Dell Technologies

Cyber Protection and Recovery

Dell Technologies Solution for Unstructured Data

GOVERNMENT / FEDERAL

Consequences of Cyber Attacks for Federal Government agencies

Cyber attacks at the rate of one happening every 11 seconds have become a serious and continuous threat to organizations of all sizes and verticals. With the sprawling IT footprint, Federal Government agencies are no exception to this threat. The average cost of a cyber attack for US Federal agencies is estimated to be $13.7M in the annual Cyber Security publication by the IT Services major Accenture.

Federal government agencies for a country like the United States have a very large IT footprint across a wide range of public services of national importance. The top areas include:

- **Defense**
- **Health Research**
- **Homeland security**
- **Scientific and Space Research**
- **Critical infrastructure like Energy production and distribution networks**
- **Commerce**
- **Citizen services with high value confidential data**

Cyber attacks happen every

11 seconds[1]

Average cost of a cyber attack for US Federal agencies is estimated to be

$13.7M[2]

Cyber attacks on the above organizations and facilities can have far reaching impact given their importance to the national security, citizen safety, and sources of economic competitiveness and wealth generation.

Federal Mandates for Cybersecurity

Governments across the world have identified Cyber security as a critical theme for national security as well as the freedom and well being of their citizens in the cyber space. Here are a few examples:

- **The Cybersecurity and Infrasutrcture Security Agency (CISA) in the US**
- **The Europian Union Agency for Security - enisa**
- **Japan's National Center of Incident Readiness and Strategy for Cyber Security**

These organizations have laid out comprehensive strategies, processes and best practices to be followed and technologies to be implemented by Federal, State and Local governments when it comes to building cyber resiliency.

References:

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

[2] https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

Unstructured Data in Government Organizations

Deloitte estimates unstructured data accounts for about 80% of all enterprise data. With the ongoing digitization of citizen services, infrastructure management and physical security more and more of this data is becoming is becoming attractive target for cyber attackers to go after. Once the attackers have access to this data, depending on the intent of the attack they may resort to various activities including:

- **Selling the data on the dark net**
- **Control or disrupt critical infrastructure**
- **Denying access to critical data and services to defame organizations**
- **Disrupt operations related to homeland security**
- **Expose national security data openly to destabilize international relations**

Unstructured data accounts for about

80% of all enterprise data[1]

While 100% immunity is not practical, IT Organizations can do a lot to significantly improve the cyber resiliency of the systems to protect business-critical data and setup systems for faster recovery of business operations.

Superna Eyeglass Ransomware Defender for Dell PowerScale and ECS systems boosts the cyber resiliency of unstructured data by providing customers comprehensive capabilities to protect data, detect attack events in real-time and recover from cyber-attacks.

CRIME
Theft and extortion for financial gain

INSIDER
Trusted insiders with malicious intent

ESPIONAGE
Corporate or nation-state actors steal valuable data

HACKTIVISM
Advanced political or social causes

TERRORISM
Sabotage and destruction to instill fear

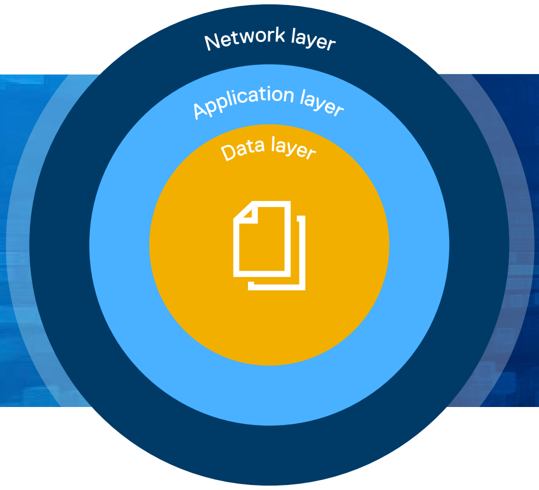
WARFARE
With destructive cyber weapons (NotPetya)

Reference:

[1] https://www2.deloitte.com/us/en/insights/focus/tech-trends/2017/dark-data-analyzing-unstructured-data.html

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.



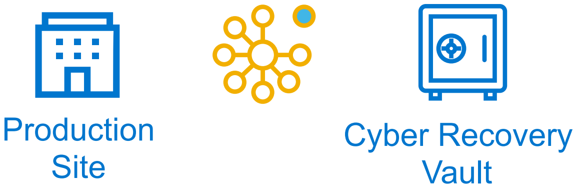
Fortify Your Data Layer

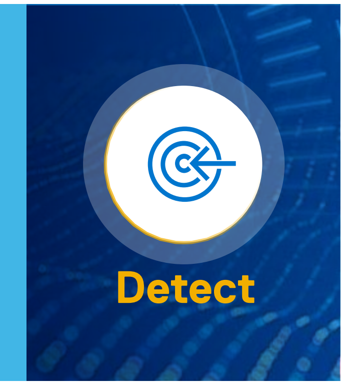
Network isolation of data, AI-powered threat detection at the data layer as well as rapid recovery mechanisms are critical components of a robust cyber resiliency strategy.

Dell Technologies Solution for unstructured data

Isolate with smart air-gap technology

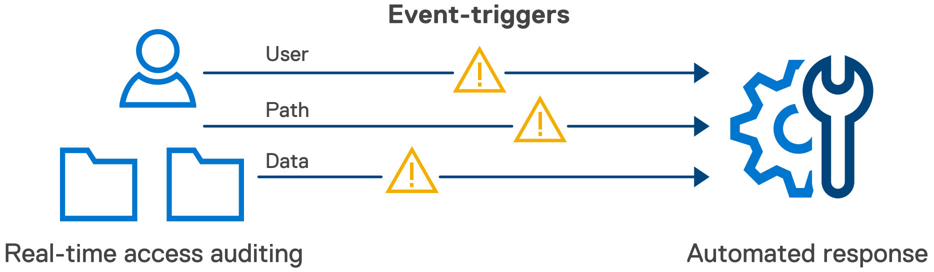
A robust cyber resiliency strategy involves using all the best practices involved in protecting data: right level of access controls, immutable copies of data, anti-virus and anti-malware. In addition to these capabilities, Ransomware Defender offers the protection of last resort, which is a copy of 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.

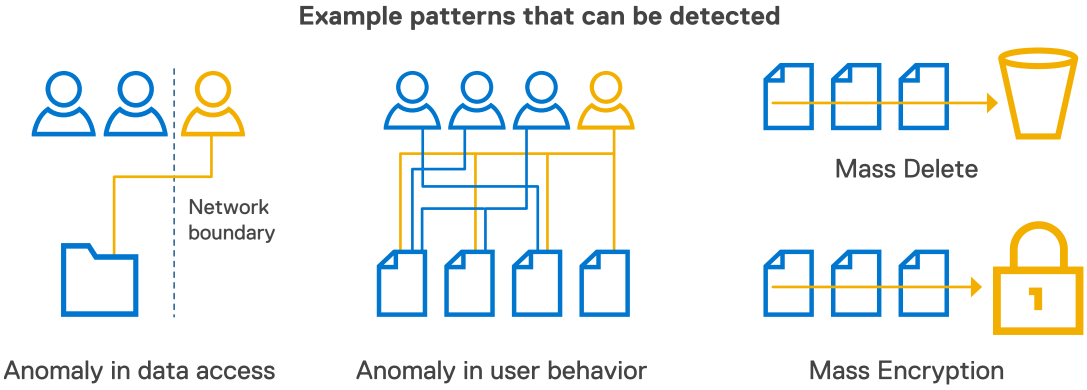




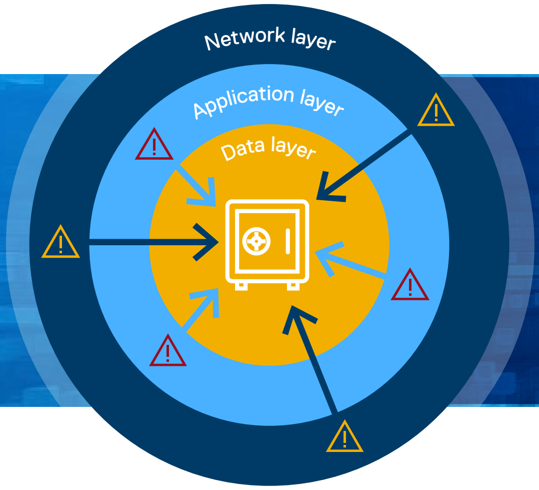
Detect cyber attacks in real-time

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.





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.



Zero Trust API

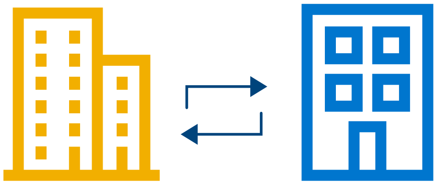
Cascading threat intelligence to the data layer

Recover

Operational and Data Recovery

Failover and failback without run books

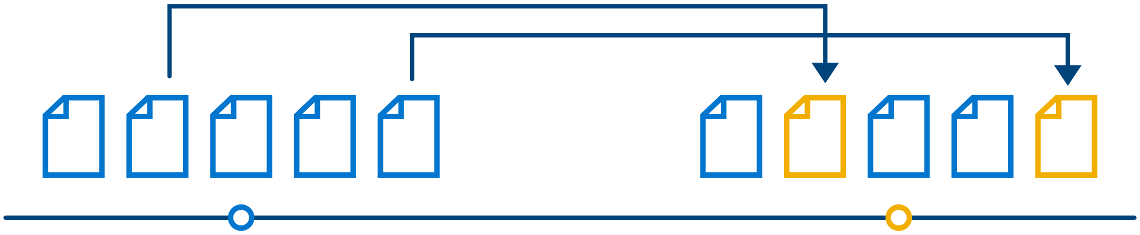
In case a cyber attack goes undetected and results in a denial of data access or denial of a key service that is essential to run business operations, customers will have the option of failing over to the Cyber vault. Ransomware Defender is integrated with the Eyeglass DR Edition's capabilities that 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

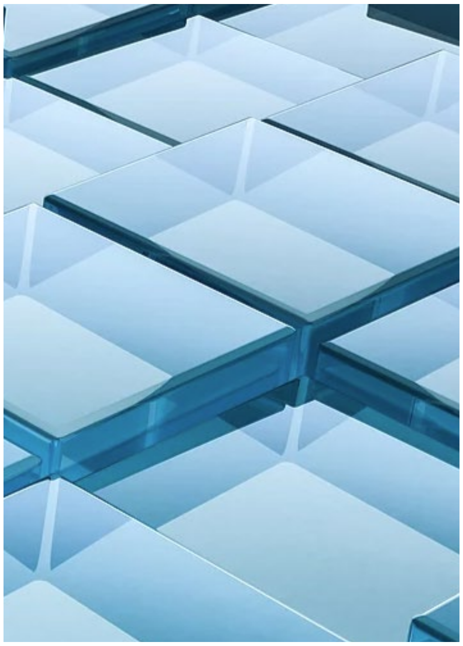
Data Recovery at blazing speeds

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. In case of Dell ECS platform the S3-compliant versioning at the bucket level can be used to restore affected data.



Data Recovery from immutable snapshots in the Cyber vault

Superna Eyeglass Suite



Cyber Protection solutions for Dell PowerScale and ECS platforms are powered in part by 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
- Zero Trust API

The Airgap solution 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.

Discover more about PowerScale platform

Learn more about our PowerScale platform

Learn more about Dell ECS platform

Follow Dell Storage on Twitter

Contact a Dell Technologies Expert for Sales or Support

DELL Technologies