superna®

Cyber Scanner

Product Datasheet

Superna © 2018

The Cyber Scanner module monitors new or modified files and inspects the data for data integrity, corruption or encryption

Superna Eyeglass©

Cyber Scanner

Next Generation data security solution for large file systems such as Dell EMC Powerscale. Data integrity for billions of files requires a tightly integrated solution that can scan files with content aware security. This solution integrates with the market leading Ransomware Defender solution to extend the detection capabilities to include full content aware scanning that can detect corruption, non-readable text, fully or partially encrypted files with file type aware metadata analysis.

Alerts administrators immediately upon detection of data integrity issues, providing the best solution to protect data from a wide range of threats to corporate data. Allows targeting by file type, a file system path or the entire cluster.

The solution is an add-on product to Ransomware Defender with the ability to scan new or modified data in near real time to provide deeper detection capabilities to expand threat detection beyond only Ransomware attacks.

The content aware detectors are integrated with Ransomware Defenders' learning mode to fully automate configuration and tuning of the system.

Any threats to data that are detected will raise an alarm in Ransomware Defender content security UI, listing the files and the threat detected against the files.

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

superna®

Cyber Scanner

Product Datasheet

Superna © 2018

The Cyber Scanner module monitors new or modified files and inspects the data for data integrity, corruption or encryption

Key Features

1. Full content analysis for data corruption, encryption or malicious modifications
2. File Entropy calculation on all data is compared to a baseline using Ransomware Defenders learning mode. File are detected.
   a. Measures the randomness of the data in a file to detect partial encryption even at the block level.
3. Metadata analysis
4. Partial encryption detection
5. File type mismatch detection
6. Role based Access Controls
7. Full scanning of file system paths
8. Incremental always scanning for created or modified files for continuous cyber scanning of production data
9. File type targeting by extension
10. File type or path based included or exclude option to target which data should be scanned
11. Image file metadata analysis
12. Ransomware Defender Enterprise Airgap 2.0 integration blocks airgap data synchronization if any cyber content threats detected
13. Smart Airgap API support for integration with 3rd party SIEM tools

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

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