M+E JOURNAL

WHAT'S NEXT?

An M&E industry that's learned to adapt and excel after a year like no other, for one

LOCALIZATION
Dubbing from home is a work in progress

SECURITY
How to beat piracy and secure your business during a pandemic

SMART CONTENT
The new ways content players are using data to connect with consumers

NEW WORKFLOWS
Adopting the latest tools fuels a successful change to remote work

20.02

THE END OF CO-LOCATED, PHYSICAL REVIEWS

Watermarking is proving essential to protecting approval and screener workflows, along with live marketing events

By Eric Bénetière, VP Marketing, Sales, ContentArmor

ABSTRACT: Dailies, approval workflows, screeners, marketing campaigns, film festivals and distribution … the COVID-19 era accelerated the transition from collocated physical reviews to digital distribution in the M&E industry. Pirates are on the look-out to exploit any vulnerability in these new digital workflows. This article will review some of these new use cases and the actions taken to mitigate the risks inherent to sharing the most premium content.

There is no doubt that the COVID-19 crisis has deeply changed our attitude to work. WFH is now the new standard in many geographies that have strict lockdown rules. Additionally, several surveys have been recently published showing that we will probably not be going back entirely to our old working styles or habits. And for once, both employers and employees seem to be on the same page: 67 percent of company decision makers expect WFH policies implemented for the pandemic to remain in place long term or permanently, according to an S&P global coronavirus survey.

In our M&E industry, companies have been forced to cope with this new situation and have moved a number of on premises and physical workflows to distributed and cloud-based infrastructure. These workflows include content sharing applications such as dailies, localization and commercial screeners. However, it has also accelerated the emergence and deployment of new applications such as virtual marketing events and virtual film festivals. Obviously, all these new applications are driven by the inability to set up a physical event in a theater, a mall, or any corporate location. Gathering several colleagues for internal daily reviews or tens of end-users for a test screener is not a given anymore. Therefore, numerous companies have turned to digital platforms in lieu of co-located physical reviews. It can be for instance a live set up for some virtual film festival, a marketing launch with sensitive content available only in real time or a VOD like experience where viewers are given a number of hours/days to watch the content.

A NEW SET OF THREATS FOR VIRTUAL REVIEWS

Leaks of unreleased premium content have already been the nightmare of content security owners for a long time. However, this acceleration of virtual reviews from dailies to screeners for the full production pipeline as well as the appearance of virtual film festivals and early window VOD, is increasing the attack surface and inducing a new set of threats.

The first area of risks is obviously cybersecurity as the hackers have not taken any break during the pandemic. The FBI's Internet Crime Complaint Center received 3,000-4,000 calls each day in June, compared to a 1,000 per day before the pandemic.

A second set of risks is related to identity management and credentials sharing that has flourished over the last months/years in the B2C SVOD services, but can be applied in the same ways for some post production workflows and virtual festivals.

A third domain relates to the lack of social control and enforcement when you move from public to private locations. In most geographic regions today, it's hard to imagine someone setting up a high quality 4K camcorder on a tripod in a theater or a corporate office. However, nothing prevents a malicious user doing this at home on a large 4K TV set where they are in control of the environment with respect to lighting and sound to achieve a very high quality copy of a feature film. In the same way, trying to circumvent content security measures around device management and DRM licensing authorizations to enable screen grabbing is also much easier on private devices than running the same exercise on corporate PCs.

We will focus for the rest of this paper on the latest threat that raises new security challenges.

LEAKS OF UNRELEASED premium content have already been the nightmare of content security owners for a long time. However, this acceleration of virtual reviews from dailies to screeners for the full production pipeline as well as the appearance of virtual film festivals and early window VOD, is increasing the attack surface and inducing a new set of threats.

HOW TO MITIGATE THESE NEW RISKS

At ContentArmor, we believe that the precedent has been set for this type of pre-release content consumption. As these events are showcasing exclusive content which is viewed in less controlled environments our industry needs to come together to mitigate the risks associated with professional piracy or casual re-streaming.

To secure these applications against these new risks, we are happy to share a few best practices or attention points.

- **Rigorous** Account and ID management. There are obviously a number of tools available in the corporate world, but the notion of online and real-time ID checking is progressing even in the consumer world. Instagram attempts to reduce fake news with ID, the introduction of this verification since August 2020 is one good example from another industry and the initiative will favor mainstream customer acceptance for ID checking.

- **Controlling** the number of simultaneous sessions for a given account utilizing DRM and/or your video delivery solutions.

Eric leads product marketing and sales activities for ContentArmor a leading forensic watermarking vendor. Prior to ContentArmor, he spent 20 years in the video delivery industry, starting as software engineer with Philips and then evolved towards customer facing positions with NXP Software and Technicolor. *eric.benetiere@contentarmor.net @contentarmor*

- **Implement** network based visual burn-ins into the video to insert personal data such as an account number to advise your users that they can be traced as the source of a leak. This approach is effective as a deterrent to the "casual" sharers, but it may not be adopted in a given context.
- **As video burn-ins** (even dynamic) remains relatively easy to remove for seasoned hackers, apply forensic watermarking to add the ability to pinpoint the source of any potential leak being a camcorder or a screengrab.
- **Choosing** the right forensic watermarking solution. Being able to forensically watermark a live piece of content from a Hollywood marketing event, which includes an as yet unreleased blockbuster trailer is of prime importance in our industry. Up to now, Hollywood studios requirements for watermarking have been only applied to offline workflows such as screeners or VOD.

Therefore, when choosing a watermarking solution to protect live events, one should look at its ability to manage live feeds while maintaining Hollywood requirements:

- **"Golden-eye"** approval for super high picture quality
- **Robustness** to advanced content transformation introduced by the pirates video acquisition and publishing process (camcorder, video compression, etc.), including on short extracts.

One should also evaluate the ingest time of new assets for offline workflow and/or the latency introduced for live events, as the time to distribution is often a key criteria for those workflows. Many of the existing Hollywood-approved watermarking solutions have more relaxed configurations for some or all of the above requirements to be able to cope with live events.

While this performance-security balance might be acceptable for sports right owners, we at ContentArmor have always thought that live content is as valuable as offline content and have adapted our technology to work in both cases with the same level of fidelity and robustness, which happened to be somewhat visionary in a COVID era.

LOOKING FORWARD

At ContentArmor, we have observed a 65 percent increase in the monthly usage of our watermarking solutions in the pre-release market compared to pre-COVID numbers. This growth is observed on well-established watermarking applications such as approval and screener workflows but also in new use cases such as live marketing events with sensitive content or virtual festivals. As we have no doubts that virtual review usage will keep growing in our M&E industry, there is definitely a need to develop the rights tools required to mitigate the new threats coming along. ⊞

CONTENT**ARMOR**

FROM DAILIES TO SCREENERS

PROTECT YOUR PREMIUM CONTENT WITH FORENSIC WATERMARKING

Learn more at **contentarmor.net/pre-release**

autrement.bzh 02 99 78 09 09 - Credit Photo : ©iStock.com

WE PROTECT YOUR CONTENT | YOU MAXIMIZE YOUR REVENUES

contact@contentarmor.net