DATASHEET

superna®

Superna® Ransomware Defender™ for Object

The Ransomware Defender module monitors individual user behaviors to detect, stop, and recover from ransomware attacks for the Dell ECS storage platform.

OVERVIEW

Superna® Ransomware Defender™ for Object is the only Zero-Trust, S3-native real-time data protection solution. The software detects if a user has been compromised and will take a series of automated actions to stop the infected user by locking out access. Object tracking provides a list of affected objects for recovery.

REAL-TIME PROTECTION AT THE DATA LEVEL

Ransomware Defender is designed to detect, stop and recover from ransomware attacks and other cyberthreats on Dell ECS storage platforms. 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.

KEY FEATURES

Detects Cyber Threads. Superna Ransomware Defender for Object detects user behaviors consistent with ransomware access patterns, and automatically initiates steps to lock-out user access.

Auto-Detects Your Storage. Ransomware Defender automatically detects Name Space, Bucket and Object, with auto discovery of Dell Elastic Cloud Storage.

Multiple Protection Use Cases. Protects your GeoDrive data; Backup Servers; PACS Archive Servers; and any S3 Application IO transparent data independent data protection.

Fully Automated Learning Mode. Automatically monitors behaviors and customizes detection logic; avoids false positives.

Automatic Alerting. Administrators are alerted upon detection of suspicious or unusual behavior.

Highly Customizable. Easily configurable to allow a wide range of automated responses, from “monitor only” to “immediate user lockout.

HIGHLIGHTS

- Detects user behaviors consistent with ransomware access patterns
- Fully-automated learning mode monitors behaviors and uses learnings to customize detection logic
- Security Event Data helps simplify recovery
- Automated penetration tests help ensure that defenses are fully operational
- The only rapid recovery solution (< 2 hour) for petabyte-scale data.
- Based on best practices established by the National Institute of Standards and Technology (NIST)

Automated Lockout. Automated lockout action against user S3 keys prevents the attack from compromising data and limits the damage.

Security Event Data Simplifies Recovery. Security Incidents track compromised user account; infected files; previous file access history prior to attack; and client machine IP address, to track the attack's origin.

Monitor List Support. Protects with alerts, snapshots but with no lockout. Configurable by path, by user or by IP. Allows customized protection for application servers and avoids the risk of lockout while still protecting the data.

Whitelist Support. Allows administrator to maintain a list of file system paths, user accounts, server IP addresses, all of which are to be excluded from monitoring (example: application server service account).

Multi-Cluster-Aware Monitoring. If malicious behavior is detected on one cluster, protective actions are automatically applied to all Superna Eyeglass-clusters on the network to which the user has access.

Security Guard. An automated penetration test helps ensure that defenses are fully operational. Penetration test logs allow administrators to easily assess the health of their security defenses, along with alerts of failed penetration tests. Tests are automated and scheduled, and can cover multiple clusters.

SUMMARY

Superna Ransomware Defender for Object provides real-time security for object data in on Dell ECS storage platforms. 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 terabyte 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.

20230715