Ransomware Defender for Object

Product Datasheet

The Ransomware Defender module monitors individual user behaviors to detect, stop and recover from ransomware attacks for the Dell ECS storage platform.

Superna Eyeglass©

Ransomware Defender

The only Zero Trust S3 native real time data protection solution. 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. Object tracking provides a list of affected objects for recovery.

Key Features

1. Ransomware defender detects user behaviours consistent with ransomware access patterns
2. Name Space, Bucket and object aware solution with auto discovery of ECS
3. **Use cases**
   a. Protect GeoDrive data
   b. Backup server protection
   c. PACS Archive server protection
   d. Any S3 Application IO transparent data independent data protection
4. **Fully Automated Learning mode -** Automatically monitors behaviors and customizes detection logic, **avoids false positives**
5. Administrators will be alerted if unusual behavior is detected
6. Configurable to allow a wide range of automated responses from monitor only to immediate user lockout
7. Automated lockout action against user S3 keys stops the attack from compromising data and limits the damage.
8. **Security event data simplifies recovery**
   a. Security Incidents track: compromised user account,infected files, previous

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

file access history prior to the attack, and client machine IP address to track the origin of the attack.

9. **Monitor List support**
    a. Protects with alerts, snapshots 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.
10. **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
11. **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)
12. **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
13. Eyeglass Ransomware Defender for ECS Overview

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