubber hits the road, control mapping. Control mapping is the concept of mapping your security controls to the services a vendor offers to determine what controls affect what type of vendors. For example,

**THE RESULTS OF SECURITY MISSES CAN BE DETRIMENTAL to operations, finances and especially reputation when things go wrong. But through collaboration and an understanding of your vendor's company, a secure relationship is always possible.**

you may say photo IDs are required for a company that has 100 employees, but maybe it is not required for a company with only five employees, or you may have a policy that all vendor employees should be under an NDA with their own company and that applies to everyone no matter the service. Maybe you want to be more stringent with a vendor who is providing legal services as opposed to someone providing catering services. Mapping controls to vendor services gives you a dynamic framework and helps to ensure that the right controls are applied to where your highest risk may lie.

#### **Results**

Applying the “one size does NOT fit all” mindset benefits both your assessors and vendors undergoing assessments. Assessors no longer have the burden of trying to determine if a certain control applies to a given vendor. It allows them to focus on the risk in front of them without having to add additional steps to their workflow. Similarly, vendors now have a set of controls that apply to their given services/state. This reduces complicated situations where the vendor is being asked about security controls that have nothing to do with them. It creates a streamlined experience for both assessors and vendors to enable better collaboration.

The results of security misses can be detrimental to operations, finances and especially reputation when things go wrong. But through collaboration and an understanding of your vendor's company, a secure relationship is always possible. ■



*Katie Pickrell is the senior product and operations manager for Independent Security Evaluators, and senior manager of software development operations for vendor risk management software application Start. She has 10-plus years of experience in media and entertainment and spent all that time on content security and technology teams. She has been working on the Start application for 8.5 years now and is a process aficionado. [kpickrell@ise.io](mailto:kpickrell@ise.io) @ISEsecurity*





THE ART OF STORYTELLING

INTERNATIONAL DIGITAL CENTRE

NEW YORK • LOS ANGELES



SUBTITLING



CREATIVE POST



QUALITY CONTROL



DUBBING



MEDIA SERVICES



CREATIVE AUDIO



ACCESSIBILITY



CONTENT SECURITY

[www.idcdigital.com](http://www.idcdigital.com)



[www.idc-la.com](http://www.idc-la.com)





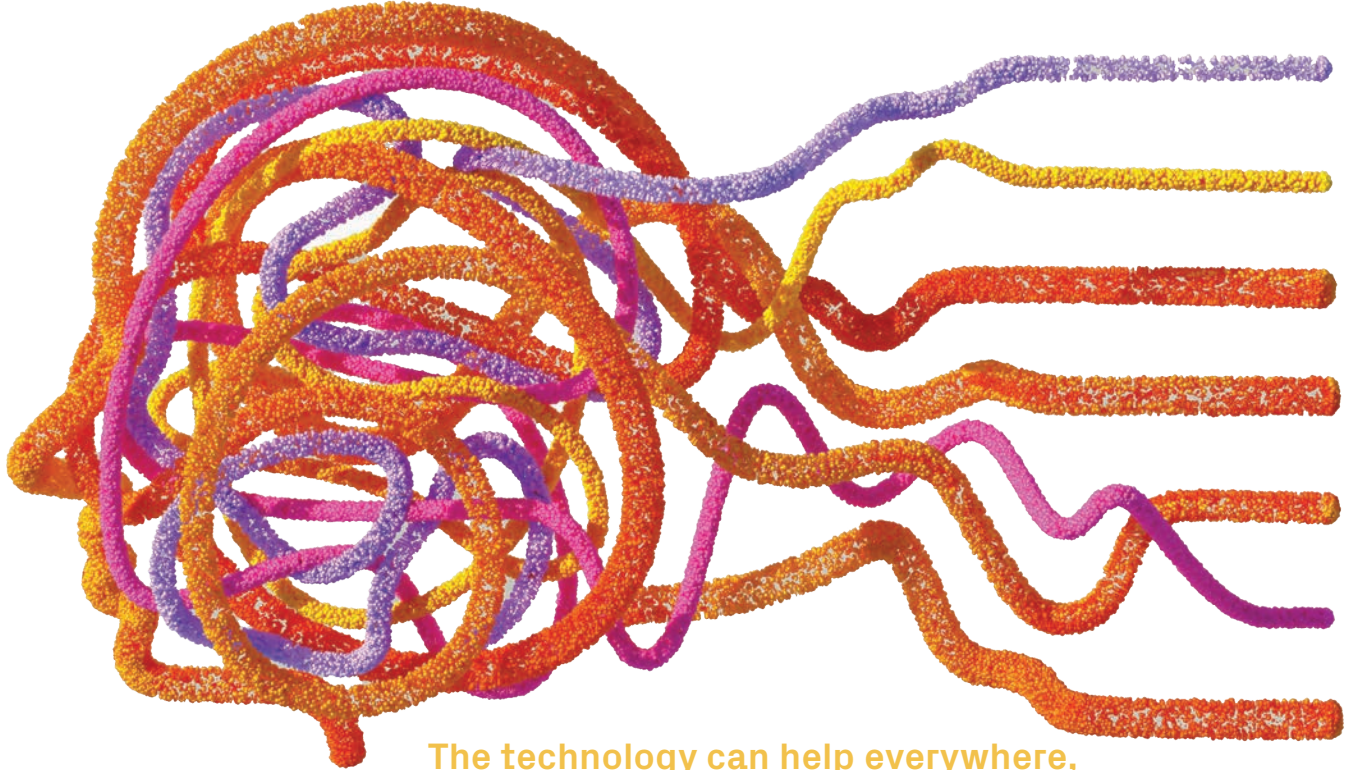
# SMART CONTENT



The concern of the day with the employment of AI in our industry is that it will render some human jobs irrelevant. Instead, media and entertainment players are finding ways to employ the technology without replacing the human element, from localization, to the content supply chain, to the sifting and sorting of the mountains of data we deal with.



# AI ACCELERATING THE M&E CONTENT SUPPLY CHAIN



The technology can help everywhere,  
from ideation and creation, to  
consumption and monetization

**ABSTRACT:** The buzz word of the day seems to be AI and its endless potential and benefits. Its potential in the M&E industry is equally exciting, especially as we look at its applications across the content supply chain and the various cost and revenue optimization benefits. There is also a lot of public concern around its usage and concerns around AI replacing human jobs. AI is just an accelerator and not a replacement for human skills, and building a responsible AI solution is key for future adoption and to ensure AI solutions are explainable, ethical, and trustworthy. In this article, we'll provide a quick background around AI, how it applies towards the M&E content supply chain, and dive into some challenges and things to consider while starting your AI journey.

By Dave Liu, Principal, Business Consulting, EPAM Systems

Since there tends to be confusion and misunderstanding of what AI is and is not and how it relates to things like machine learning, deep learning, and generative AI, let's start with a brief history of AI.

Contrary to public belief, AI isn't a new concept. It all started in 1956 at a conference where researchers

birthed artificial intelligence as the field of computer science that seeks to create intelligent machines that can replicate or exceed human intelligence. Machine learning (ML) is a subset of AI that was developed in 1997 to enable machines to learn from existing data and improve upon that data to make decisions or predictions. Deep

learning is a more recent area that was established in 2017 and is a machine learning technique in which layers of neural networks are used to process data and make decisions ... basically, attempts to simulate the behavior of the human brain. In 2021, generative AI was born as a type of AI that uses deep learning techniques to create new written, visual, and auditory content given prompts or existing data. This is the area where large language models like ChatGPT and Bard or image generators like Stable Diffusion, Midjourney and DALL-E and audio generation tools like VALL-E have recently gained their claim to fame.

To help put those generative AI models into perspective, let's use an M&E analogy of producing a movie or TV show where you have the director, the sets and the actors coming together for the production itself. Think of AI companies like OpenAI as the directors creating the broad AI architectures. AI models like GPT4 are the sets and actors. These template models come in all shapes and sizes and have differences that make them unique, like understanding language, while others are made for images, etc. The unique purpose-built model and interface like ChatGPT's online chat are the production, as they take the models and customize them to a unique use case and experience.

## THE AI FUTURE FOR CONTENT SUPPLY CHAIN

Now how does AI help within the M&E content supply chain? As I'm sure you all know, the content supply chain is a large and complex space. It's easy to get bogged down by all the complicated workflows and processes. But what parts add value, and are the things we enjoy doing? The parts of their work that people love, the reasons they keep coming back or find fulfillment: that's their craft. Everything else? From forms to paperwork, to routine tasks to logistics — that's the stuff. Companies and the M&E industry win when they help their employees focus on the craft and work to eliminate the stuff.

If we focus on the key areas of the supply chain, from ideation and creation through to editing and distribution, and consumption and monetization, there's a lot of stuff day-to-day that we can start simplifying with AI. At EPAM, we're already seeing significant productivity gains and cost savings for ourselves and our clients by integrating Generative AI into day-to-day activities.

## IDEATION AND CREATION

Let's start by looking at the AI opportunities within the ideation and creation part of the content supply chain. This is heavily creative, but AI can be a great accelerator around things like:

- *Helping writers to generate draft idea starters or sounding boards for script development of movies, TV shows or other media content based on historical and current audience trends.*
- *Leveraging the script and director's vision to create draft visual storyboards.*
- *Leveraging AI to create thematic script summaries by character to help actors and directors prep for their script readings.*
- *It can even help draft content acquisition valuations and plans based on the script, pilot, similar titles, and historical and current audience trends.*
- *From a planning perspective, AI can help generate template orders for the various title versions and localization based on historical titles, similar genres, and cast members.*
- *From a visual perspective, it can create virtual set imagery for virtual production stages and venues based on the script and director's vision.*
- *And you can even have intelligent metahumans (think AI tied to computer vision and a high-fidelity human avatar) that you can speak and interact with as virtual stand ins for actors, background extras, or script readers in a pinch.*

## EDIT AND DISTRIBUTION

Moving onto editing and distribution, that's where AI can shine even more to help accelerate those workflows. For instance:

- *The simple yet tedious tasks of tagging metadata to content can be done by AI leveraging computer vision to recognize objects, actors, and sentiment.*
- *It can take all the disparate video footage and assemble stringouts based on the dialogue and camera angles.*



*Dave Liu is the head of media and entertainment consulting for North America at EPAM. He has more than 20 years of work and project experience across various industries, such as media and entertainment, technology, retail, automotive, telecom, consumer products, and financial services. He's a cross-functional leader whose expertise and passion is in defining innovative strategies and bringing them to life across the media technology and operations landscape. [dave\\_liu@epam.com](mailto:dave_liu@epam.com) @EPAMSystems*

**IT'S CRITICAL TO TAKE A HOLISTIC APPROACH WHEN YOU'RE BUILDING a responsible AI solution to make sure it's explainable, ethical, and trustworthy so that you can have confidence in what it does, why it does it and that it's securely doing things, while making sure it's considering business context and adhering to governance and laws so that you have a truly responsible AI solution.**

■ For things like initial rough cut, color correction and color grading, AI can help determine the shot selection and trimming based on “interestingness” and tweak coloring based on director style and preferences, genre, etc.

■ Leveraging image generators, you can dynamically generate visual effects based on shot descriptions, storyboards, and director style.

■ And through audio generators, you can generate sound effects or use AI to suggest sound effects to accompany scenes based on the script and existing audio assets in your MAM system.

■ It gets even more interesting as we look at content distribution and localization, as AI can generate translated subtitles, closed captions, dubbing scripts, and voiceovers in various languages and adjust the video footage to match.

■ Based on the content schedules and delivery templates, AI can also dynamically generate classifications and content packages for various distribution partners.

## CONSUMPTION AND MONETIZATION

Lastly, from the consumption and monetization part of the content supply chain:

■ AI models can be built to look at current rights and avail information to automatically know when it's time to distribute media content through various channels such as social media, streaming platforms, and traditional distribution channels.

■ From a monetization perspective, it can help provide insights on customer behavior patterns and use that to propose various monetization strategies for advertising, subscription-based models, and pay-per-view.

■ It can predict when there will be user churn based on their activities and proactively propose new product offer bundles based on existing products, user data and user interests.

■ And even automatically create short form personalized ad or promo content based on analysis of past user engagement and existing

digital assets that would be relatable.

■ From a user experience perspective, it can generate truly personalized user experience and content recommendations based on the user's viewing history and preferences.

■ Through large language models, it can interactively engage users through chatbots, quizzes and games.

■ You can even leverage a virtual metahuman paired with generative AI to have a conversational metahuman assistant for customer support that can address simple questions or pass over to a shared call center behind the scenes for harder questions.

## THINGS TO CONSIDER

As you can see, there's a lot of potential for AI. That brings us to the things to consider. As with any new technology, there are expected and unexpected challenges that you will run into, and AI is no different. These are a few expected challenges to consider:

■ AI models require training just like the people who are going to use them.

■ If you kept up with the writer's strike, you knew AI was a big part of their concern. There is a lot of fear, uncertainty, and doubt about AI's place within M&E.

■ Especially the multitude of intellectual property rights concerns since AI laws are still being defined.

In addition to those, there are many unexpected challenges that AI adopters need to consider:

■ AIs don't think or feel like humans do. Although they seem more human-like, LLMs do not have common sense, a sense of humor, or sensitivity/appropriateness.

■ Language is more nuanced than what LLMs can predict. Because of this, one may find applications to be repetitive in responses.

*Continued on page 75*



# Technology to Elevate the **Value of Metadata**

## **Audit**

Automated processes to  
confirm that your metadata  
is fit for purpose



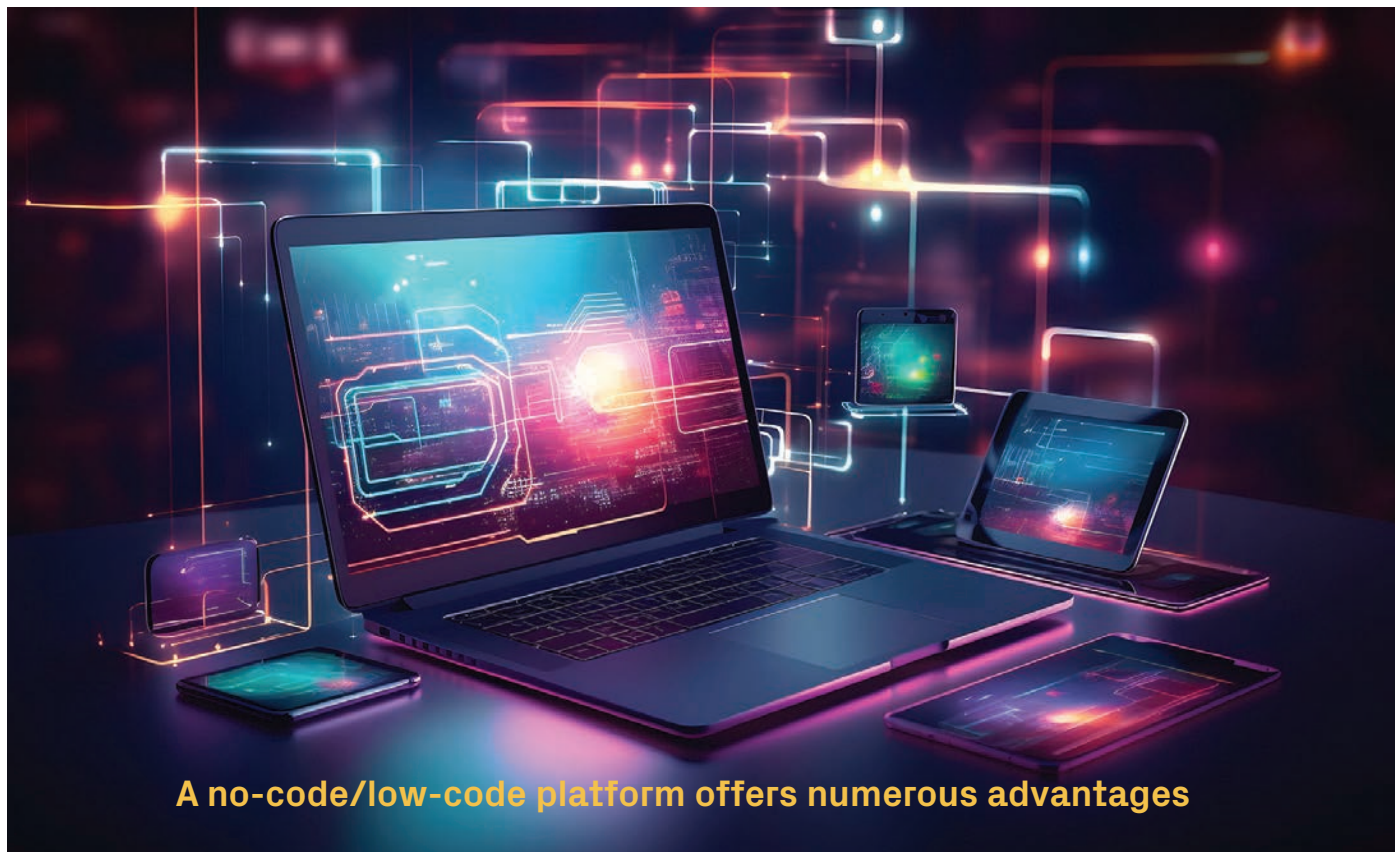
Systematically unify and  
update the descriptive  
metadata showcasing the  
depth and breadth of your  
content investments.

**Learn more about how we help optimise your descriptive metadata**

**[www.metabroadcast.com](http://www.metabroadcast.com)**



# CHANGE THE (CUSTOM) SCRIPT FOR YOUR MEDIA SUPPLY CHAIN WITH A NO-CODE PLATFORM



**A no-code/low-code platform offers numerous advantages**

**By Dan Goman, CEO, Ateliere Creative Technologies**

**ABSTRACT:** In this article, we will delve into the challenges and business risks associated with the custom scripting approach to the media supply chain, and unveil the future: a no-code/low-code approach enabled by cloud-native media supply chain platforms.

As technology continues to evolve, companies in the media industry are constantly seeking ways to optimize their workflows and supply chains. One method that has gained traction involves using custom scripting to stitch together many different workflow tools, and for that reason it's known as "the toolbox approach." Scripting in the media supply chain involves the use of tailored code to automate tasks and enhance workflow efficiency.

While custom scripts may initially seem like a good idea, they pose significant drawbacks. Most critically, this "duct tape and chewing gum" way of doing things seriously compromises the integrity of your media supply chain. It's the equivalent of trying to assemble a couch from IKEA but all the nuts and bolts have been scattered across your yard.

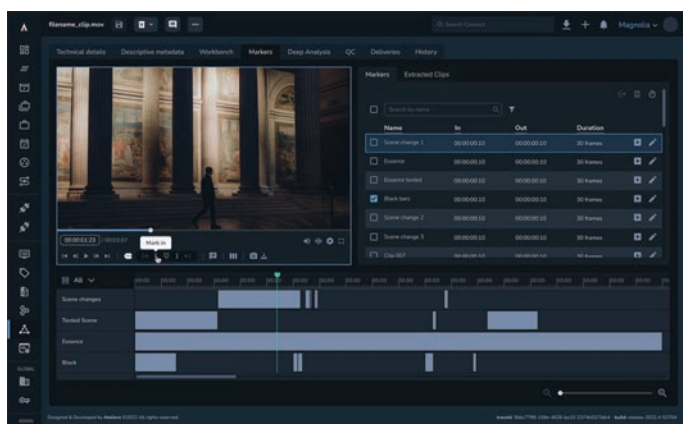


## IT'S NOT A PLATFORM, IT'S PRODUCTIZED PROFESSIONAL SERVICES

Custom scripts demand considerable time and resources for designing, coding, testing, and implementation. As a result, managing custom scripts can be complex, relying on individual documentation practices and developer expertise. If a developer leaves the company, their knowledge and understanding of the custom scripts go with them, potentially creating a critical gap in workflow continuity.

To avoid this, you'll need third-party professional services to manage your custom scripts. Although these services might be wrapped up and presented as a platform (or toolbox), they'll never have the agility of a cloud-native platform. Even though these professional

**EVEN THOUGH THESE PROFESSIONAL SERVICES ALLEVIATE the day-to-day management of custom scripts, these services are costly and drive up ongoing development costs in addition to limiting the amount of direct control companies have over their media supply chain.**



*Ateliere offers a no-code/low-code solution, allowing users to design and configure workflows visually.*

services alleviate the day-to-day management of custom scripts, these services are costly and drive up ongoing development costs in addition to limiting the amount of direct control companies have over their media supply chain. Combined with the time-intensive nature of scripting, it's nearly impossible to keep pace with the rate of change within the media and entertainment industry. This means that any updates will require costly updates or overhauls as technology advances.

## THE RISE OF CLOUD-NATIVE MEDIA SUPPLY CHAIN PLATFORMS

Cloud-native media supply chain platforms, like Ateliere Connect, signify the next evolution in workflow

optimization. Unlike productized professional services and custom scripting, these platforms directly leverage the power of the cloud, enabling media companies to handle large volumes of data smoothly and efficiently. The scalability and flexibility of these platforms allow for rapid response to changes in the industry, ensuring your business stays agile and competitive.

Perhaps most importantly, we offer a no-code/low-code solution, allowing users to design and configure workflows visually without writing any code. This empowers non-technical users to take part in the workflow creation process and frees up IT resources from constant custom script maintenance.

## BENEFITS OF A PLATFORM OVER CUSTOM SCRIPTS

In comparison to custom scripts, our no-code/low-code platform offers numerous advantages which expedites the time-to-ROI for media businesses.

Ateliere's user-friendly platform allows media operators, managers, and QC teams to easily configure and customize their media supply chain. With Ateliere, you can skip the lengthy design, coding, testing, and implementation processes of custom-coded solutions. Our platform enables rapid development and deployment, reducing your time-to-market significantly.

Unlike custom-coded solutions, Ateliere offers pre-built package templates and turnkey functionality, eliminating the need for costly custom scripting and reducing the total cost of ownership (TCO) dramatically.

*Continued on page 77*



*Dan Goman is the founder and CEO of Ateliere Creative Technologies. As a digital trailblazer, he has helped media companies such as Microsoft, Lucent Technologies and AT&T Wireless advance their technology, even managing Microsoft's entire worldwide network as a software developer and network management specialist. [dgoman@ateliere.com](mailto:dgoman@ateliere.com) @TeamAteliere*





# IDENTITY FORCES

The  
future  
of  
talent  
identity  
provenance  
automation

**ABSTRACT:** A new talent ID registration solution has emerged, bringing 21st century supply chain automation — enabling attribution, provenance, and chain-of-custody to the future of smart contracts — to an industry that has been talking about it for years.

**By Will Kreth, CEO, HAND (Human & Digital)**

Systemic change is once again impacting the talent industries of entertainment and sports — and existential questions are on the table. As I write this, the SAG-AFTRA strike settlement (with the AMPTP) has been sent to union members to approve. We all know that 2023 saw a historic work stoppage by both SAG-AFTRA and WGA, and while the main issue of compensation rates over streaming revenues were at the core of the beef, another issue stole the headlines across the mediasphere — and that was, and is, AI.

Rising voices about concerns about the mis-use of generative AI and deep fake technology, whether with the Hollywood talent strikes, or from the White House (with President Biden's U.S. executive order on artificial intelligence), or from the U.S. Senate's Nurture Originals, Foster Art, and Keep Entertainment Safe (NO FAKES) Act of 2023 bipartisan proposal, all have elevated awareness about protecting the autonomy and value of talent's

*IT IS SAID THAT ‘YOU CANNOT AUTOMATE what you cannot identify,’ so, accordingly, the need for tagging and labeling tools — using a standards-based, machine-readable unique identifier, to help attest to the provenance and authenticity of legal persons, their virtual identities, and fictional characters in the value chain — is essential.*

identity essence (their name, image, and likeness, or NIL, rights). Talent and their management will want to be both protected from unauthorized uses of their NIL rights (e.g., like the recent “Dental Plan” Tom Hanks deep fake, and the fraudulent deep fake videos of Mr. Beast, and Scarlett Johansson) — and at the same time, want the option, the agency, to be virtual — to have a digital twin — and will want to properly license, track, and monetize instances and versions of themselves.

With the new three-year SAG-AFTRA contract, actors will “have the right of [informed] consent, and the right to fair compensation anytime some sort of digital replica or replacement of them is used,” according to Duncan Crabtree-Ireland, lead counsel for the actor’s union. The proposed agreement sets a minimum compensation level for AI uses, and actors also are free to negotiate higher payments. The three types of talent that are articulated in the agreement (that we know of) are: Employment-Based Digital Replicas, Independently Created Digital Replicas, and Synthetic Performers (full details on these three definitions can be found online).

But here’s the undeniable thing: it is said that “you cannot automate what you cannot identify,” so, accordingly, the need for tagging and labeling tools — using a standards-based, machine-readable unique identifier, to help attest to the provenance and authenticity of legal persons, their virtual identities, and fictional characters in the value chain — is essential.

#### A BIT OF HISTORY

Since 2017, Hollywood (studios, networks, talent agencies and payment processors) have explored the concept of creating a registry to manage a global, interoperable talent ID standard (a unique, persistent,

machine-readable and freely resolvable ID number, like the Emmy-winning EIDR content ID or a UPC barcode/GTIN number) to automate current costly manual processes of talent ID matching, disambiguation, and verification. All in the service of efficient discoverability, royalty collection, and revenue tracking. Additionally, new privacy laws like California’s California Privacy Rights Act (CPRA, effective Jan. 1, 2023) make it critical that companies (to avoid liability) not use personally identifiable information (PII), like Social Security Numbers, for legal individuals in business and transactional workflows.

And while other media sectors have successfully automated and scaled their supply chains around standardized, unique IDs — such as music (ISRC), advertising (Ad-ID), and book publishing (ISBN) — not so the talent side of the M&E industry.

With the need for a global B2B talent ID registry established, the question of the precise definition of “talent” has emerged. The criteria and critical metrics of talent notability must be defined and articulated — not just for legal entity actors and athletes, but, with the growth of talent participations in 3D video game and virtual world environments, their licensed virtual human identities as well.

A methodology to cover persistent identification of unique performing arts talent in both real and virtual world appearances therefore is key.

Further, with the monetizable NIL rights participation of talent from professional athletics in TV advertising, broadcast, film, video games, and virtual worlds, the registry would be beneficial if inclusive of these identities as well.

Lastly, a well-designed talent ontology would em-

*Continued on page 79*



*Will Kreth is the founder and CEO of HAND (Human & Digital). He has been involved in broadband and digital media for more than three decades and is the former executive director of the Entertainment ID Registry (EIDR), director of metadata governance at Showtime Networks, and director of video product management at Charter/Time Warner. Kreth is also the working group co-chair at the music industry’s standards body Digital Data Exchange (DDEX) and co-chair of the standards register working group of the Metaverse Standards Forum. [wk@handidentity.com](mailto:wk@handidentity.com) @wkreth*



# THE PSYCHOLOGY BEHIND USING MUSIC IN VIDEO GAMES

The study of video game music continues to show surprising psychological impacts

**ABSTRACT:** This article serves as an insight into the psychological implications of ludomusicology, and several studies have emerged that comment on the immersive experience, better player performance, and physiological impacts of using music in video games.

By Emily E. Garcia, Senior, Tulane University, Intern, RSG Media

There has been a relative boom in gameplay research that has brought about a new understanding of the multi-dimensional relationship between music and play, allowing players to feel more immersed in a video game.

The study of video game music is referred to as ludomusicology. This term takes into consideration the anthropological, psychological, cultural, societal, economic, and musicological aspects of the music used in video games. Furthermore, it examines multiple facets of video game music such as its history, audio, interactivity, technology, and composition of the music. The psychological implications of ludomusicology are of keen interest as several studies have emerged that comment on the immersive experience, better player performance, and physiological impacts of using music in video games.

Gameplay models represent key elements that structure the gameplay experience as it relates to all modes of immersion factors. They illustrate the complex internal organization of a game and focus on the consciousness structured by the interplay. Examples of gameplay models include the SCI model and the ALI model. The SCI model is a heuristic model that includes three components:



sensory, challenge-based, and imaginative immersion. Sensory immersion is when the player becomes entirely focused on the game world and its stimuli. This can sometimes be accomplished with large screens close to the player's face and powerful sounds. The goal being to overpower the sensory information coming from the real world.

Challenge-based immersion is achieved when there is a satisfying balance of challenges and abilities whereas imaginative immersion is when the player becomes absorbed with the stories and the world of the game. Another representation of gameplay is the ALI (affect, literacy, interaction) model. The ALI model seeks to explain the meaning and identification of video game music. The three components are musical affect, media literacy, and interaction. This model emphasizes the importance of the emotional connections that video game players create through music. Affect is related to memory, emotion, and identification and is often driven by media literacy. Players who have previous knowledge of certain tropes and musical conventions can assimilate at a subconscious level through other audiovisual media.

### PLAYER EXPERIENCE

As supported by the ALI and SCI models, music plays a key role in the feeling of being immersed in a game. The player begins to feel as though they are “there” in the world when the game creates spatial presence. Spatial presence involves using images, movement, sounds, etc. in the game to help the player, either consciously or subconsciously, form a mental model and decide whether they feel as though they are in the imagined world. Immersion is the feeling of being completely enthralled by the other reality that it takes over all our attention, and entire perceptual system. The creation of this illusion is often closely connected to the entertainment value of the game. Feelings of immersion are often reported alongside a lack of awareness of time. The addition of music has been shown to increase spatial presence, or the players' sense of being there. Background music is suggested to make the video game environment more authentic and convincing, allowing the player to form a richer mental model of the game world.

The music in video games can be used to facilitate certain experiences for the players. For instance, by

*AS THE SCIENCE PROGRESSES IN the field of ludomusicology, investment will surely follow. Coupled with technology advances, there will be an evolution to sounds and music found in the newest games.*

creating an association between musical sounds and actions or situations, auditory cues can be used to improve not only the experience but also the performance of the player. Sound features can provide basic information to the player within the game, such as if certain points have been achieved through an action, a mission was completed, or if the player has enemies waiting up ahead. A high pitch sound, usually that of a small bell, is commonly associated with a reward whereas an ascending or descending glissando signifies an increase or loss of energy of the character. This type of relationship assumes the player recognizes the integration of the elements of the sound to the mechanics of the video game. Accordingly, the player can decipher the meaning and make in-game decisions.

Background music complements the gameplay by creating a new attractive world for the user to escape to and can reinforce the story within the game. Game soundtrack music may not only trigger individual associations, but can also activate memories of related media experiences, such as movies (characters, scenes, actions, etc.) that might influence the player's imagination and their overall game enjoyment. When video game players can recognize the musical traits and composition used in the game, they become more actively involved in the dynamics of the world. During the development of game music, composers will create sounds and music that fit into the overall narrative setting, mood, and visual aesthetics of the world. Furthermore, the soundtrack will often be congruent to what is happening in a game situation. For the player, if the instruments and sounds are consistent with the game's world, they are likely to feel that the world is more realistic and legitimate.



*Emily E. Garcia is a senior at Tulane University, with a double major in neuroscience and psychology and a minor in strategy, leadership, and analytics. Upon graduation, she plans to pursue her doctorate in cognitive neuroscience with a focus on neurocinematics and neuromusicology. This whitepaper is a product of her internship at RSG Media during the summer of 2023 as part of a consulting engagement with one of their clients.*

Music can be used as a storytelling tool by accentuating the emotions and themes of the story, especially those that might recur throughout the game. Furthermore, music can reinforce the emotional impact of story events to the player, such as battle scenes. The development and evolution of a musical theme over the course of the story reinforces the connection and emotion of the changes to the character or place. In addition, it can help the player represent these elements in their minds which can allow them to better remember them later. Furthermore, music can be used as a guiding measure through the game. It can help the player remember different elements of the story that are associated with a melody and musical pattern and, thus, strengthen their emotional connection to those elements. In this way, the player will feel more immersed in the story and the world of the game.

Music can also reinforce immersion by targeting the emotional effect of the player. Studies have shown that the elements in music can trigger or amplify specific emotions in players. For instance, if a game contains music fragments of rapidly changing frequencies, non-standard harmonies, or those that imitate animal cries or screams, during the appearance of a boss enemy, the game is likely to either activate or intensify the emotion of fear. Overall, the effects of soundtrack music in video games have been linked to greater positive emotional response and enjoyment during gameplay due to the extent that players value more intense emotions.

This effect also applies equally for positive emotions elicited from video game music, such as the feeling of relief and pride the player experiences when listening to joyful music accompanying the defeat of the boss enemy. However, according to one study, players were more immersed when they enjoyed the music. Thus, a badly designed soundtrack may hinder a player's ability to feel immersed in the game. Music soundtracks, when developed appropriately, reinforce the player's emotional connection to the story, characters, and the game world.

## PLAYER PERFORMANCE

Not only does music heighten the immersive experience of the player but it can also improve their performance in the game as well. According to one study, music present in video games increase the player's high score, as male gamers were able to score almost twice as many points while playing the first-person shooter game *DOOM* with the sound on compared to those playing with no sound. In other studies, results were more complex. While playing a driving game, people playing with "highly arousing" music drove the fastest but made the greatest number of mistakes, such as hitting barriers or knocking over road cones. However, in role-playing games, such as *Legend of Zelda*, players performed worse when playing with both music and sound effects off. As more game audio was progressively added, performance improved.

According to the same study, participants performed best when playing with background music on a boombox that was unrelated to the game. Similarly, another study has shown that the presence of self-selected music by the player increased not only their enjoyment of the game, but also their performance. Players were more efficient,

perceived lowest distraction, and experienced a reduction in tension-anxiety compared to when researchers selected high arousing music. A reason why player performance improves with music could be due to greater proactive cognitive control when music is playing. Background music might add cues to the game, such as linking sound patterns to enemy attacks that will allow time for the player to make an appropriate response or quickly modify their behavior. In turn, they will begin to memorize and recognize certain musical cues in the game, which can help them improve their performance in the future.

## PHYSIOLOGICAL IMPACTS

Lastly, the physiological impacts of music in games are also of great research interest. Studies have shown that there is an increase in cortisol levels when music accompanies gameplay showing that the auditory input contributes significantly to the stress response found during video game playing. Studies have shown that there are effects of sound on physiological activity. For example, classical music has been shown to elicit relaxing effects on the listener, as well as cause a decrease in blood pressure and heart rate. On the other hand, when listening to rock/ techno music, listeners experienced increased self-ratings of anxiety, aggressiveness, tension, and discomfort. Furthermore, the participants were found to have significant increases in heart rate, systolic blood pressure, and cortisol levels when listening to heavy metal music, rock, or techno music. "First person shooter" games generally use techno and rock music and, therefore, the effects found in this study are representative of those that would be obtained with those games.

Music in video games, whether it be soundtracks originating from music compositions created specifically for the game or music derived from the adaptive reuse of orchestral compositions that originated from the production of a TV show or movie, or simply sound effects meant to accentuate an action, have been shown to enhance the experience. Original music created for games has found new revenue streams as stand-alone content repurposed for advertising, ringtones, or other film/tv content, both long form and short form. Enormous numbers of user generated content found on TikTok or YouTube readily utilize music from games. Because of the impact on the user experience and the potential for revenue streams beyond the purchase of the game, gaming companies are investing in the creative process to produce original music for their games. This trend has opened new opportunities within the creative community. The empirical evidence has influenced this investment.

As the science progresses in the field of ludomusicology, investment will surely follow. Coupled with technology advances, there will be an evolution to sounds and music found in the newest games. Within most major game producers, there are many composers, voice actors, foley artists, and sound engineers that make up their incredibly large sound department. New technologies centered on AR and Generative AI will challenge these music artists to create more immersive experiences and soundscapes within the game experience. The future of ludomusicology will be fascinating, no doubt. ■



## Speed or Security?

With Fortinet, You Can Have Both.

The shift to Direct-to-Consumer platforms has made M&E companies popular targets for disruptive cyberattacks. With customer expectations that services “just work,” delivering anything less than high-quality, reliable streaming is unacceptable. But many vendors can’t securely scale to meet customer demand, turning off security controls in favor of speed.

Fortinet solves this problem with ultra-low latency next-generation firewalls. Our custom ASICs deliver up to 36x better performance than competitor firewalls. Now you can deliver fast and secure entertainment experiences. To learn more, visit [www.fortinet.com/m&e](http://www.fortinet.com/m&e)



# UNLOCK THE VALUE OF YOUR CONTENT WITH AI

AI technology is having profound impacts on automating various aspects of content creation, organization, and distribution

**ABSTRACT:** In today's fast-paced digital landscape, the integration of AI and automation has emerged as a game-changer for content management. This article explores the profound impact that AI technology is having on automating various aspects of content creation, organization, and distribution.

**By Jade McQueen, VP, Managing Director,  
Media and Entertainment, Box**

Every business has two types of data: structured and unstructured. But while the typical organization has a handle on its structured data — which can be organized in a database — most don't take full advantage of their unstructured data. In media and entertainment, this includes all the files, videos, PDFs, raw imagery, VFX files, finance spreadsheets, production and release schedules, and other types of content businesses produce every day.

Ninety percent of an organization's data is unstructured, yet 41 percent of companies say less than half of content gets reused.

The media and entertainment market is expected to grow from \$27.72 billion in 2023 to \$40.36 billion by 2028, at a CAGR of 7.80 percent during the forecast period (2023-2028). To make the most of this new golden era, every media and entertainment company needs to have a strategy empowering creative teams to bring stories to life. You also need to streamline your workflows and

## AI WILL DRIVE A GENERATIONAL SHIFT in how people work, and nowhere is AI more powerful than within enterprise content.

get your productions to market faster. And you need to accomplish all this while protecting critical IP and maintaining proper compliance and governance. This is where AI and automation come in.

### THE FUTURE OF WORK WILL BE POWERED BY AI

The amount of content organizations produce is growing rapidly. By the end of this year, organizations globally will have created 73,000 exabytes of unstructured data. That's a lot of content. Now, with the rise of generative AI, organizations will be able to take advantage of this untapped resource more than ever before. AI will drive a generational shift in how people work, and nowhere is AI more powerful than within enterprise content. Earlier this year, we announced Box AI, which will shine a light on all your unstructured data, illuminating your content so you can extract value from it. And, because that content is housed in Box — a single, secure content platform — you can leverage Box AI securely and apply it across your organization.

### BOX AI: BREAKTHROUGH AI MEETS ENTERPRISE-GRADE SECURITY, COMPLIANCE, AND PRIVACY

Over time, you'll see Box AI infused across many Box products and features. To start, we're excited to share our first Box AI releases across previewing files and Box Notes. You can preview over 200 document types in Box and apply Box AI (via a chat-like feature) to PDFs, PPTs, DOCs, and more — summarizing long-form information such as scripts, pulling out key insights on releases, and quickly crafting new content such as social media campaigns based on content you already have. Plus, with Box AI in Box Notes, users can generate content on command, refine it as needed, and securely save it automatically in Box. Box AI will begin rolling out to Box Enterprise Plus plan users in beta later this fall.

### INTRODUCING BOX HUBS

Teams typically spend a lot of time — and IT spends a lot of money — on tools to organize finalized content and distribute it to stakeholders. Not anymore. Meet Box Hubs: customizable portals that help you surface great content across and beyond your organization, quickly and securely.

With Box Hubs, we've simplified the way teams curate, organize, and distribute content. From cast and crew resource portals to production wrapping sites, and marketing sites, or anything in between, your teams can easily consume updated, source-of-truth content from intuitive, secure portals and share information securely with external partners. Create a Hub at the click of a button and customize it with links to any content or folder within your Box account, all without needing to move or copy that content and risk versioning or compliance issues. Think of it as a playlist — but for your content.

Box AI will also be added to Hubs, so you can harness the power of your content like never before — directly from the search bar. Looking for a particular document? Box's powerful engine will route your query to search. And if you want to dig in and understand complex concepts across the curated contents of a Hub, you can ask Box AI any question and receive AI-generated answers such as summaries, information analysis, and more, across multiple files within your Hub, right away.

Box Hubs will be available to all Box users on Enterprise plans and above, with intelligent Box AI-powered Hubs available to Box Enterprise Plus plans. To learn more, visit the Box Hubs website, check out the deep dive on the Box blog, and look for the beta next year.

### NATIVE DOCUMENT GENERATION IN BOX

Organizations today are dealing with too many tools to manage their content workflows. One such standalone

*Continued on page 73*



*Jade McQueen is the VP and managing director of media and entertainment at Box. She began her career as an A&R executive at DreamWorks and Interscope Records. After 10 years in music, she transitioned to film and TV where she wrote, directed, and produced. [jade@box.com](mailto:jade@box.com) @Box*

## WITH *Continued from page 14*

■ **KCAI Mentorship Program:** We facilitate a group mentorship initiative focused on connecting high-performing diverse technologists with executive advocates and allies in the media and entertainment industry. Its goal is to empower participants to drive positive change in their communities and workplaces, with each knowledge circle offering opportunities for peer learning, networking, and professional development.

### *WiTH's impact in numbers*

WiTH's commitment to making a difference in the lives of women in technology is evident in our impact:

■ More than 700 lives impacted throughout the charitable organization that we support

■ \$100,000 donated to support new technology, scholarships, and educational opportunities

### *Get involved and support WiTH*

Supporting the Women in Technology: Hollywood Foundation is crucial to advancing our mission. There are several ways to get involved:

■ **Donation:** You can donate directly to support our efforts. Your

contributions help us continue our work in empowering women in technology.

■ **Newsletter subscription:** Stay up to date on women's initiatives in the entertainment technology field by subscribing to our weekly newsletter.

• **Committee participation:** If you're looking to actively contribute to the industry's progress, joining one of WiTH's committees is a great way to make an impact.

### *Be a part of our story*

In the world of media and entertainment technology, where technology creates the canvas for dreams, WiTH Foundation is weaving a narrative of unity, belonging, and empowerment. Together, we can turn aspirations into achievements and create a lasting impact that resonates far beyond Hollywood's horizons.

Join us in scripting a new narrative where inclusion is the spotlight's true star. Support the Women in Technology: Hollywood Foundation and be a catalyst for change in the industry. Connect with us at [withollywood.org](http://withollywood.org) or [hello@WiTHollywood.org](mailto:hello@WiTHollywood.org).

Let's create a world where technology is a canvas for all dreams, and every aspiring technologist finds their path to success. ■

## EIDR *Continued from page 10*

within your own systems. The issue is compounded when we pull distribution partners into the mix. As a consumer, it is incredibly challenging to find content considering the vast array of streaming services because most consumers do not follow the industry closely enough to know which studio or streamer has the content they want to see.

These days, a lot of conversations about the future are centered around content discoverability. How can we help viewers to navigate the streaming landscape, anyplace, anytime, on any device? How can we ensure that the content they want is available? How can we improve the overall experience that streaming customers are having? How can we cleanse and prevent bad data or untagged or mis-tagged assets from polluting the environment? If an asset (or any of its accompanying assets) is misidentified or is missing key metadata, it is invisible to search mechanisms.

It is a reminder of a question we were asked to answer in philosophy courses in our university days. It is an ages-old question, "If content is tagged incorrectly, does it exist?" ■

## BAINES *Continued from page 12*

evolve as technology innovations develop and become more pervasive and MESA's work with the Content Localisation Council will only build and strengthen as these changes take place. As an association we embrace all sectors of the localization industry including academia and freelance translators and we will continue to work with players large and small to ensure we engage in full and open collaboration.

So, what's the next step? We are just getting started on this new journey and want to encourage our localization community to get behind the initiative and help us to drive it forward. We will have a sign-up page on the website, which will enable anyone who wants to get involved to register their interest. We also have some key events coming up which will provide an opportunity to discuss ideas, enlist support and begin to plot a roadmap for the months ahead. For more information on the Content Localisation Council or to get involved with the Cloud Localization Blueprint, please email [caroline.baines@MESAonline.org](mailto:caroline.baines@MESAonline.org). ■

## ASCENDION *Continued from page 30*

DRM, and AI, and other cutting-edge technologies to bolster its anti-piracy and cybersecurity efforts. Collaboration, education, and a proactive approach are essential in safeguarding creative content and intellectual property in this ever-changing landscape.

By adopting the right strategies, the M&E industry can strike a

balance between accessibility and security, ensuring a prosperous future for content creators, distributors, and consumers alike to thrive and remain resilient in the face of an ever-evolving digital landscape. ■



## BOX *Continued from page 71*

tool is for document generation, which has to be stitched together with the rest of the workflow. IT has little time to spend cobbling together these separate tools, which also lead to siloed data and higher business risks from inconsistent security and compliance. This also means more manual steps for end users, breaking the workflow and leading to unnecessary human errors and a fragmented user experience. To address the above, a new native document generation capability, called Box Doc Gen, will enable you to automatically generate custom documents on the fly natively in Box from multiple data sources. The best part: it works seamlessly with the rest of your secure content workflows in Box.

Box makes document generation simple. Author your document templates with our Box Doc Gen add-in for Microsoft Word, map your data sources (for instance, customer info from Salesforce or inventory levels from your ERP system), and leave the rest to Box Doc Gen. Boom — out come professional-looking documents, formatted exactly as you desired. Zero exporting, no uploading, sans typos. You can mix and match data sources, and even use Box metadata. Whether you're looking to get customized documents signed, like NDAs and talent agreements, or automatically create client-specific reports that are securely stored and shared in the Content Cloud, Box Doc Gen will be a gamechanger. We're taking an API-first approach so you can tackle your high-volume use cases first. Look for the Box Doc Gen API private beta next spring.

### SECURITY GETS BETTER AND STRONGER AT BOX

With the estimated cost of a data breach in 2023 at \$4.5M, protecting your growing volume of content is paramount. Having every-

thing centralized in one place — the Content Cloud — is the first step to strong security.

First off, we're excited to announce our new partnership with CrowdStrike, a global security leader, that will help organizations of all sizes secure their data in the cloud and stop data-related breaches. Included in the partnership is a new integration where Box will leverage CrowdStrike Falcon Zero Trust device risk signals to reduce the risk of malware infiltration and data breaches by preventing unsecured or potentially compromised devices from accessing content in Box. This integration empowers joint customers to bring together powerful contextual insights from device posture and data access to evaluate risks in real-time, build granular policies and take remediation actions.

Box Shield will ingest a risk score from CrowdStrike, determined from several variables including built-in OS security options, firmware availability, and CVE mitigations. Box admins can use this risk score to automatically terminate user sessions and block login from devices determined to be high risk, protecting the organization from compromised devices. This new integration expands content protection across the entire cloud-to-endpoint-to application estate, bringing an extra layer of security without getting in the way of work.

### A NEW ERA FOR MEDIA AND ENTERTAINMENT IS HERE

With one secure platform — and the power to harness the incredible value of your content — your business can capitalize on new, intelligent ways to captivate your audiences. There's never been a better time to streamline data security and simplify production. Learn more at [box.com/overview](https://box.com/overview) today. ■

**M+E**  
TECH JOB BOARD

The #1 resource for  
technology career  
opportunities in  
Media & Entertainment.  
[www.mesaonline.org/jobs](https://www.mesaonline.org/jobs)





# Leading the Future of Security in Media + Entertainment

## CDSA MEMBERS

2G Digital • Adobe • Amazon Studios • AWS • Amblin Entertainment • Apple  
ARM • BBC Studios • BeBop Technology • Bob Gold & Associates • Buy DRM  
CineSend • Cognizant • Convergent Risks • Creative Future • Deluxe  
Digital Silence • Eluvio • EZDRM • Fastly • Fortinet • Fortium • FriendMTS  
Funko • Google Cloud • Hasbro • Huawei Cloud Computing • IDC Digital  
Indee • PallyCon • Irdeto • Iyuno • Jakks Pacific • Keywords Studios • LADB  
Legendary • LEGO Group • Lionsgate • MESA • Microsoft • Microstrategy  
NAGRA • NBCUniversal • Netflix • OpSec Security • Paramount • Pixelogic  
Resillion • Richey May • Riscure • Secure the Village • SHIFT • Signiant  
Skydance • Softtek • Sohonet • Sony Pictures Entertainment • Synamedia  
Taksati Consulting • Technicolor • Testronic • The Walt Disney Company  
TPOP • Vision Media • Vubiquity • Warner Bros. Discovery • Wasabi  
Widevine • Xcapism Learning • XL8 • Zixi

■ *They only know what you tell them. Trained models that are not maintained can quickly become irrelevant or outdated.*

■ *It's not a one-and-done, standalone solution. Implemented models need continual fine-tuning, integration, and updated APIs to make them effective.*

■ *Your data's biases become their biases. Models can come pre-trained on data. This data can be biased, hard to remove and make the downstream application biased.*

■ *It's not always acceptable for high-risk applications; models can still have vulnerabilities and get answers wrong depending on the model architecture.*

When it comes to implementing AI solutions, organizations need to build their technical ability to support new products, but equally as important is to consider governance, ethics, and legal processes around AI tools. Keep in mind that AI:

■ *Is a probabilistic model – expect the unexpected: AI is not designed to obey strict policies; therefore, restricting its responses' spectrum could prove complex in practice.*

■ *AI is trained on data that you need to supply. In many cases, the*

*data needs to be delivered to the model's company (i.e., OpenAI), and you need to ensure they have security of the data.*

■ *AI accumulates data to continuously refine and improve, so removing data from its knowledge base is not straightforward.*

With great AI power comes great AI responsibility. At EPAM, we have had a lot of experience building and implementing responsible AI solutions to address these challenges and limitations. It's critical to take a holistic approach when you're building a responsible AI solution to make sure it's explainable, ethical, and trustworthy so that you can have confidence around what it does, why it does it, and that doing things in a secure manner, while making sure it's considering business context and adhering to governance and laws so that you have a truly responsible AI solution.

## CONCLUSION

I just want to leave you with this final thought. The use of AI is still early on and we're still writing the narrative for how it'll impact the M&E space. Keep in mind that it's not a silver bullet on its own, and its impact lies in the intersection of people, processes, and tools. How we responsibly leverage AI, and that balance is what will determine whether AI is an opportunity that can help the M&E industry accelerate and grow together, or whether it's a threat where we'll be left behind in its wake. ■

# MESA

# UPCOMING EVENTS

## 2024 SCHEDULE

- **28-29 February** - LONDON
  - ITS: Localisation (event)
- **14-17 April** - NAB in LAS VEGAS
  - CDSA's CPS@NAB (event)
  - MESA Las Vegas (reception @NAB)
- **21-22 May** - LOS ANGELES
  - Hollywood Innovation + Transformation Summit (HITS)
  - EIDR Annual Participant Meeting
  - WiTH@HITS
- **19-20 June** - LONDON
  - Content Localisation Council (meeting)
  - CDSA Working Group (meeting)
- **13-16 September** - IBC in AMSTERDAM
  - ITS: Automation! (event)
  - Amsterdam (reception @IBC)
- **9-10 October** - NAB NEW YORK
  - M+E Networking Reception
- **7-8 November** - LOS ANGELES
  - WiTH SoCal Women's Leadership Summit (event)
- **18-19 November** - LONDON
  - Content Localisation Council (meeting)
  - CDSA Working Group (meeting)
- **2-3 December** - LOS ANGELES
  - CDSA Content Protection Summit (CPS)
  - MESA Holiday Party



Learn more at: [MESAonline.org/events](https://MESAonline.org/events)



## MESA AD INDEX

MEMBER	PAGE	WEBSITE	MEMBER	PAGE	WEBSITE
Altman Solon .....	43 .....	altmansolon.com	HAND (Human & Digital) .....	51 .....	handidentity.com
Box .....	2 .....	box.com	International Digital Centre .....	55 .....	idcdigital.com
Content Delivery & Security Association (CDSA) .....	69 .....	cdsaonline.org	M+E Job Board .....	73 .....	mesaonline.org/jobs/
Content Delivery & Security Association (CDSA) Spoiler Alert .....	74 .....	clwg.cdsaonline.org	MEDCA .....	46 .....	medcaonline.org
CineSend .....	41 .....	cinesend.com	MetaBroadcast .....	61 .....	metabroadcast.com
Collot Baca .....	35 .....	collotbaca-sub.com	OOONA .....	11 .....	ooona.net
Convergent Risks .....	53 .....	convergentrisks.com	Reelgood .....	49 .....	reelgood.com
Deluxe .....	9 .....	bydeluxe.com	Verimatrix .....	37 .....	verimatrix.com
Digital Bedrock .....	47 .....	digitalbedrock.com	Vistex .....	45 .....	vistex.com
EditShare .....	33 .....	editshare.com	VSI .....	31 .....	vsi.tv
Fastly .....	83 .....	fastly.com	Wasabi .....	13 .....	wasabi.com
Fortinet .....	69, 84 .....	fortinet.com	Women in Technology: Hollywood (WITH) .....	80 .....	withollywood.org
Gracenote .....	5 .....	gracenote.com	Zixi .....	15 .....	zixi.com
			ZOO Digital .....	17 .....	zoodigital.com

## ATELIERE *Continued from page 63*

ly. Our platform is designed to adapt to emerging technologies and quickly onboard new delivery partners, ensuring your business stays competitive.

Maintenance is also simplified with Ateliere's platform. Package templates are componentized, allowing for easy modification and adjustment of delivery profiles, reducing reliance on professional services and associated maintenance costs. Our platform is built by a team of industry experts, ensuring stability, reliability, and minimizing the risk of system failures or disruptions.

Lastly, Ateliere's platform offers an agile and adaptable workflow. The no/low-code approach empowers users to select preset configurations and build business logic without programming or scripting knowledge, enabling quick response to changing demands and maintaining competitiveness.

## A BRIGHTER FUTURE

In today's ever-evolving media industry, it is crucial to embrace new and efficiency-maximizing solutions to maintain a competitive edge. While custom scripts have served their purpose in the past by automating tasks and enhancing workflow efficiency in the media supply chain, it's time to acknowledge the challenges and business risks associated with them. The future lies in adopting cloud-native media supply chain platforms that offer a no-code/low-code approach. With these groundbreaking platforms, media companies gain greater control over their supply chain, experience heightened productivity, and achieve significant cost savings. It's time to step into the future and leave behind the pitfalls of custom scripts. ■

## FINLEY *Continued from page 6*

come in, and who's embraced it and how the studios have evolved their thinking around their supply chain, and not ascribe to the old theories of vendor lock, everything's turned into a value proposition. That's where MESA shows its true colors and it is through the organizations we manage that the "get sh\*t done" mentality in working groups starts to save our industry money on orders of magnitude.

Let's start with CDSA, an organization near and dear to me because my grandfather started it in 1970 as the International Tape Association (ITA). After enduring an incredibly difficult pandemic year, CDSA and its president, Richard Atkinson, moved away from an audit and compliance-driven business focus to member companies self-organizing and driving their own issues to be discussed in a working group. Common problems need common solutions, this is CDSA's mantra, and Richard provided a clear path for members to identify the issues where they wanted to work most. Richard is a subject matter expert, there's no doubt about it, and that expertise helped take the community/association to the next level.

Hollie Choi does the same thing with EIDR, which is less a trade association and more a community around their product that performs a critical role inside of our industry. And, again, having somebody who knows exactly what that product is, does, and can do, has transformed their business. EIDR came out of their austerity plan this year and Hollie's understanding of where EIDR sits in the global entertainment supply chain, along with what the value proposition is to the industry as a whole, is what's allowing it to be successful.

WiTH and their president, Christina Aguilera, are another shining example of self-organization at its finest! Rarely do you find a charitable organization where almost 95 percent of the money raised gets delivered back to the local charities they support. Starting in 2014 as a special interest group within MESA, WiTH formalized their board in 2019 and continues to grow and build leaders for M+E, all in the name of advancing wisdom, skills and careers across our global industry.

Then you have the Content Localisation Council championed by MESA's Caroline Baines. No one has their finger on the pulse of localization like she does and no other segment in our industry is facing the scale/globalization issues that these Language Service Providers are solving. Eight years old now, the Content Localisation Council is making more headway in addressing industry issues across the supply chain than it ever has before.

By modifying the content to serve different markets or demographics you're making it "smarter" and this leads into both Smart Content Council, led by Mary Yurkovic, and the Language Metadata Table, led by Yonah Levenson. These SMEs (along with Hollie and Caroline) are creating a community of data custodians, data librarians, and data enthusiasts. They care about that field level data that makes the global supply chain work. And when you start talking about AI, our industry's future, and where we're all going, we've got to be automated and integrated for Artificial Intelligence to be a viable option. AI2 is the theme of HITS, our tent-pole event every year, on May 22 in Los Angeles.

And speaking of AI, too fast, too much, too soon is not something that Hollywood does well. We'd rather tell stories the old-fashioned way than take a risk on something new or outside of the box, especially at scale. And after getting through arguably the worst three years of our lives (start with a pandemic and end in a 100-plus day strike) we have to start wondering, where's the hope? Yes, there is more pie, there is more content, there is more everything in our future, but who are you holding on to (or throwing under the bus) while you get there?

That's where MESA's message is salient. We're the heartbeat of the global entertainment supply chain. We take risks as vendors and help bring our content creator customers into the next era of entertainment. Sometimes they push, sometimes we pull. But no other trade group provides a home for a community when that community is so new and unknown that many in Hollywood don't get it. And ahead of MESA's 15th anniversary, we're proud to continue to take risks that are centered around innovation. ■

bounds of licensing agreements, which may restrict the extent to which content can be modified or distributed. Organizations must conduct thorough reviews of licensing agreements, ensuring that AI-generated content complies with the terms and conditions set forth.

Moreover, AI's involvement in content creation can raise concerns about meeting contractual obligations. For example, if a company uses AI to produce content for a client, they must ensure that the content aligns with the agreed-upon terms and quality standards. It is crucial to establish clear contracts that outline the scope of AI involvement, quality expectations, and mechanisms for dispute resolution.

## SECURITY RISKS

AI systems can exacerbate security risks and create new ones. AI models, particularly those used for content generation, may be vulnerable to cyberattacks, including adversarial attacks that manipulate the AI's output. To protect against such threats, organizations should regularly update AI models, implement robust security measures, and conduct penetration testing to identify vulnerabilities.

In addition, AI relies on vast datasets, which can contain sensitive information. Mishandling or inadequate protection of these datasets can lead to data breaches, resulting in significant legal and financial consequences. Organizations should prioritize encryption, access controls, and data protection protocols while adhering to data privacy regulations.

## AI AND DATA PROTECTION

UK and EU GDPR laws have disrupted the way organizations around the world are required to protect personal data. The processes through which businesses collect, process, store and share personal data have irreversibly changed, and as more of these organizations use AI technologies as a part of their business processes, data protection laws are being extended to accommodate these new and emerging technologies.

The UK's ICO has identified AI as a priority area and advises organizations to take a risk-based approach when developing and deploying AI. Specifically, the ICO recommends that organizations assess whether they need to use AI for the context it will deploy it in - AI is generally considered a high-risk technology and there may be a more privacy-preserving and effective alternative.

Where an organization does develop and/or deploy AI, it needs to assess the risks and implement appropriate technical and organizational measures to sufficiently mitigate them. It is impossible to realistically remove every risk (and data protection law does not require organizations to do so) however, certain measures should be taken to ensure accountability:

■ *Take time and dedicate resources to ensure the quality of the data inputted into the AI system – preparing the data to train an AI system will result in better outputs.*

■ *Conduct a data protection impact assessment (DPIA) to help identify and minimize the risk of non-compliance with applicable data protection legislation that the use of AI poses, as well as preventing harm to individuals.*

■ *Be clear, open, and honest with people within a privacy notice about how and why you use their personal data and consider what explanation is needed in the context that you will deploy your AI system in.*

■ *Obtain user consent for data collection and specific processing purposes where required. Users have the right to know how their data is being used and to have the option to opt out.*

■ *Obtain documentation from any supplier that demonstrates a data protection by design approach.*

■ *When using AI for decision-making, decide whether to use it to support a human decision-maker, or whether it will make solely automated decisions — under the GDPR, individuals have the right not to be subject to solely automated decisions with legal or similarly significant effects.*

■ *Ensure that informed consent of use is obtained for personal data that is collected and used for AI training. When sensitive personal data, such as voice, is being used, obtain explicit opt-in consent of use, and make sure data subject consent is updated on a regular basis.*

■ *Securely store personal data used for training AI. If it's not adequately protected, it can become vulnerable to data breaches, leading to unauthorized access and exposure of private information.*

■ *Determine who owns the personal data used for training AI. Ownership can be a complex legal and ethical issue. Individuals may expect that their data is being used solely for their benefit and using it for AI training purposes without their consent can raise questions about data ownership and control.*

## RISK VS. REWARD

The adoption of AI in content creation and localization offers transformative benefits but carries a profound responsibility to address legal, security, and data privacy risks. Concerns surrounding copyright infringement, data mishandling, and vulnerabilities to cyber threats demand meticulous attention. Achieving the ethical and legal compliance required for training AI and in AI-driven processes necessitates a comprehensive strategy that safeguards information while harnessing the power of automation responsibly. As technology continues to advance, organizations must remain vigilant in protecting both their interests and the privacy rights of their users and clients. ■



**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. ■

---

**HAND** *Continued from page 65*

brace the identification of fictional characters (e.g., Barbie, Spider-Man, Batman, etc.) interchangeably portrayed on screen and stage by the aforementioned legal entity/natural persons.

HAND (Human & Digital) is just such a new talent ID registration agency, operating as a B2B/SaaS platform under the nonprofit Digital Object Identifier (DOI) Foundation (ISO 26324:2022, est. 1997), serving the research and scientific community, as well as EIDR, and currently managing 308 million unique IDs at 1.3 billion ID resolutions per month.

As the first talent ID designed with the business and IP needs of Hollywood and sports federations in mind, the HAND Talent ID brings 21st century supply chain automation to an industry that has been talking about it for years. And as future revenue potential

for top-level talent undoubtedly includes virtual participations, HAND Talent IDs are both metaverse ready and blockchain ready, enabling attribution, provenance, and chain-of-custody to the future of smart contracts. Attestations of authenticity that matter.

HAND's platform is now in beta, working with notable companies such as the American Film Institute, Fabric Data, Wild Capture, Nash Info Services, The Scan Truck, and MetaRex Media, and in discussions with international film studios and TV networks. We welcome companies who are interested in joining our B2B Beta Partners Program and look forward to announcing general availability of the freely-resolvable HAND Talent ID for use in global workflows in 2024. ■

---

**VUBIQUITY** *Continued from page 42*

that they are observing all the required security regulations. For operators, it reduces investment in infrastructure, which requires all operators to meet the same standards. It simplifies their media operations and allows the ever-increasing cost of security compliance to be amortized, by the cloud providers, across multiple operators.

**CONCLUSION**

Whilst there will always be operators who want to 'own' this technology, most operators view these security tasks and measures as "things that just need doing."

To do those things more efficiently, securely, and cost-effectively,

Vubiquity believes that a shared cloud-based content repository addresses the needs of both the studios and the operators. Media delivery has become commoditized, and cloud-based delivery is an ideal solution for operators who want to offer as much streaming content as possible while minimizing the growing costs and complexities of doing so. Does such a solution exist? Yes ... enter Content Cloud! Content Cloud is Vubiquity's streaming solution that ensures studios' content protection (and usage) rules are followed, amortizes the cost of development across numerous operators and allows them to keep pace without having to continually re-justify investment into their business. ■

INTRODUCING...



**WiTH** | women in  
technology  
hollywood



**WiTH  
BELIEVES IN:**

**MAKING A DIFFERENCE**

Lifting the aspirations  
and careers of one,  
raises all

**BELONGING**

Celebrating and respecting our  
differences while making space where  
we can unleash our unique genius

**CURIOSITY**

Exploring paths to fuel  
learning and growth

**LEADERSHIP**

Blazing new trails to  
confidence, courage, vision,  
and joy

**THE PILLARS OF WiTH**

Where WiTH members get into action:

- **Professional Development** — leverage our resources to broaden our collective expertise
- **Mentoring and Networking** — connect, inspire, and encourage each other while fostering growth in our professional network
- **Community Engagement** — be avid ambassadors of technology by encouraging youth to pursue careers in our field

**WITH EVENTS**

The members of WiTH gather\* at these events:



- **WiTH Leadership Awards** — honoring contributors who serve as role models and mentors and who empower women to be bold leaders



- **SoCal Women's Leadership Summit** — designed to inform and inspire members around issues vital to the community



- **WiTH Workshops** — periodic educational and interactive events featuring keynote speakers and round table discussions with industry leaders

\*In-person and online



For more information, visit [withhollywood.org](http://withhollywood.org)

WiTH is a 501(c)3 charitable organization

## **NAGRA** *Continued from page 50*

services and social media, production timelines will come under pressure, particularly at a time of industrial unrest. This can open the door to new original or variant generative AI content and/or content formats as seen in the Netflix example above.

However, existing technologies can help address some of these challenges. Those creating “human-intelligence” generated content use a variety of tools to identify whether AI-generated work has stolen their content — which can include likeness and speech/ tone. Some of these tools and techniques are the same as those used to track conventional content piracy and include watermarking both the video and/or audio so the source can be authenticated evidentially if required. In addition, investigative techniques are also used to identify entities posting or selling illicit AI-generated content.

Whether generative AI will form the next content revolution and change established industry practices and business models remains to be seen. While there is a positive yet cautious tone emerging,

history also tells us that not adopting new technologies such as generative AI for the reasons discussed here, may ultimately have a greater impact. As Paul Cramer from Veritone recently commented: “Gen AI won’t replace humans, but it will replace the humans who are not using AI.”

### **NAVIGATE THE DISRUPTION. SECURE YOUR FUTURE**

NAGRA has been securing content in all its forms for more than 30 years. Our technologies extend across both content distribution and content production. As consumers start to interact and pay for a wider selection of content with their eyeballs (FAST, AdTech, loyalty rewards etc.) rather than their wallets, new security approaches, beyond just content security are required. NAGRA teams are actively working with new GenAI innovations to ensure our solutions remain robust in the face of attack and the benefits of AI and GenAI for our industry are maximized. ■

---

## **ATKINSON** *Continued from page 8*

### **Security automation:**

■ AI and machine learning can automate routine security tasks, allowing security professionals to focus on more complex threats.

### **Vulnerability assessment:**

■ AI can identify vulnerabilities in software and infrastructure, helping organizations patch weaknesses before they are exploited.

### **Phishing detection:**

■ AI-driven email security tools can identify phishing emails and other forms of social engineering attacks.

### **Security analytics:**

■ AI can process and analyze large datasets to provide security professionals with insights into potential risks and trends.

### **Threat intelligence:**

■ AI can help organizations gather, process, and analyze threat intelligence data from various sources to anticipate and prepare for emerging threats.

### **Autonomous security systems:**

■ AI-powered security systems can make real-time decisions and take actions to mitigate threats without human intervention.

### **Privacy concerns:**

■ AI’s capabilities can also be a threat to privacy when used for surveillance, data mining, or profiling. There are ongoing debates about balancing security with privacy concerns. With AI development moving so fast and so broadly, with such potential impact, what should we be doing as AI leaders to just keep up ... much less get ahead of this revolution?

Recognize that you are not alone. In fact, pretty much every one of

us is being eclipsed by this revolution. What this means is that we can leverage each other in learning, sharing, and trying. Be a part of a community that has a culture of sharing (such as CDSA and MESA) and get involved with your experiences and importantly your perceptions.

Don’t fear AI: it is simply a tool. Incredibly powerful and amazing, but still just a tool. So, the more we can keep this perspective, the more we can see it as an enabler and force-multiplier and keep our thinking in context, the easier it will be to keep AI in context.

Try using it, in safe ways. Getting real-world experience with AI-based tools (and seeing what you can do that maybe you could not prior) builds perspectives. For example, try ChatGPT ([openai.com/chatgpt](https://openai.com/chatgpt)) by asking it some questions, and getting its formatted and curated answers in moments. Try things you wonder, but also try things that you know very well. You might see that the AI engine is interpreting the sources it has and might be getting things right...or maybe very wrong.

Understand that these AI engines are interpretive, by design. Different from the types of queries/results that we are used to from computer systems for the past 20 years. This is more like asking another person, and getting a response that could be delivered with confidence and passion but could be fundamentally wrong. But this ability to “interpret” is exactly what also makes them extremely powerful. Adobe’s ability to simply request their AI systems to “create” imagery that did not exist before is a great example where this type of function is fueling a new revolution.

Look on the bright side, cautiously. Yes, AI is being leveraged for fraudulent means. Bad guys have always used whatever tools are available. But AI-enabled tools are changing our lives for the positive too.

AI and security are colliding, in many ways. And while it feels like this has come out of nowhere and is hitting us from all angles (and it is), this is also a revolution of tools that has been in vision and development for many years and will take many years to mature. Don’t panic. Learn to drive, in a context, and let’s all work together as a community to deal with this — and grow — together. ■



tent converge, that's Smart Content!

**Audience Insights.** Understanding the audience is paramount in the M&E space. Data provides comprehensive audience insights, think demographics, behavior, and viewing habits. This information helps companies tailor their content, marketing strategies, and even pricing to better meet the expectations of their viewers. By effectively using audience insights, organizations can adapt their offerings to suit the ever-changing preferences of their viewers, ensuring they remain relevant and in-demand wherever they are in the world.

**Predictive analytics.** Data is a powerful tool for predicting future trends and developments in the industry. By analyzing historical data, you can make informed decisions about investments, market expansion, and technological adoption, ensuring they stay ahead of the competition. Effective use of predictive analytics enables M&E companies to proactively respond to industry changes, giving them a strategic advantage.

**Cost reduction.** Data can lead to significant cost reductions. By understanding the viewership patterns and preferences, companies can avoid overproducing content that won't perform well. This efficiency in content production can translate into substantial savings. Effective data-driven cost reduction measures can improve the financial health of any institution.

**Monetization opportunities.** The value of data extends to monetization opportunities. Leveraging data to identify potential partnerships, licensing deals, and revenue streams. This diversification can help increase profitability, making effective data utilization a crucial component of financial success.

**Content security.** Data is also crucial for content security. With the rise of digital piracy and unauthorized distribution, M&E companies rely on data to monitor and protect their intellectual property. This includes identifying copyright violations and ensuring content remains exclusive. Effective data usage for content security safeguards the financial interests and reputation. Particularly in Hollywood where your reputation means everything.

**Competitive advantage.** In a crowded and competitive industry, data can be a game-changer. Organizations that harness data effectively gain a competitive edge by offering superior content recommendations, targeted advertising, and a better understanding of

their audience. This edge can translate into higher market share and increased profitability. Effectively leveraging data is essential to staying ahead of your competitors and retain market leadership.

### WITH GREAT DATA POWER ...

While realizing the worth of data, M&E companies must also address any potential issues:

**Data privacy.** M&E companies must adhere to data privacy regulations to protect user information and build trust. Ensuring that data collection and utilization are compliant with privacy laws is crucial to maintain the trust of their viewers.

**Data security.** As data becomes more valuable, it becomes a prime target for cyberattacks. Robust data security measures are essential to protect sensitive information and avoid data breaches that could harm both the company and its users.

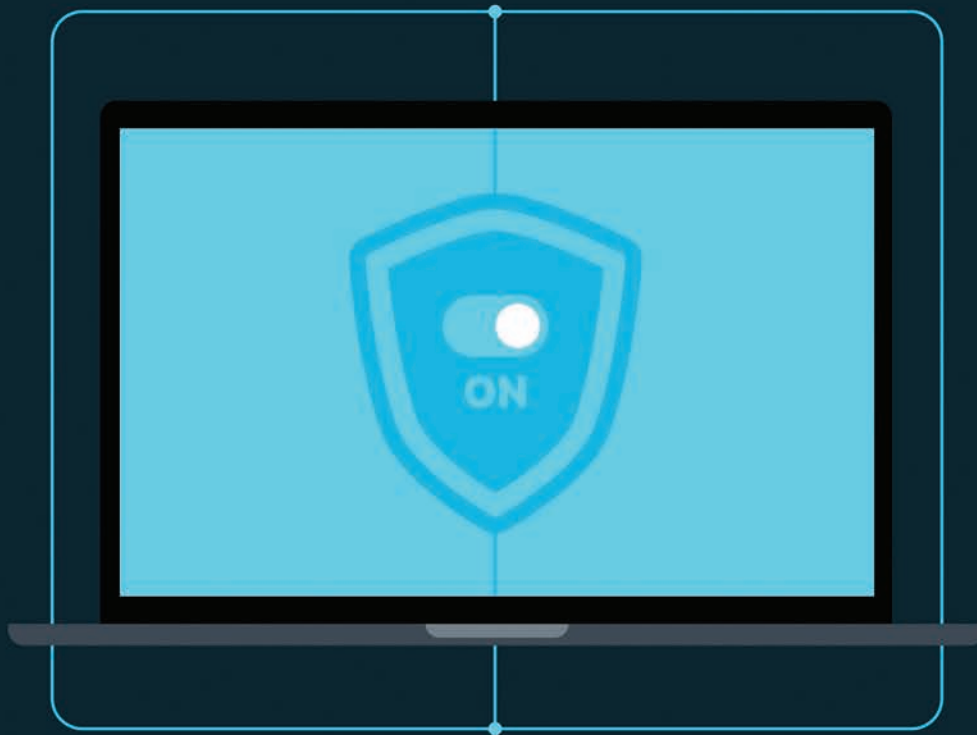
**Ethical use.** Responsible data use is paramount. Organizations must ensure that they use data in an ethical and transparent manner, respecting user consent and maintaining trust. Ethical data practices are vital to safeguard the reputation of big studios and small ones.

**Data quality.** The value of data hinges on its quality. Companies must invest in data collection and management processes to ensure the data they use is accurate, up-to-date, and reliable. High-quality data is essential for effective decision-making.

**Data analytics expertise.** Employing data scientists and analysts who can interpret and derive insights from data is crucial. Expertise in data analytics is the key to making informed decisions and leveraging data effectively.

Data is the backbone of modern M&E companies, and the effective use of data is crucial for success. By leveraging data to provide personalized content, optimize operations, and maintain a competitive edge, organizations can ensure continued growth and profitability. However, with great power comes, you guessed it, great responsibility. M&E companies must handle data with care, respecting privacy, security, ethical considerations, and data quality.

As technology continues to evolve, the worth of data will only grow, making it a valuable asset in an ever-evolving industry. The strategic use of data is not just luxury and excessive splashy bling, but a necessity in the digital age of media and entertainment. ■



## Secure your web apps and APIs, wherever they live

Traditional web application firewalls (WAF) rely on regular expression pattern-matching rules. They're difficult to manage and require never-ending rules tuning to eliminate false positives that can block legitimate traffic. The Fastly Next-Gen WAF leverages a fundamentally different approach, developed by Signal Sciences, that effectively detects and blocks malicious traffic without rules tuning, leaving your AppSec teams to focus on bigger problems. To learn more, [visit \*\*fastly.com/secure\*\*](https://fastly.com/secure)

**~90%**

customers in full  
blocking mode

**90k+**

app deployments  
protected

**100+**

Cloud-native and datacenter  
platforms supported

**5**

Consecutive years as a  
Gartner Peer Insights  
Customer' Choice

## Content Delivery Speed or Security?

# With Fortinet, You Don't Need to Compromise.

Today's consumer expects instant, reliable, high-quality streaming. Hyperscale data centers provide ultrafast content delivery, but when security solutions can't keep up, you're left with a tough decision. Fortinet provides security at speed with the industry's best threat protection performance. Ultra-low latency next-generation firewalls deliver fast and secure entertainment experiences from live sports to family movies. Fortinet's purpose-built security hardware protects network traffic and sensitive data without constraining bandwidth or compromising customer experience. To learn more, visit [www.fortinet.com/m&e](http://www.fortinet.com/m&e)

