DATASHEET

superna®

Superna® Ransomware Defender™ Smart AirGap

Smart AirGap add-on modules offer the most secure data protection available for maintaining offline data copies to comply with the NIST Cybersecurity Framework.

OVERVIEW

Superna® Ransomware Defender™ is a highly scalable, real-time event processing solution that employs user behavior analytics to detect and halt a ransomware attack on data stored on Dell EMC Isilon and PowerScale storage arrays. By monitoring user access to file systems, Ransomware Defender detects changes to normal data access patterns. When administrator-defined thresholds are met, Ransomware Defender can take defensive action to prevent major damage and minimize the recovery time. Ransomware Defender is designed to detect, stop and recover from ransomware attacks and other cyberthreats on Dell Isilon, PowerScale, and ECS storage platforms.

SMART AIRGAP ADDS A FULLY-AUTOMATED CYBERVAULT

Supera's Smart AirGap add-on for Ransomware Defender provides a a fully-automated cyber vault for a last line of defense for your critical data. By creating an "air gap" between the storage system and the external network, a hacker who has gained access to the network will be unable to access the data stored in the system without going through additional layers of security.

Superna's Smart AirGap adds security features to create a virtual break between the storage system and the network, to combat cyberthreats.

Smart AirGap add-on accomplishes this by creating a virtual air gap between the object storage system and the external network. This virtual air gap is achieved by creating a secure communication channel between the object storage system and a designated security appliance, which acts as a proxy for external communications.

HIGHLIGHTS

- Superna® AirGap 2.0 is an add-on to Superna Defender™ that offers enhanced protection of data stored on Dell PowerScale hardware
- Protects critical configuration data in a PowerScale vault
- Inside- or Outside-The-Vault automation
- Double-door vault protection
- The only rapid recovery solution (< 2 hour) for petabyte-scale data.
- Fully-automated cyber vault, with daily synced data reporting, and in-band vault cluster monitoring
- Based on best practices established by the National Institute of Standards and Technology (NIST)

AVAILABLE IN 2 CONFIGURATIONS

Smart AirGap is available in 2 configurations – **AirGap Basic** and **AirGap Enterprise** – providing two levels of protection for your storage appliances, in compliance with best practices suggested by the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

By integrating Smart AirGap's cybervault capabilities, you're able to automatically suspend data copy operations whenever source data is under threat. Superna's Smart AirGap offers the industry's fastest rapid recovery mode, eliminating the days (and even weeks) required by typical backup solutions to restore data from vault devices. Superna's rapid recovery enables offline data to be accessible in as little as 2 hours (or less), regardless of the size of the protected dataset. Rapid recovery also restores SMB and NFS share definitions.

KEY FEATURES

Available with Inside- or Outside-the-Vault automation. The Inside-the-Vault hardened solution offers double door vault protection. Two network doors must be open at the same in order for data to replicate. Superna offers the *only* double door cybervault solution. Outside-the-Vault protection enables a lower-cost secure solution with end-to-end automation and a single door vault solution.

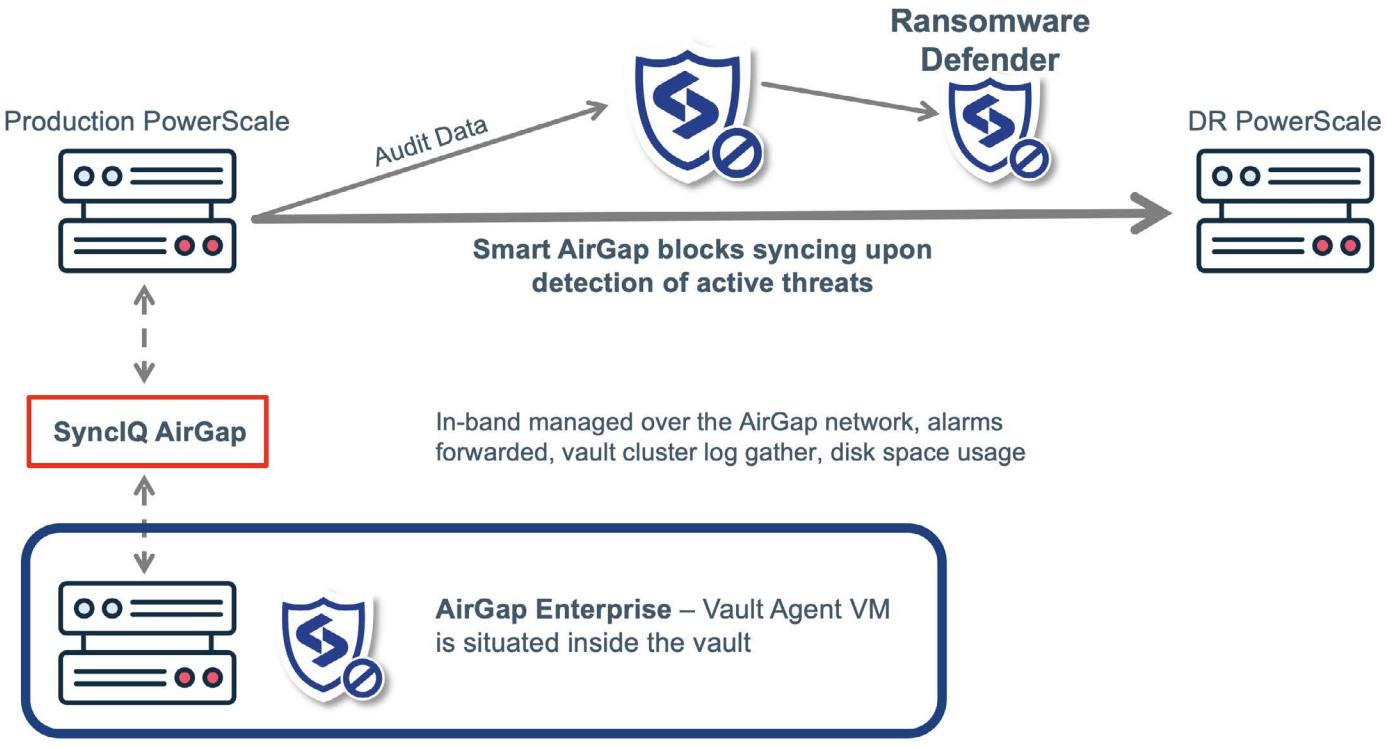
Rapid Recovery. Superna offers the only < 2-hour rapid recovery solution for petabyte-scale data.

Robust Protection. Superna protects Powerscale critical configuration data in the vault (Shares, NFS exports, quotas)

Flexible. Many to one support for protection of multiple source clusters to a single vault cluster.

Cost-Effective. Dell Powerscale offers the lowest-cost cyber vault-protected offline copy of data. It provides for space-efficient block differential snapshots; block level replication; and immutable snapshots with automated data retention management.

Combines user-based behavior detection with added security features to create a virtual gap between the storage system and the network.



Flexible Data Protection. Select your data protection by path, with custom replication policies managed by Superna Ransomware Defender. Protect all or just a subset of your production data.

AirGap Anywhere. The source of the AirGap copy can be production or the DR cluster copy of data. Allows maximum flexibility for deploying your cyber vault.

Flexibile Network Options. Utilizes layer 3 or layer 2 between production and vault cluster for network flexibility.

Simplified Network Management. Ransomware Defender manages the network between the production cluster and the vault cluster.

Smart AirGap. The only solution in the market that uses real-time, zero-trust user behavior monitoring to restrict updates to a vault copy if the source data is under threat. Smart AirGap custom policies allow Easy Auditor integration to enable real time policies for determining criteria for opening or closing the cyber vault. And role-based access control simplifies management of your AirGap.

Robust Reporting. Fully-automated daily reporting covering synced data and in-band vault cluster hardware monitoring.

Golden Copy Integration. Superna Golden Copy integration for File-to-Object-aware secure copying to offsite AWS S3 cloud storage. Allows Golden Copy to pause backups in the event that source data is under attack.

ENABLES COMPLIANCE WITH NIST CYBERSECURITY FRAMEWORK

Created through collaboration between industry and government, the framework consists of standards, guidelines, and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable, and cost-effective approach of the framework helps owners and operators of critical infrastructure to better manage their cybersecurity-related risk.

Attribute	How Ransomware Defender Enables Compliance	Compliance
Identify	Threat identified by User Name and IP Address	✓
Protect	Stops the threat in real time with user lockout	✓
Detect	User behavior based, tripwire, and well-known extension detection	✓
Respond	Alerting email, syslog, and auto-matic snapshot creation	✓
Recover	File-level tracking and snapshot data recovery	✓

For more insight into how Superna® can help solve your organization's unstructured data security challenges, visit us at superna.io.

superna
Securing unstructured data, wherever it resides

superna.io
letschat@superna.io

20230715