superna®

Ransomware Defender

Product Datasheet

Superna © 2018

The Ransomware Defender module monitors individual user behaviors to detect, stop and recover from ransomware attacks for the Isilon/PowerScale or ECS storage platforms.

Superna Eyeglass©

Ransomware Defender

The software detects if a user has been compromised and will take a series of automated actions to stop the infected user by locking out access at the share and export level. Automated Snapshots also protect the file system from multi-user attacks to minimize data loss.

New - Protect object storage on Dell ECS
New - Integrated AirGap Automation

Key Features

1. Ransomware defender detects user behaviours consistent with ransomware access patterns
2. **Fully Automated Learning mode -** Automatically monitors behaviors and customizes detection logic, **avoids false positives**
3. Administrators will be alerted if unusual behavior is detected
4. Configurable to allow a wide range of automated responses from monitor only to immediate user lockout
5. Automated lockout action against shares and NFS exports accessible by infected users stops the attack from compromising data and limits the damage.
6. **Security event data simplifies recovery**
   a. Security Incidents track: compromised AD user account,infected files, previous file access history prior to the attack, user accessible shares on all managed clusters, snapshot names that protect the file system, and client machine IP address to track the origin of the attack (example VPN, office network, data center network)
7. **Monitor List support**
   a. Protects with alerts, snapshots

United States
225 Cedar Hill Street, Suite 200
Marlborough, Massachusetts 01752

superna®

Ransomware Defender

Product Datasheet

Superna © 2018

The Ransomware Defender module monitors individual user behaviors to detect, stop and recover from ransomware attacks for the Isilon/PowerScale or ECS storage platforms.

but no lockout occurs. Configured by path, user or IP

b. Allows customized protection for application servers and avoids the risk of lockout but still protects the data.

8. **Whitelist Support**
   a. Allows the administrator to keep a list of file system paths, user accounts, server IP addresses that are excluded from monitoring example application server service account
9. **Multi-cluster aware monitoring**
   a. If malicious behavior is detected on one cluster, then protective actions are applied to all the clusters on the network that the user has access to (must be Eyeglass licensed clusters)
10. **Integrated SyncIQ with AirGAP 2.0**
    a. 3rd offline copy with Automated Airgap management, vault Isilon cluster proxy alarm monitoring and **Smart AirGap** copy manages SyncIQ sync jobs when no suspicious activity on the source data.
11. **Security Guard** - An automated penetration test ensures defenses are operational
    a. Penetration test logs allow administrators to easily see the health of security defenses and alerts failed penetration tests
    b. Multi cluster automated and scheduled test
12. **Object Data Protection**
    a. Dell ECS is monitored in real-time for suspicious activity and if enabled the authenticated user is disabled , protecting object data.
    b. Real time alerts
    c. **Smart Airgap enabled** ensures threats to Object data blocks Airgap replication.
    d. Alerts include the user and IP address of the attacking host
    e. Fully multi ECS node aware solution

United States
225 Cedar Hill Street, Suite 200
Marlborough, Massachusetts 01752

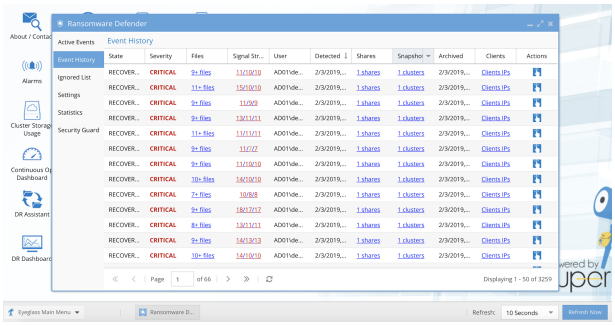
superna®

Ransomware Defender

Product Datasheet

The Ransomware Defender module monitors individual user behaviors to detect, stop and recover from ransomware attacks for the Isilon/PowerScale or ECS storage platforms.

f. Full REST API integration with Dell ECS
g. [Watch the video demo]



Visit the product page at
https://www.supernaeyeglass.com/ransomware-defender
Contact us at sales@superna.net

United States
225 Cedar Hill Street, Suite 200
Marlborough, Massachusetts 01752