DELL Technologies

Solution Brief

Cyber Protection and Recovery for Dell EMC PowerScale

Cyber attacks have become a serious and continuous threat to businesses of all sizes and verticals. A cyber attack is happening every 11 seconds and the average cost of one is $13M and growing. Cyber attacks disrupt operations, damage reputation and can result in law suits related to data protection regulations. 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 EMC 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.

Protect

Detect

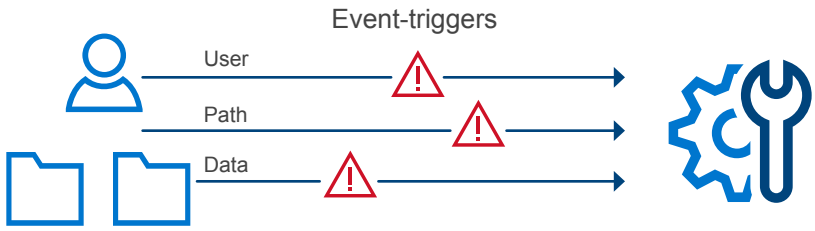
Recover

Protect 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

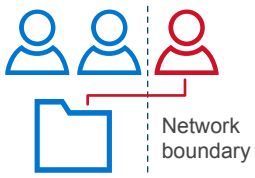
The earlier a team can detect an attack the better they can respond and recover from it. Ransomware Defender comes with the ability to configure event triggers based on patterns of data access that are indicative of a cyber attack. These include detecting for mass deletion of data, mass encryption of 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. Automated 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.



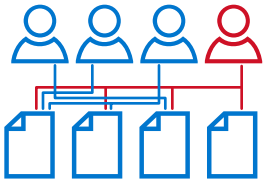
Real-time access auditing

Automated response

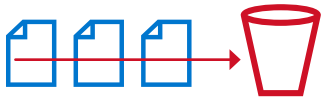
Example patterns that can be detected



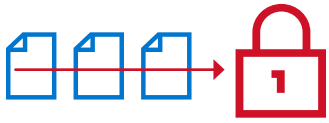
Anomaly in data access



Anomaly in user behavior



Mass Delete

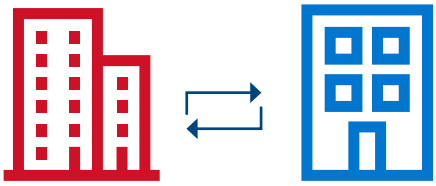


Mass Encryption

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

In order to take the most advantage of Superna Eyeglass Ransomware, the following products that are part of the Superna Eyeglass Suite are required:

- Superna Eyeglass DR Edition
- Superna Eyeglass Easy Auditor

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

Follow Dell EMC Storage on Twitter

Contact a Dell Technologies Expert for Sales or Support

DELL Technologies