DELL Technologies

Cyber Protection and Recovery

Dell PowerScale Cyber Protection Solution

MEDIA AND ENTERTAINMENT

Consequences of Cyber Attacks for Media and Entertainment

Today Cyber crime is a reality that every organization needs to acknowledge and take measures to prevent, detect, and recover from cyber attacks. World wide governments have passed legislations to mandate cyber protection measures as well as streamline transparent reporting mechanisms. With an estimated rate of a cyber-attack happening every 11 seconds and severe labor shortage (more than 600,000 unfi lled positions) in cyber security, a robust multi-layer cyber defense along the entire IT data-chain and across the attack surfaces is the need of the hour.

Cyber attacks happen every

11 seconds[1]

The severe labor shortage in cyber security estimates for unfilled positions are at more than

600,000[3]

Cyber security in Media and Entertainment

Media and Entertainment (M&E) industry produces media content often with specific opinions and view points. By the nature of it content and message can be controversial. Therefore in many cases the intent of the attackers goes beyond the fi nancial gains and may be to block and damage certain media projects. In fact the Motion Picture Association (MPA) and Content Delivery and Security Association (CDSA) have come with specific frameworks to help the industry build cyber defenses.

Increased risk with distributed production workfl ows

When it comes to M&E, the digital media fi les often become the targets of attackers. With an increasingly multi-cloud and distributed workfl ow, artists, editors and producers are constantly moving and managing large amounts of data between cloud providers and on-prem storage platforms. This exposes the valuable digital intellectual property of a studio or production house to cyber attackers. The average cost of a cyber attack in the Media/Communications industry is estimated to be $9.2M[2].

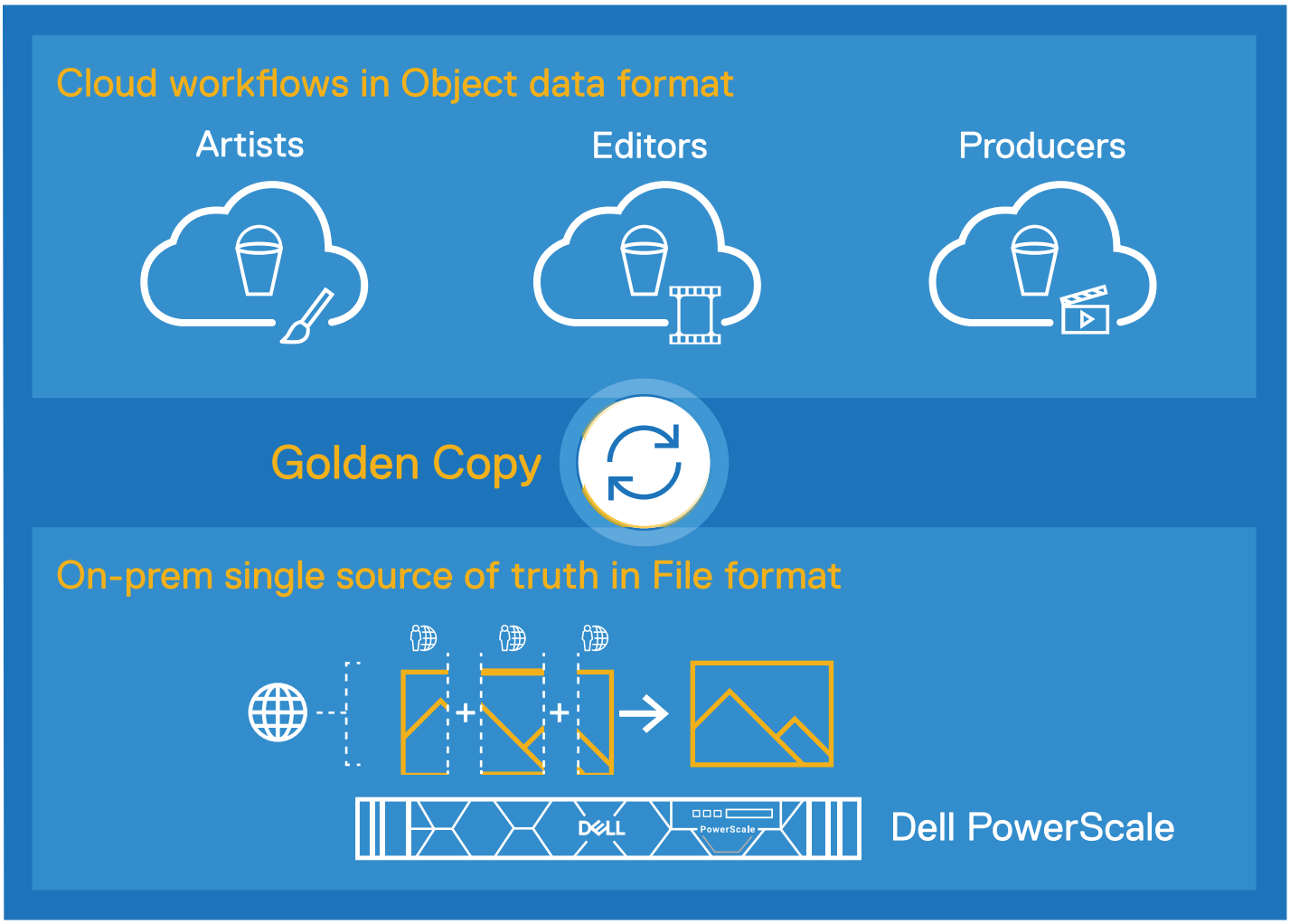
The average cost of a cyber attack in the Media/Communications industry is estimated to be **$9.2 Million**.[2]

References:

[1] https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

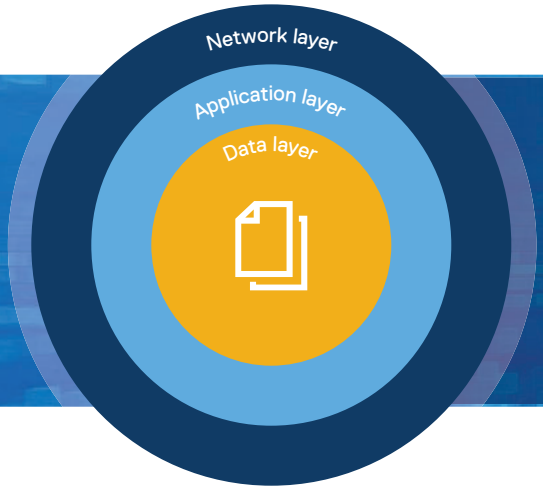
[2] https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf

[3] https://www.bloomberg.com/news/articles/2022-03-30/hackers-path-is-eased-as-600-000-cybersecurity-jobs-sit-empty



Cyber defense at the data layer

Cyber Security tools and frameworks exist across IT ecosystem, but mostly in the network and application layers. We present a cyber protection and recovery solution that is acting at the data layer that boosts the overall cyber resiliency of your media business operations! The PowerScale Cyber Protection solution includes data isolation using intelligent airgap separation of high value media content, AI-powered detection capabilities that puts the IT teams a step ahead of the attackers and rapid recovery mechanisms can recover and restore a peta byte of data in a few hours.



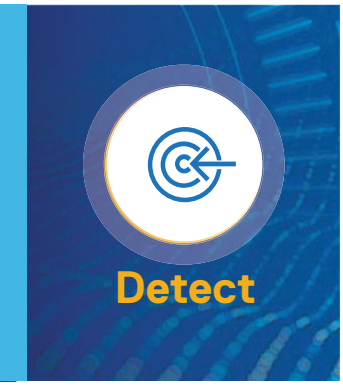
Fortify your data layer

Network isolation of data, AI-powered threat detection at the data layer as well as rapid recovery mechanisms are critical components of a robust cyber resiliency strategy.

Dell PowerScale Cyber Protection Solution

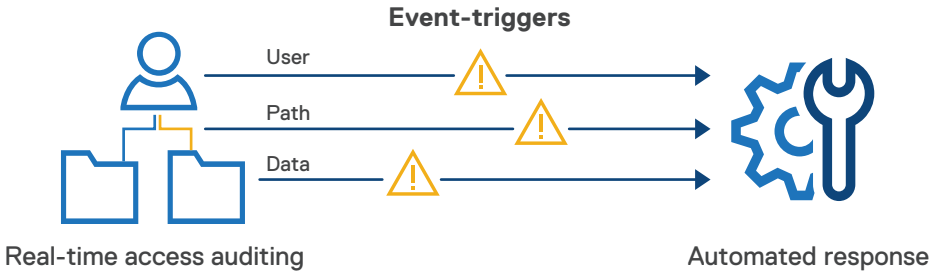
Isolate with smart air-gap technology

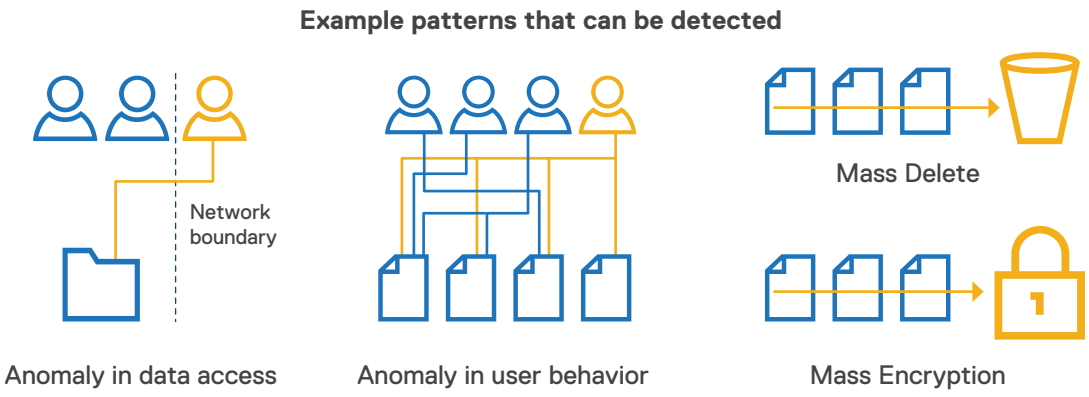
A robust cyber resiliency strategy involves using all the best practices involved in protecting data: right level of access controls, immutable copies of data, anti-virus and anti-malware. In addition to these capabilities, Ransomware Defender offers the protection of last resort, which is a copy of the data in a cyber vault that is isolated from the production environment. After the initial replication of data to the cyber vault, an air-gap is maintained between the production environment and the vault copy. Any further incremental replication is done only intermittently by closing the airgap after ensuring there are no known events that indicate a security breach on the production site.



Detect cyber attacks in real-time

The earlier a team can detect an attack the better they can respond and recover from it. Ransomware Defender comes with the ability to configure event triggers based on patterns of data access that are indicative of a cyber attack. These include detecting for mass deletion of data, mass encryption of data, unauthorized network access or a marked deviation of user behavior from historical data access pattern and so on. These events can be captured with alerts and used for root cause analysis of security breaches. Auto-mated tasks can be setup respond to events indicating a high probability of a cyber attack like terminating replication to cyber vault or denying access to certain users as well as taking additional snapshots of the vault copy of the data can be setup to. Users can also enable learning mode where the systems get more accurate at predicting positives.





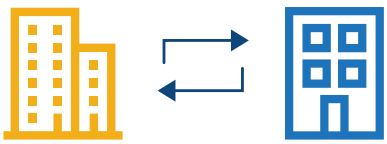
Detect cyber attacks in real-time (continued)

ZeroTrust API extends the ability to respond in the data layer when an attack or compromise is detected elsewhere in the IT Ecosystem: like the application and network layers. The Zero Trust API allows leveraging sensor knowledge at multiple layers combined with an integrated Smart Airgap Cyber vault with Dell Powerscale. The API provides an integration point to connect detection systems at the network and application layers, for example email gateways, Intrusion detection system, Firewalls, SIEM tools, endpoint protection etc. By connecting network detection threat warnings to the intelligent storage layer defenses, the Smart AirGap API can provide a hand off for decisions and responses to the storage layer to take proactive actions to safeguard the data before the impending attack advances.

Operational and Data Recovery

Failover and failback without run books

In case a cyber attack goes undetected and results in a denial of data access or denial of a key service that is essential to run business operations, customers will have the option of failing over to the Cyber vault. Ransomware Defender is integrated with the Eyeglass DR Edition's capabilities that include a continuous monitoring of failover readiness which enables a single-click failover that does not require complicated or outdated run-books.



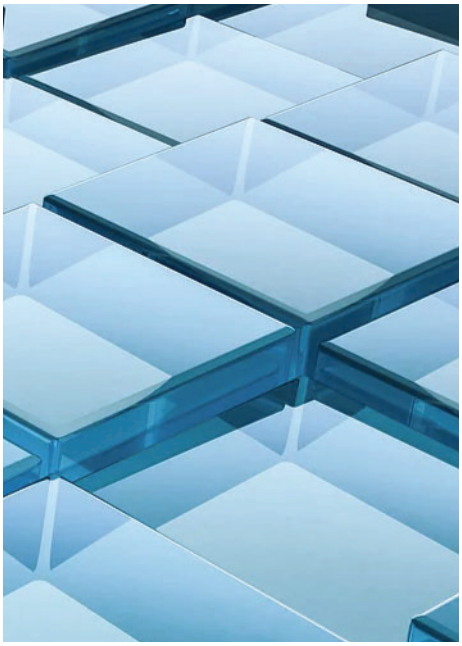
Orchestrated failovers to Cyber vault and failback to production

Data Recovery at blazing speeds

For data recovery you can utilize the immutable snapshots in the cyber vault to granularly restore data to last clean version of it. Not all vault copies are the same. A cyber vault copy on PowerScale enables unmatched RPO of a few hours for a Petabyte of data, something that can take weeks with a typical Object store.

Data Recovery from immutable snapshots in the Cyber vault

Superna Eyeglass Suite



Superna Eyeglass Ransomware Defender is deployed together with the following products that are part of the Superna Eyeglass Suite for a complete threat detection and response system:

- DR Edition
- Easy Auditor

The Airgap solution[1] can be deployed in two configurations depending on the scale of clusters as well as security features:

- **Basic** Airgap Configuration that deploys the Ransomware Defender agent on one of the primary clusters being protected
- **Enterprise** Airgap Configuration that deploys the Ransomware Defender agent on the cyber vault cluster. This solution comes with greater scalability and additional security features.

[1] Airgap solution is available only for PowerScale and not for the ECS platform.

Discover more about PowerScale platform

Learn more about our PowerScale platform

Follow Dell EMC Storage on Twitter

Contact a Dell Technologies Expert for Sales or Support

DELL Technologies