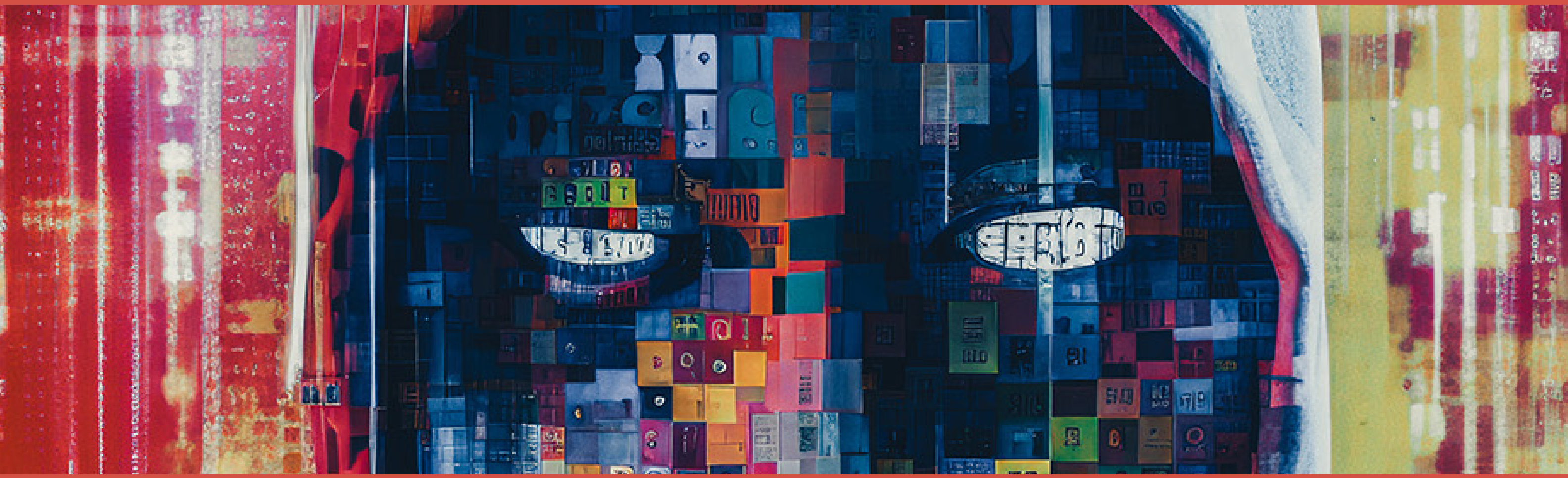
M+E JOURNAL

A SECURE



AI WORLD?

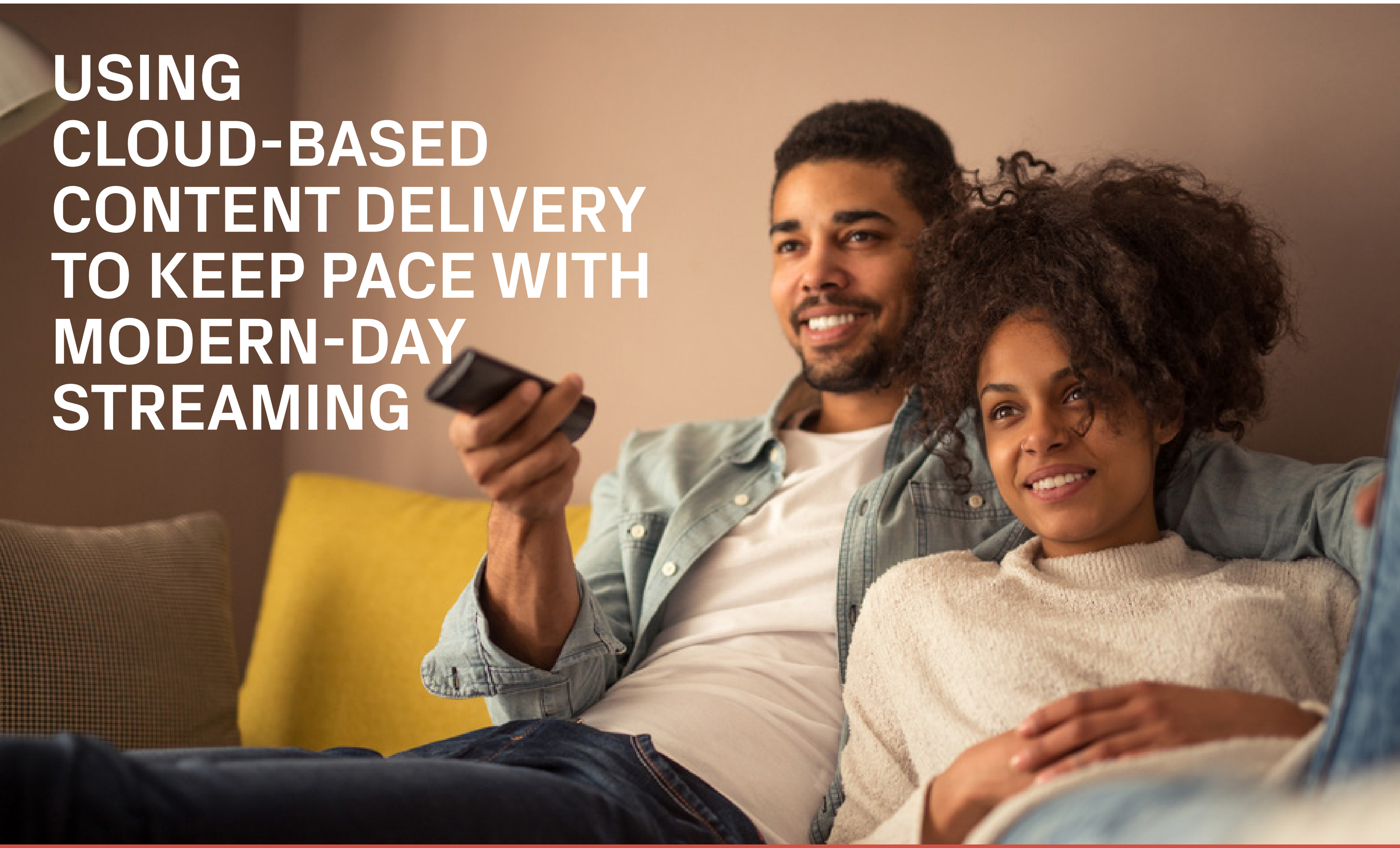
How AI is being used both by and against the industry

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

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

> *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 4

***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 @vubiquity*

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. ⊞