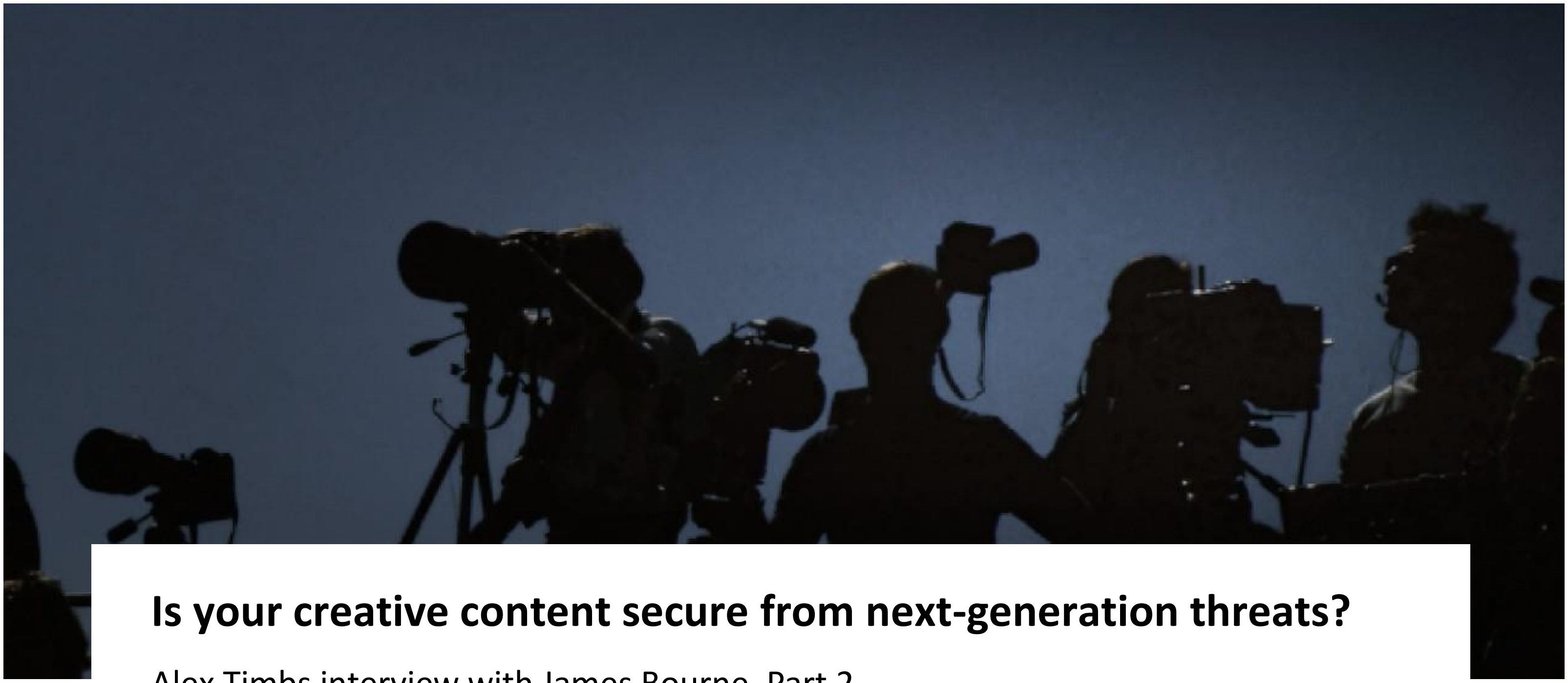

Is your creative content secure from next-generation threats?

Alex Timbs interview with James Bourne, Part 2

April 6, 2023 I Read time 4 min

Last month I spent some quality time with James Bourne, founder of Groundwire Security, to discuss how cybersecurity challenges are evolving in the media and entertainment (M&E) space. If you haven't read part one of my interview with him, I highly recommend doing so. We covered some ground unravelling where he sees challenges for studios in terms of having the right security mindset and infrastructure. We spoke at length on governance, a topic near and dear to his heart as he is a Trusted Partner Network (TPN) and International Organization for Standardization (ISO) accredited assessor.

In Part 1, we touched on the fact that data protection involves more than just creative content. For example, companies must also consider individual information about their employees and customers. In intensely collaborative media and entertainment workflows, it can be a challenge to silo, encrypt or lock down this data. And doing so takes time. I asked James for his advice on better ways companies can protect their data, including personal data and high-value content.

His response was, *"Where do I start with this? The first thing is separating personally identifiable information from the content that's used to make a show, let's say, animatics or elements or scenes and so forth. Segmentation of your networks is the most simplistic form of addressing many of these risks. Start breaking up networks into corporate networks or your corporate SAS solutions, keeping them far away from the production networks. Then, work on a production network layered approach. The key here is authenticating identity - Who is really at the other end? Is it a human, or is it a machine? And how do we genuinely authenticate who that individual is? We can look at numerous mechanisms, from providing the basic credentials, usernames and passwords, to MFA and OTP one-time passwords or even behavioural analytics.*

A Yubikey (USB-C), for example, is an excellent step in authenticating that the individual is physically in possession of the key, therefore, much more likely to be correctly identified. Starting with systems administrators, companies must begin using physical keys to gain access to specific pieces of critical infrastructure. There isn't enough emphasis placed on establishing and maintaining authentication. I've seen it often at facilities recently, where employees don't know who's accessing their data and/or are being excessively permissive."

The just-in-time approach is always a killer inside M&E. (e.g. "I've got to share this file and get it to this individual right now. Just let's open up those ports") James mentioned that he had seen this in a facility recently where they went from a locked down, TPN compliant, facility to a disaster because they didn't understand the importance of security hygiene. *"They had spent all this money tightening it up, finished their audit, then turned everything off again. They contacted me a few weeks ago, saying they had some content that shouldn't be with another client, but it was. It comes down to discipline and maintaining the course if you're going to put all this time and effort into the stratification of your networks."*

Another essential step is if you are sending and receiving content, ensure it’s packaged in such a way that you know precisely what these files are and where they are. James recalled a VFX facility he worked with last year, *“They would just get a zip file full of content that would end up in some arbitrary shared folder that then gets immediately lost because it’s not being tracked. Now, for broadcasters, when they’re receiving transcode jobs, it’s a completely different kettle of fish. There’s an XML file that contains the metadata. In this packet, only specifically permitted file types are validated before they start going into a transcoding pipeline for live playout. The point here is to know who’s accessing, what you’re receiving, where it’s going, and track it.”*

The bottom line is that companies need good asset management, appropriate use of metadata, and dependency tracking for organization, efficiency and security.

Another problem for media companies is identity and access. Do the right people have the proper access to files? It is common to see a company’s facilities being relatively flat in terms of access. Once a user has proven their credentials, they have access to everything and can take any number of actions, including deleting.

James agreed with this assertion saying, *“I have witnessed companies that had a “free for all approach” but I have also seen well-designed AAD (Azure Active Directory) users and AD groups, where artists only have access to specific portions of the file system, and then within that file system they can only do specific things such as create, and later they can’t delete for example. There are facilities out there that have taken the time to be mindful of that. But the bulk hasn’t. It’s, “here’s a share, go for it”, and really, the data is just this big lump of unstructured data, and you could do anything you want to it, delete it, copy it, and so forth. I recall a time when a studio had a temp folder, and the temp folder was used to complete transfers between suites. Over time, the temp folder became an integral part of the entire business to the point that the data there was now hot, i.e. it was actively being used. They stopped keeping the data on the edge device because they found it was better when it was centralized to collaborate on, but it was centralized in the temp folder. I was blown away by the fact that it had organically evolved in that manner. I said, “Maybe you would think about redesigning this and having something called slash temp jobs” to make it an official work area.”*

Zero trust has become a widely adopted security model where you don’t trust by default at any step. It is the key for studios to be successful in their approach to networks, users and data. But James mentioned that he hadn’t seen zero trust implemented in a facility to date. *“I see elements of it at the edge where they are accessing services through Cloudflare, for example, and using the warp clients that the facility requires to connect to the network. Then, various SaaS and Paas-based services run on the other side, but I haven’t seen a full zero trust approach regarding core facility infrastructure like storage.”*

While you can authenticate your access control, it becomes highly granular, raising many issues and, ultimately, tickets on the helpdesk system. However, the good news is that taking this approach provides visibility to what each individual is able to access at every level. This is a significantly more secure approach to the aforementioned large open flat networks and filesystems that are partially segmented with simple file sharing, with everyone in the same group having no control or idea of what is happening.

Getting your security strategy in place involves many considerations, a well-thought-out strategy, and a roadmap. It’s a journey. But it is a journey worth taking when it saves you from leaked content, threat penetration or devastating reputation and financial costs associated with breaches. This is why Dell security experts put together a comprehensive cybersecurity e-guide which provides the latest insights from industry experts on today’s advanced threat landscape and offers detailed advice on building a resilient cybersecurity strategy.

Look for a final part three blog of my conversation with James Bourne next month!

For more information~~,~~ and the latest content on Dell Media and Entertainment storage solutions, please visit us online.

Click here to learn more bout the author, Alex Timbs