DATASHEET

superna®

Superna® Ransomware Defender™

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

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.

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.

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 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)

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.

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 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.

USE CASES

Auditing

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

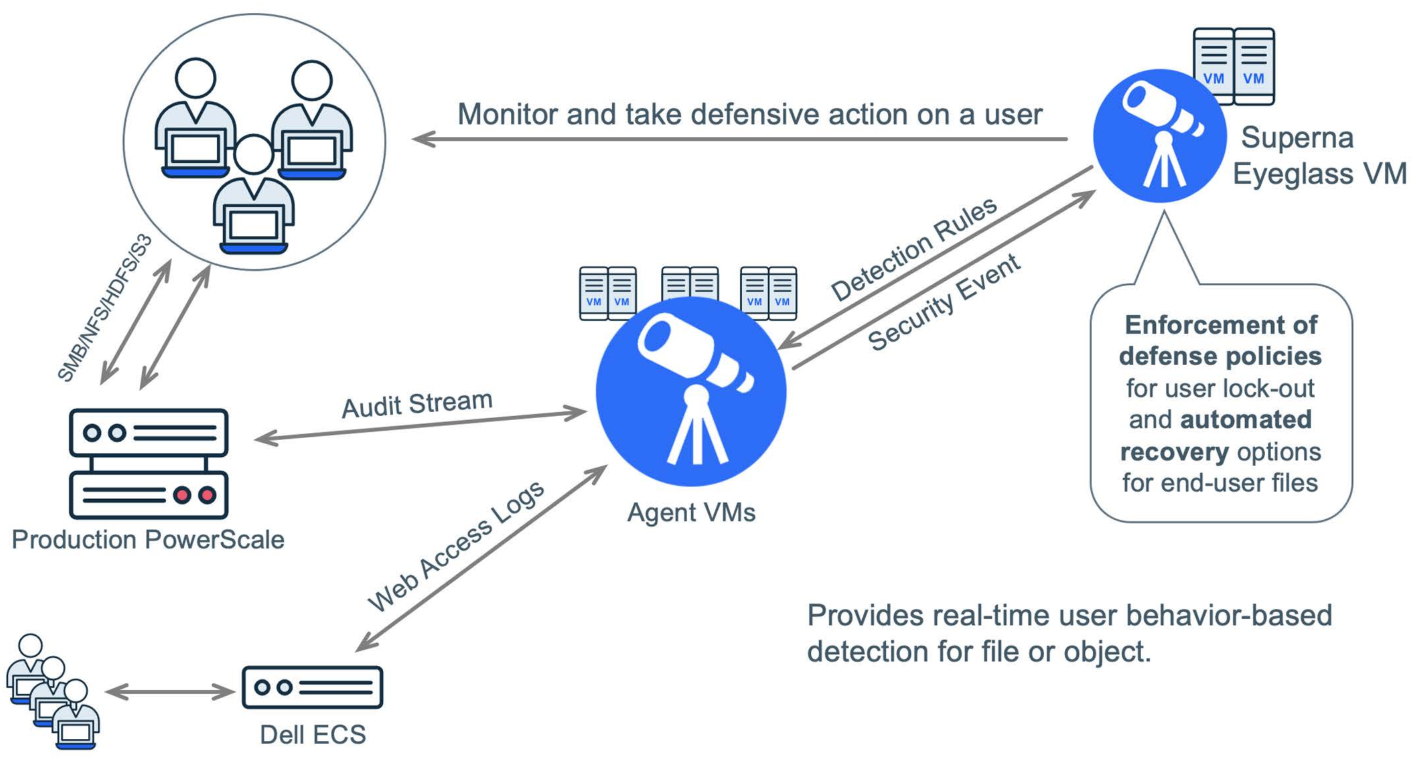
Forensic audit of data acess

- 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

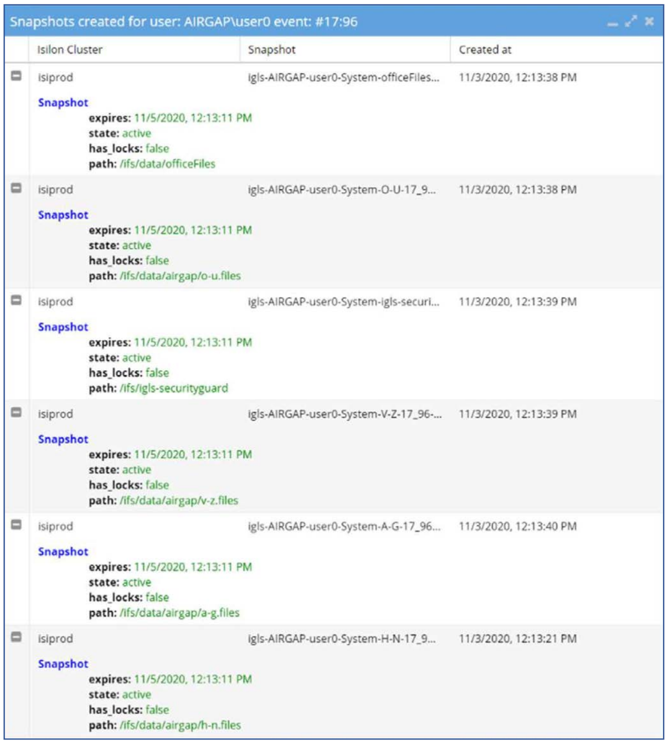
Superna Ransomware Defender provides unified data protection for file and object.


Monitor and take defensive action on a user
VM
VM
Superna Eyeglass VM
SMB/NFS/HDFS/S3
Detection Rules
Security Event
Audit Stream
Agent VMs
Production PowerScale
Web Access Logs
Dell ECS
Enforcement of defense policies for user lock-out and **automated recovery** options for end-user files

Provides real-time user behavior-based detection for file or object.

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.



```
Snapshots created for user: AIRGAP\user0 event: #17:96

Isilon Cluster     Snapshot                                  Created at
isiprod            igls-AIRGAP-user0-System-officeFiles...   11/3/2020, 12:13:38 PM
Snapshot
        expires: 11/5/2020, 12:13:11 PM
        state: active
        has_locks: false
        path: /ifs/data/officeFiles
isiprod            igls-AIRGAP-user0-System-O-U-17_9...      11/3/2020, 12:13:38 PM
Snapshot
        expires: 11/5/2020, 12:13:11 PM
        state: active
        has_locks: false
        path: /ifs/data/airgap/o-u.files
isiprod            igls-AIRGAP-user0-System-igls-securi...   11/3/2020, 12:13:39 PM
Snapshot
        expires: 11/5/2020, 12:13:11 PM
        state: active
        has_locks: false
        path: /ifs/igls-securityguard
isiprod            igls-AIRGAP-user0-System-V-Z-17_96-...    11/3/2020, 12:13:39 PM
Snapshot
        expires: 11/5/2020, 12:13:11 PM
        state: active
        has_locks: false
        path: /ifs/data/airgap/v-z.files
isiprod            igls-AIRGAP-user0-System-A-G-17_96...     11/3/2020, 12:13:40 PM
Snapshot
        expires: 11/5/2020, 12:13:11 PM
        state: active
        has_locks: false
        path: /ifs/data/airgap/a-g.files
isiprod            igls-AIRGAP-user0-System-H-N-17_9...      11/3/2020, 12:13:21 PM
Snapshot
        expires: 11/5/2020, 12:13:11 PM
        state: active
        has_locks: false
        path: /ifs/data/airgap/h-n.files
```

The storage device maintains file system snapshots applied by Superna that allows for data recovery in a multi-user infection attack scenario.

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.

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 such as 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.

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