DATASHEET

superna®

Superna® Ransomware Defender™ AirGap for Object with Dell ECS

The Ransomware Defender Enterprise module offers the most secure data protection available for maintaining offline data copies that 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 CYBER VAULT

This add-on solution to Superna's Ransomware Defender for ECS provides 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 AirGap for Object adds security features to create a virtual break between the storage system and the network, to combat cyberthreats.

Superna's AirGap for Object accomplishes this by creating a virtual air gap between the object storage system and the external network. This virtual air gap creates 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 is an add-on to Superna Defender™ that offers enhanced protection of data with a fully-automated cyber vault
- AWS S3 to S3 Air Gap support
- CAS (Cloud Access Connector) to CAS Air Gap support
- Inside-the-Vault automation
- 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)

KEY FEATURES

AWS S3 to S3 Air Gap Support. Defender AirGap for Object supports air gapping between S3 buckets.

CAS to CAS Air Gap Support. Defender AirGap for Object supports air gapping between Cloud Access Connectors.

Inside-the-Vault Automation. Enterprise AirGap's Inside-the-Vault hardened solution with in-band management and full automation from a virtual machine within the cyber vault. It leverages Smart AirGap technology to only sync data when it's actually safe to replicate. It also offers S3 bucket-level replication. And it supports immutability with ECS Object Lock and bucket versioning.

Rapid Recovery. Allows the vault ECS cluster to present an immutable copy of data at petabyte scale. The Object Lock feature keeps the object data safe from modifications in a recovery scenario.

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

Flexible Data Protection. Many-to-one support for protection of multiple source ECS clusters to a single ECS vault cluster. Select your data protection by bucket or object path.

Powered by Dell ECS-Sync. Provides a high-performance object-to-object sync tool that's designed for ECS to ECS sync operations.

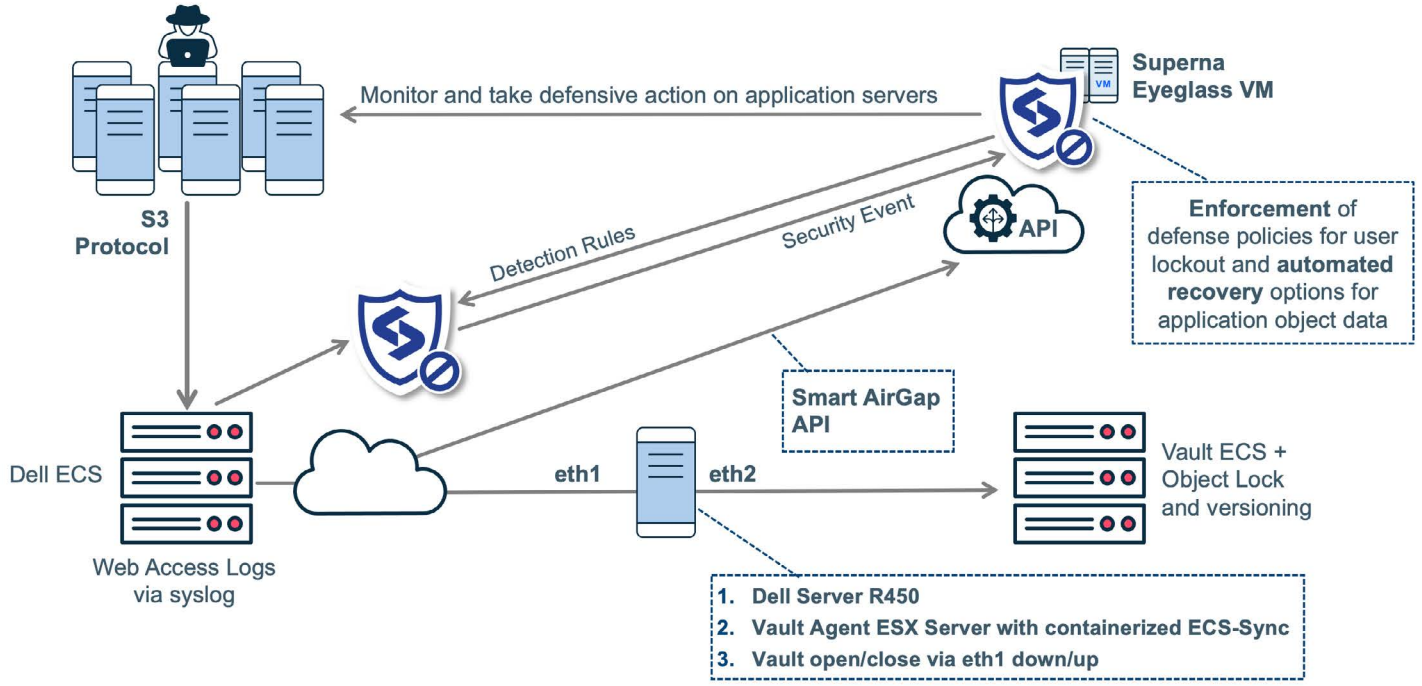
Smart AirGap. The only solution in the market that uses real-time, zero-trust user behavior monitoring to restrict updates to a vault copy if the source data is under threat. Smart AirGap custom policies allow Easy Auditor integration to enable real time policies for determining criteria for opening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

Simplified Network Management. Ransomware Defender Enterprise Vault Agent manages the network between the production cluster and the vault cluster with full ethernet interface down or up automation..

Robust Reporting. Fully-automated daily reporting of synced data with summary reports; per-sync-job object list of successful or failed syncs; in-band ECS vault cluster hardware monitoring for alerts and free space management

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.

Superna Ransomware Defender for Dell ECS: Air Gap with Containerized ECS-Sync



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 automatic snapshot creation	✓
Recover	File-level tracking and snapshot data recovery	✓

SUMMARY

Superna Ransomware Defender provides real-time security for object data in on Dell Isilon, PowerScale, and ECS. It provides monitoring, alerting and automated lockout of accounts experiencing malicious object data IO patterns. It audits and monitors all access and analyzes data access behavior for indications of suspicious or undesired behaviors including ransomware. Superna Ransomware Defender allows you to determine *who* is accessing your data and *when* they're doing so. It enables forensic auditing of data access, and helps defend against untrusted data access behaviors.

With Superna Ransomware Defender, you can defend against security threats, protecting data from leakage, ransomware, and cyberthreats. You can audit and analyze data easily and extensively, to help maintain regulatory compliance. And you can simplify root cause analysis of a data breach or other data event.

By focusing on a "data first" strategy, Superna's tools for security, analytics and protection can help you reduce risk and achieve better business results. Superna Ransomware Defender is a subscription service, and is licensed per terrabyte within protected buckets.

WANT TO LEARN MORE?

Interested in learning more about how Superna allows you to secure and protect your structured and unstructured data regardless of where it resides: on-prem, in the cloud, or in a hybrid environment? Contact us to speak to one of our data protection experts or to schedule a personalized demo.

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