



## Securing your media and entertainment content

Alex Timbs

March, 9, 2023 | Read time 2 min

As a former Head of IT for one of the world's leading animation and VFX studios, I've witnessed, firsthand, the challenges and opportunities that the media and entertainment (M&E) industry faces when it comes to cybersecurity. My passion for technology that accelerates the future of entertainment is what drove me to work for Dell Technologies. Understanding the challenges that are top of mind for the industry, I am always looking to advise media companies on how they can drive performance and simplify workloads securely. I want to share some important insights on M&E threat prevention by demonstrating how Dell enhances security with the exciting new release of [PowerScale OneFS 9.5](#).

It is no surprise that the M&E industry is a prime target for cyber criminals who seek to steal, leak, or ransom valuable content such as movies, TV shows, music and games. According to a [report by Digital Citizens Alliance](#), content theft costs the U.S. economy \$29.2 billion annually in lost revenue. Moreover, content theft can damage the reputation and brand value of content creators and distributors.

To prevent these losses and risks, media and entertainment organizations need to adopt a proactive approach to cybersecurity that covers the entire content lifecycle - from production to post-production to distribution. This requires implementing robust security controls across people, processes and, of course, technology, such as storage, which holds the keys to the data kingdom.

One of the key initiatives to help media and entertainment organizations achieve this goal is the Trusted Partner Network (TPN). The TPN is a global industry-wide film and television content protection initiative that was launched in 2018 by two major trade associations: The Motion Picture Association (MPA) and The Content Delivery & Security Association (CDSA). The TPN helps companies prevent leaks and breaches.

When it comes to choosing the right storage, or any technology solution, security is just one of the many important features and benefits media customers look for. Scalability, performance, and flexibility are other important considerations that directly align with the demands of modern media pipelines. When it comes to these features, Dell PowerScale hits all the marks for [media workloads](#), including alignment with industry and regulatory standards. This allows organizations to meet their content protection obligations and pass audits more efficiently, avoiding hefty fines and maintaining their reputation.

With the new PowerScale OneFS 9.5 release Dell introduced an array of additional new features including these upgrades:

1. Multi-factor authentication, single sign-on support, data encryption in-flight and at rest, TLS 1.2, USGv6R1 IPv6 support, SED Master Key rekey, and a new host-based firewall.

With these features, a large multinational visual effects facility (for example) with thousands of employees worldwide can securely store sensitive data in a central repository and ensure that the data is protected against unauthorized access and data breaches.

2. Data at Rest Encryption (DARE) through self-encrypting drives (SEDs) and a key management system.

An example of this would be a postproduction facility using this feature set so that SEDs automatically encrypt the data without user intervention, and the KMS manages the encryption keys, ensuring only authorized personnel can access them. The KMS provisions the encryption keys to the SEDs, which encrypt the data automatically, and the KMS manages the keys throughout their lifecycle, including key recovery. By implementing this solution, the facility ensures its sensitive data is secure and compliant with its client's content protection policies.

3. Compliance with US Federal and DoD mandates, such as FIPS 140-2, Common Criteria, and DISA.

With this, a defense contractor that specializes in training and simulation content can store sensitive data and comply with strict data privacy and security regulations. The solution protects the data using encryption and other security measures to ensure that it is inaccessible to unauthorized users. Regular compliance auditing helps to identify potential vulnerabilities or gaps in security measures and take corrective actions to mitigate them.

4. SmartQoS, which gives network administrators the power to prioritize applications as determined by the needs of the business thereby making it easier to assign higher importance to particular data sets.

Let's say that a multinational visual effects company with multiple branches worldwide needed to prioritize certain workloads to ensure optimal performance and productivity. To achieve this, they implemented a SmartQoS solution with OneFS9.5 that enables network administrators to limit the maximum number of protocol operations that NFS, S3, SMB, or mixed protocol workloads can consume. SmartQoS supports a granular policy that can be set based on path, protocol, user or group.

5. Additional, optimized performance enhancements that provide up to 55% improvement for some workloads on our all-flash nodes.

So, for example, if a small VFX house has a major push to complete a large amount of work before a looming deadline. As a PowerScale customer, they can put all their workloads, including their render farm, on one cluster. However, they are worried that they may max out the cluster performance and can't afford to expand it for this project. They are always keen to keep their storage up to date for security reasons and have decided to update to OneFS9.5 before things get too crazy. On updating their cluster, they find that they were getting 30% greater performance due to the optimizations in the 9.5 release. This allowed the VFX studio to deliver with a high degree of confidence on time and without hurting their budget.

As threats continue to evolve and regulations require strict adherence, choosing technology wisely with security top of mind will benefit media companies in the long run. Dell Technologies OneFS 9.5 on PowerScale delivers the world's most flexible<sup>1</sup> and secure scale-out NAS solution<sup>2</sup> for organizations to store, manage and collaborate on their data. With advanced data protection, access controls, encryption, compliance, and monitoring and auditing capabilities, the [Emmy® award-winning PowerScale \(Isilon\)](#) storage has been widely adopted across the media industry.

For more information, and the latest content on Dell Media and Entertainment storage solutions, please [visit us online](#). [Click here to learn more about the author, Alex Timbs](#)

[1] Based on Dell analysis, August 2021.

[2] Based on Dell analysis comparing cybersecurity software capabilities offered for Dell PowerScale vs. competitive products, September 2022.