superna®

SOLUTION BRIEF

Superna Ransomware Defender

Detect, stop, and recover from cyberattacks in Dell Isilon, PowerScale and ECS

DELL Technologies

THE CHALLENGE

Many sectors — especially financial services, healthcare, media, infrastructure, and government — have been the target of persistent ransomware attacks. Some make headline news, others are quietly covered up, but up to $265 billion in ransomware damages have been projected. You can't afford to be in a position to permanently lose data, pay extortionate bribes, suffer outages, or face productivity impacts. Unfortunately, traditional approaches to network security, disaster recovery, backups and snapshot archives don't always prevent (or even detect) these types of activities, leaving you wide open to bad actors.

You need sophisticated ransomware protection — embedded at the storage layer — along with robust mechanisms for meeting business continuity and disaster recovery efforts after an attack. You need a unified solution that provides better protection with less effort, so you can restore operations quickly and confidently. Consider this: 33 billion records lost in 2023; $456 million in ransomware payments in 2022; $243 billion in banking non-compliance fines since 2008; and a 50% increase in cyber insurance premiums in 2023. Investing now in cyberstorage protection not only makes good business sense, it's essential!

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. By monitoring user file system accesses, Ransomware Defender detects changes to users' 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 can detect, stop and recover from ransomware attacks and other cyberthreats on Dell Isilon, PowerScale, and ECS storage platforms.

HIGHLIGHTS

- Superna® Ransomware Defender™ is an add-on product to Superna Eyeglass that provides universal file and object threat mitigation for object storage environments
- Real time threat detection, alerting, mitigation with attacker lockout; infected files logged for precision recovery
- Defends against untrusted or malicious data behaviors, including ransomware, exfiltration, mass delete, and untrusted network access in object storage
- Provides post-breach analysis for compliance and forensics
- Based on best practices established by the National Institute of Standards and Technology (NIST)

WHY CYBERSTORAGE?

Gartner's 2023 Hype Cycle for Storage and Data Protection Technologies recommends that you "prioritize active protection and security of unstructured and structured data storage systems because limiting or blocking an attack is more effective than recovering from one."

Ransomware Defender works by monitoring user data in real time on storage clusters, checking for suspicious operations including file encryption. As soon as activity is detected, access from the infected user's account is blocked. The product can manage multiple clusters, each with multiple shares, and when suspicious activity is detected on one share on one cluster, the user's access to all managed shares and clusters is removed.

Once activity is detected and a user is blocked, a notification is immediately sent to the administrator. The lockout is applied at the user level, and the locked-out user will be unable to connect to the storage from any device. The product locks-out only the infected user, allowing other users to continue to access the storage. Automated snapshots help protect the file system from multi-user attacks, minimizing data loss and limiting business interruption.

KEY FEATURES

- Detects suspicious behavior consistent with ransomware access patterns, alerting administrators upon detection of unusual behavior.
- Prevents ransomware from encrypting user data on storage clusters.
- Learning Mode automatically monitors behaviors and adjusts detection logic to avoid false positives.
- Prevents attacks from compromising data with automated lockout action against shares and NFS exports accessible by infected users, limiting potential damage.
- Simplifies recovery by tracking compromised user accounts; 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 attack origin (e.g. VPN, office network; data center network; etc.).

Ransomware Defender also identifies the files that tripped the threat detector, along with the previous 1 hour's worth of files accessed by the user. This helps build a profile of the exact files that require remediation and recovery from the attack. To be properly prepared for a ransomware attack, make certain that client machine anti-virus scanning is enabled and that regular backups are being created. In the event of an attack, well-designed snapshot policies and snapshot retention policies will allow you to access multiple recovery points, to minimize business disruption.

Monitor List support. Protects with alerts, snapshots, but no lockout occurs. Can be configured by path, user, or IP address. This allows customized protection for application servers and avoids the risk of lockout but still providing protection for the data.

USE CASES

Auditing

- Who did what and when to your data?
- Idenifying stale data, or data with no access IO

Forensic audit of data acess

- Historical logs to identify root cause of any data breach
- Helps ensure compliance with industry regulations for audit data access

Defends against untrusted or malicious data behaviors

- Identifies and responds to suspicious data access behaviors including ransomware attacks

Whitelist Support. Allows the admin to keep a list of file system paths, user accounts, server IP addresses that are excluded from monitoring, such as application server service account.

Multi-cluster-aware monitoring. If malicious behavior is detected on one cluster, protective actions are applied to all (Eyeglass-licensed) clusters on the network to which the user has access.

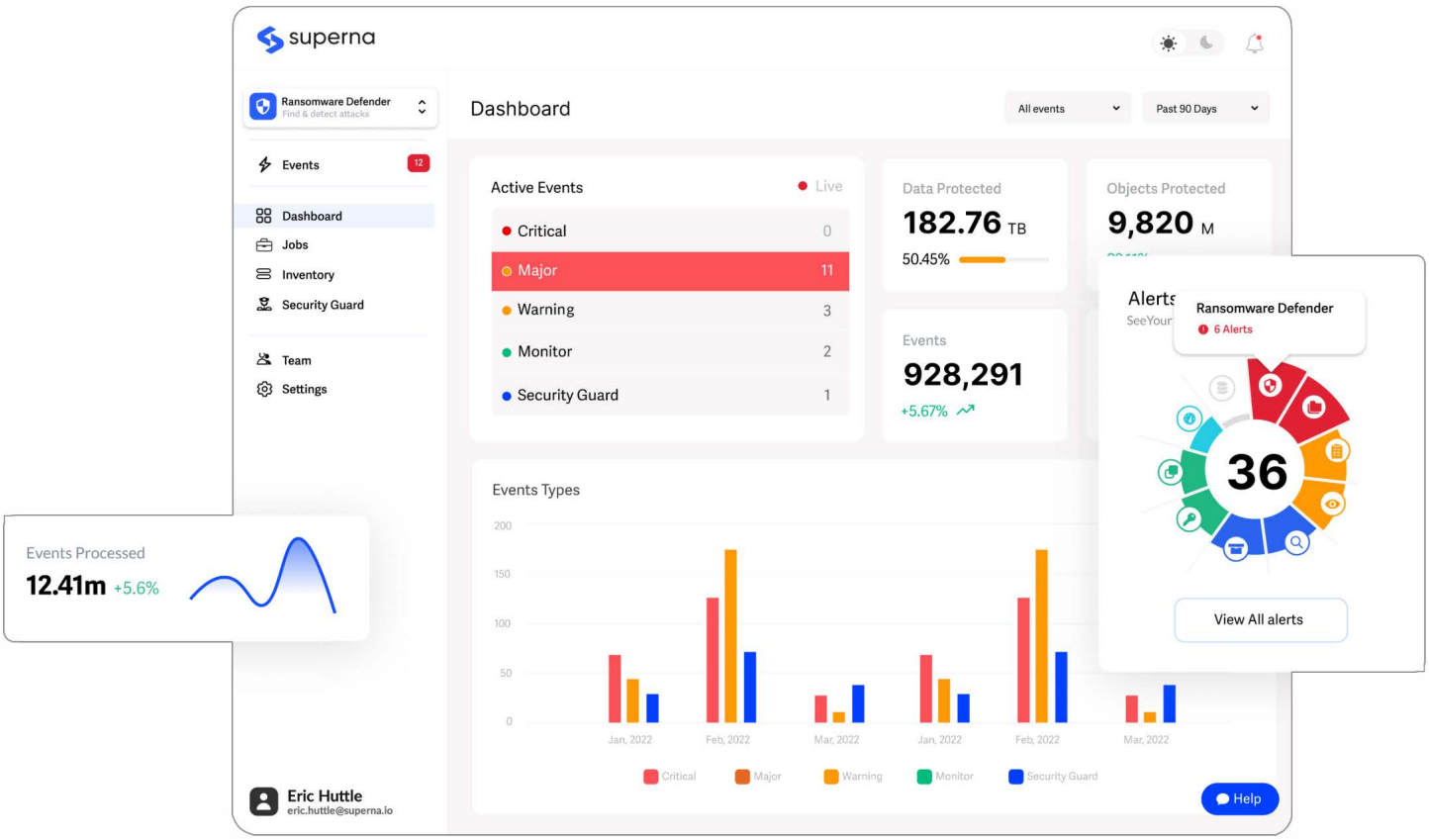
Integrated SyncIQ with AirGap 2.0. Allows for a 3rd offline copy with Automated Airgap management, vault Isilon cluster proxy alarm monitoring and Smart AirGap copy manages SyncIQ sync jobs when no suspicious activity has been detected on source data.

Security Guard. An automated penetration test ensures defenses are operational, while penetration test logs allow administrators to monitor the health of security defenses and "alerts failed" penetration tests

Object Data Protection. Storage is monitored in real-time for suspicious activity and, if enabled, the authenticated user is disabled, protecting object data. Smart AirGap identifies threats to Object data, blocking AirGap replication.

AUTOMATIC LOCKOUT PROTECTION

If Ransomware Defender detects attack behavior, it initiates multiple defensive actions, including locking users from file shares. Timed Auto-Lockout rules help ensure that action is taken even if an administrator is not available, with automatic response escalation if multiple infections are detected.



OUTSTANDING BUSINESS VALUE

Superna Ransomware Defender provides your business with numerous important benefits, including:

Enterprise Security Administration. Role Based Access Control allows Eyeglass administrators to assign a Ransomware role using Isilon Authentication providers and Active Directory groups to manage and monitor Ransomware Defender security settings and incidents separately from DR monitoring.

Scalability. Ransomware Defender is built to operate at scale using the compute and storage node concept. Integration with Dell Isilon Access Zones and HDFS features enables user behavior analytics data to be stored on Isilon.

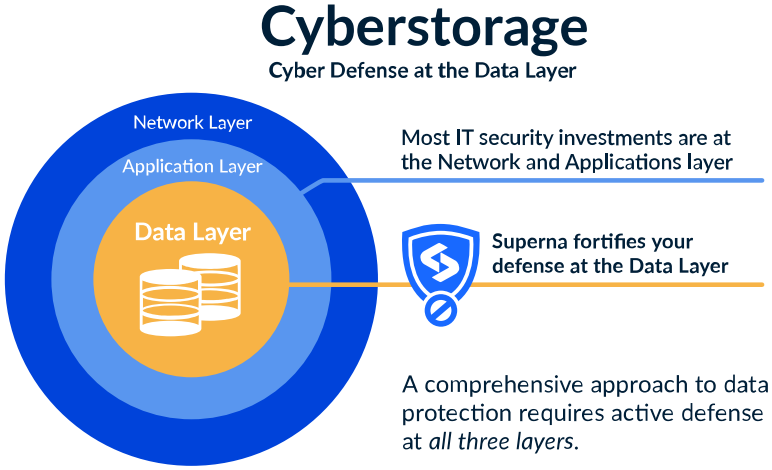
Measurable return on investment. Minimizing the impact of business disruptions, and helping reduce premiums for cyberthreat insurance.

Security tooling integration. You can set-up Webhooks, a Zero-Trust API, and even integrations with popular IT security and operations platforms like ServiceNow, Splunk, and Palo Alto Networks. These will feed Superna data into the central dashboards and alerting mechanisms for seamless monitoring in your security tools of choice!

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 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, regardless of where they originate.

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 close the gap left by traditional data security solutions, helping you reduce risk and achieve better business results. Superna Ransomware Defender is a subscription service, and is licensed per terabyte within protected buckets.

About Superna

For more than a decade, Superna has provided innovation and leadership in data security and cyberstorage solutions for unstructured data, both on-premise and in the hybrid cloud. Its solutions are in use in thousands of organizations around the globe, helping them to close the data security gap by providing automated, next-generation cyber defense at the data layer. Superna is recognized by Gartner as a solution provider in the cyberstorage category. For more information, visit www.superna.io.

Ready to get started? Contact Superna today!

superna®
Prevention is the new recovery

superna.io | sales@superna.io