

# The Future is Automated

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

## WORKFLOWS AND THE CLOUD

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

## SMART CONTENT

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

## SECURITY SOLUTIONS:

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

# 23,01

# DRIVING DOWN CONTENT FRAUD WITH AUTOMATION

Fighting scale with scalability

**ABSTRACT:** At the current pace of digitalization, the problem of rapid large-scale data processing becomes ever more pressing. In video security and anti-piracy, searching for illicitly redistributed streams across ever increasing number of websites, apps and devices has become a task that is not possible to deal with successfully if a significant level of scalability and automation is not present.

By Nik Forman, Marketing Director, Friend MTS

As the amount of video content that is created, captured, distributed, and watched continues to increase at phenomenal rates, the volume of data that it represents is likewise increasing at a speed never seen before.

Technology industries in general are discovering the opportunities that this data can afford them and how it can help them tackle current and future business challenges. However, these opportunities are accompanied by challenges, one of the biggest of which is how to deal with processing increasing volumes of data. It's clear that without rapid, automated data processing capabilities, we are constantly playing catch-up, struggling not just with day-to-day operations but also strategically.

In the field of content security and fraud prevention, the ability to process huge volumes of data in real-time plays a key role in enabling swift and comprehensive detection and disruption of instances of illegal content redistribution.

Today, content fraud has reached epic proportions; the sheer volume, high quality, and speed of redistribution of pirated content present a real and significant threat to legitimate revenues, so much so that some would even argue it has become an existential threat to legal providers. With one in 10 adults in the U.S. consuming pirated TV, movies, or live sports in 2022 (according to a YouGov survey conducted for Variety) it's clear that demand remains high, and the fight to protect content creators and rights owners from the hugely damaging effects of content fraud continue.



**AUTOMATED PROCESSES  
LARGELY ELIMINATE false  
positives and produce a far  
smaller pool of instances requiring  
additional verification.**

It is impossible to fight these threats to the sports and M&E industry without automated content protection and anti-piracy operations, including piracy detection (or content monitoring) and takedown (also known as legal piracy enforcement). These processes contain several steps, and the requirement for automation is common to them all. Automating metadata-based search processes is an obvious and relatively easy to implement – but to genuinely create the ability to analyze and process the sheer scale of data required for effective anti-fraud operations, all the subsequent steps must also be automated, from video search and capture through to content identification and legal enforcement.

The scale of some content monitoring operations is vast. As part of our daily operations at Friend MTS a vast amount of piracy sources are crawled automatically to detect stolen content, with a typical day producing several million suspect links. Obviously, a search task of this scale is impossible to perform manually, even if you employ thousands of people to look for the content; it is simply not realistic to manage and coordinate.

#### **NO EFFECTIVE DISRUPTION WITHOUT AUTOMATION**

Once suspect videos are detected, they need to be automatically verified with highly accurate yet lightweight fingerprinting content identification technology. Again, we're talking about significant numbers here, a few hundred thousand shortlisted videos per day that need to be verified to avoid erroneous takedowns or other enforcement. This is not a trivial exercise, and again requires significant, automated processes and technology to accomplish any significant result.

One may argue that it is indeed possible to verify even thousands of videos if cheap labor is enlisted but, logistical problems of organizing and managing these huge teams aside, how much could they realistically achieve? How much time is needed to complete the verification process, which, remember, is just one of several steps? Owners or distributors of live content, whose value rapidly diminishes with each second that passes, require extremely rapid detection and enforcement; in the live environment, content protection is only effective during the event, and piracy needs to be taken down well before the final whistle — in as close to real-time as possible.

And with manual resourcing comes the issue of

human error. Automated processes largely eliminate false positives and produce a far smaller pool of instances requiring additional verification. Effective, high-confidence identification is far easier to achieve with automated processes that aren't subject to fatigue or distraction.

Next, we come to legal enforcement. Whilst it's doubtful that even the least-automated monitoring and enforcement service issues DMCA notifications manually, there is much more to enforcement than that. The illegal distribution of high-value, premium content requires more than simple notice-issuing to provide effective disruption — rates of non-compliance to notices is high — and this is where it's important to partner with a service that has the experience and expertise to deploy other remedial measures, such as escalation to and direct communication with platforms and infrastructure providers. Once again, this depth of understanding of the most effective processes enables automation to be applied, greatly increasing the ability to deploy enforcement actions in real-time, at huge scale. And this, after all, is the goal: to find and disrupt as many instances of content fraud as possible, with the highest degree of accuracy, as quickly as possible.

#### **CONCLUSION**

Content fraud is a global issue — it respects no boundaries. Video in general, and in particular premium quality video content that costs huge amounts to create, license and distribute, needs to be protected to safeguard the future of those whose livelihoods depend on it. But with a global audience comes a global amount of data, which must be processed, analyzed, identified, and acted upon, in real-time and with pinpoint accuracy. Operations at this scale are only feasible with highly automated processes, that are built on a deep understanding of how piracy works, and a familiarity with the landscape that can only come from many years of spending time there. Simply put, without automation it's just not possible to detect and disrupt at any scale that can be considered effective. ■



*Nik Forman is the marketing director for Friend MTS, and responsible for the company's marketing and communications functions. He brings more than 20 years of B2B marketing experience, and a wide knowledge of the sports, media and entertainment industries.*  
[nforman@friendmts.com](mailto:nforman@friendmts.com) @friendmts

# Friend MTS

## Protect your content from fraud

Talk to the experts in live and on-demand content security

Watermarking | Monitoring & Enforcement | Business Intelligence

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