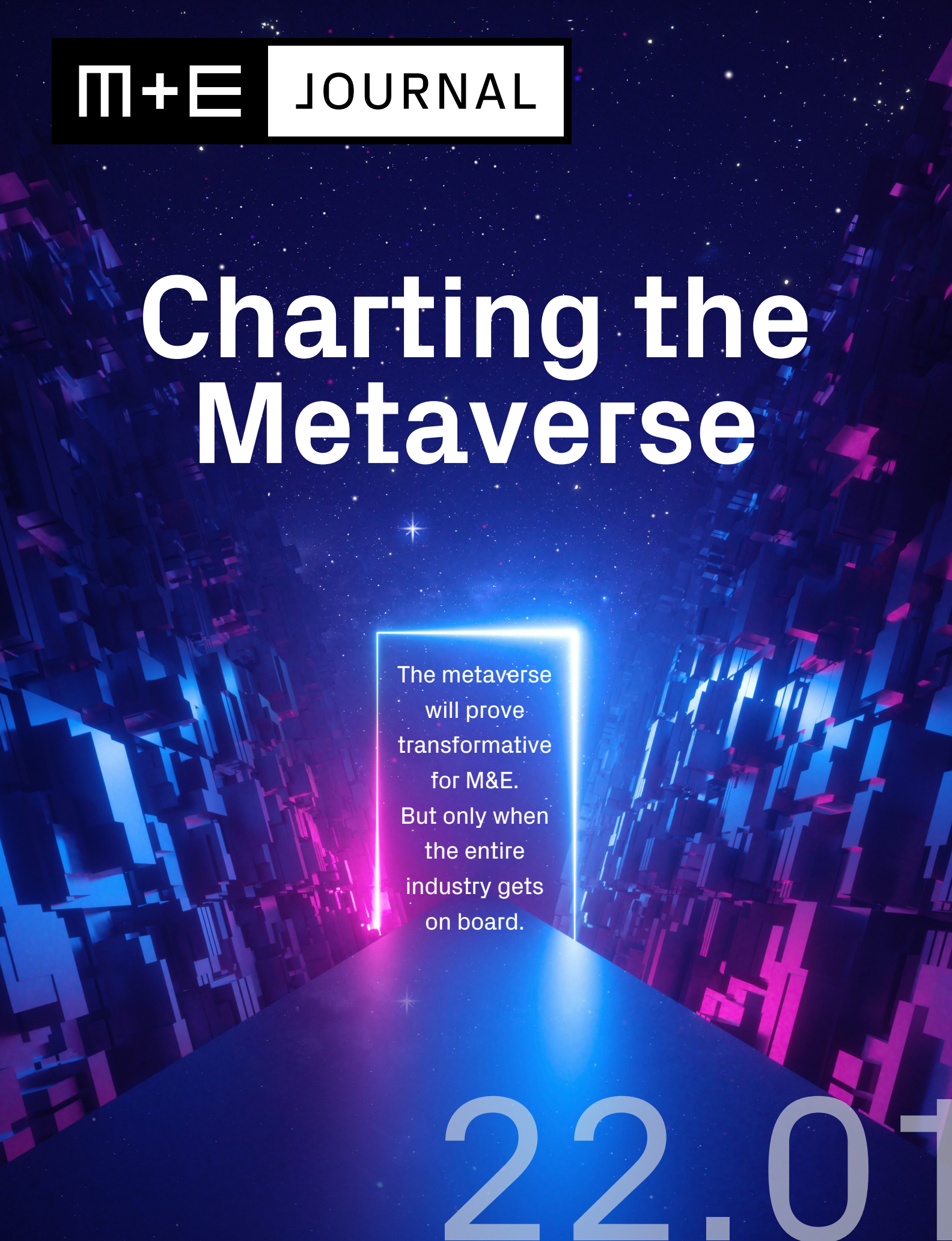
M+E JOURNAL
Charting the Metaverse
The metaverse will prove transformative for M&E. But only when the entire industry gets on board.
22.01

IS SECURITY ANY DIFFERENT FOR THE METAVERSE?

Whatever form it takes for M&E, bad actors will be there

ABSTRACT: The metaverse is underpinned by blockchain, cryptocurrencies and NFTs. And where there is money to be made there will also be bad actors, with fake identities, false promises, and scams. If media and entertainment is going to play in the metaverse, it needs to be prepared.

By Mathew Gilliat-Smith, EVP, Convergent Risks

MESA Platinum Member

A metaverse opinion poll from Ipsos stated: "Thirty-eight percent of Americans report familiarity with the metaverse, but less than one in five (16 percent) can correctly define the term." In general discussions with colleagues, there are wide-ranging views from "It's the next big thing" to "I just don't get it."

In 2000 did you believe you would watch movies on your mobile phone? Did you predict that Google Glass and second screen would fail? Probably not. No one knows for sure but when Disney,

Facebook and others invest large sums into Web3 technology, it's probably time to sit up and take note. The metaverse brings about a new dimension, creating the most immersive consumer experience to date.

What does it mean for M&E? Disney has made a big investment in a business that allows customers to create digital avatars and virtual fashion lines. Other studios will likely follow this lead. For many, it means live-action and postproduction can become a combined process. An entire screen can be visualized using backdrops rendered in real-time enabling producers to create productions with live-action and 3D characters all in-camera reducing the need for VFX - saving money and the environment from travelling to different locations across the globe. At this year's HPA Tech Retreat there was a notable mutual appreciation between the game and film sectors as there are major benefits of working more closely together.

The metaverse is underpinned by blockchain, cryptocurrencies and NFTs. In the game Minecraft, you live a character's life in a metaverse, experience adventures, do jobs and make money (or at least feel like you do). Hyperverse and Sandbox are two of many popular sites based on blockchain where you buy experiences using cryptocurrencies. The metaverse will be about making money. Paying for valuable experiences, like watching a movie, is not a new concept.

WHERE THERE IS MONEY TO BE MADE THERE WILL ALSO BE BAD ACTORS.

Fake identities, false promises and scams will be present in the metaverse just as they are everywhere else. Imagine a metaverse where the character you are communicating with is not actually what or who you think they are. Borrowed brands, characters and voices are easy to create as seen with Fake News. The risk of parting with money because you were fooled into a transaction rings major alarm bells.

THE METAVERSE BRINGS about a new dimension, creating the most immersive consumer experience to date.

When it comes to security the same principles of security apply. Protecting personal data, including your voice, is often overlooked and breaches GDPR as was discussed on Convergent's panel at CDSA's recent Content Protection Summit. There are many moving parts in video production, especially with multiple cloud accounts, third party applications, and different sets of vendors working on the same productions.

Ensuring the correct configuration for your workflow is challenging. To be secure by design is the best approach when creating a new cloud environment. If you're already past that stage, then following security best practices is the next best thing as it is derived from those who have learnt the hard way. When conducting cloud security assessments, the Convergent team find common themes including the absence of centralized identity management, and a lack of vulnerability scanning tools.

Other problems extend to missing anti-malware on virtual machines; logging being disabled from cloud services; and non-existent staff security training. However, the biggest issue is the lack of threat assessment testing. Making sure you are the only one who has control of access to your system is crucial. ⊞

Mathew Gilliat-Smith *is the EVP of Convergent Risks and has 20 years' experience in the media and entertainment sector, with strong relationships at many levels with studios, broadcasters, and vendors. He co-founded three digital security start-ups and has held senior roles in major media corporations.* *mathew.gilliat-smith@convergentrisks.com* *@ConvergentRisks*

Finding the correct security posture for your business can be challenging...

convergent can help.

Cloud & Application Security
Helping you achieve the correct security posture for your cloud and application workflows, through implementation of industry best practices and correct configuration.

Incident Response App
The Sanctum IR app helps you securely manage security incidents, with playbooks, reporting and a secure repository for evidence, removing cumbersome manual processes.

Threat Assessment Testing
Through a targeted attack simulation, safely taking you through real-world penetration testing scenarios to identify vulnerabilities, with advice and guidance on remediation.

TPN Site Security Assessments
As the leading provider of TPN security assessments, we guide you through the partner program working closely with your teams on governance, risk & compliance.

www.linkedin.com/company/convergentrisks/
#convergentrisks
ConvergentRisks

Contact Us
For more information or general enquiries:
e: info@convergentrisks.com
w: www.convergentrisks.com
US Office: +1 (818) 452 9544
UK Office: +44 (0) 1276 415 725