superna®

SOLUTION BRIEF

Superna Ransomware Defender

Protect, manage, and secure your unstructured data in Amazon S3 environments

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!

RANSOMWARE DEFENDER FOR AWS

When unstructured data moves to the cloud, security needs to move with it. Superna® Ransomware Defender™ for AWS enhances the security of cloud data stored in S3 with an adaptive security solution that monitors storage IO and separates normal from suspicious or malicious IO. It offers real-time detection, alerts, attack mitigation, and attack recovery with a precise list of infected files for rapid, surgical recovery.

Ransomware Defender™ for AWS is deployed via AWS cloud formation templates from the AWS marketplace to simplify provisioning and

HIGHLIGHTS

- Superna® Ransomware Defender™ for AWS provides universal file and object threat mitigation for Amazon S3 hybrid cloud environments
- Defends against untrusted or malicious data behaviors, including ransomware, exfiltration, mass delete, and untrusted network access in S3 buckets
- 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."

management on AWS, and leverages AWS services for simplicity and scalability. It automatically learns behaviors and customizes configuration using a learning mode.

Stress test your security with the Security Guard feature that offers a simulated "attack and defend" automation to test your cyber defenses, train operations staff, verify detection is active, and integrate alarms into your SOC test procedures.

Ransomware Defender works by monitoring user data in real time, 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
- Real time threat detection, alerting, mitigation with attacker lockout; infected files logged for recovery
- Defends against encryption, high-rate/mass deletes, suspicious IO behaviors
- Native AWS deployment leverages AWS services (Cloud Trails, Kafka MSK, SNS, EC2 Autoscaling Groups)
- Role-Based Access Controls
- Auto-learning baselines normal bucket access pattern to distinguish attacks from normal IO patterns
- Per-bucket protection configuration
- Centralized support for multiple regions
- Alerts via email, syslog, web hooks, other integrations
- Dynamic scaling matches processing to workload
- Event rate graphing for performance management
- Historical event tracking
- False positive flagging for manual overrides
- Ignore list to suppress monitoring by bucket or object key path wildcard
- Monitor list to disable user account lockout function and enable only detection, object tracking and alerting, with per-bucket or object key path wildcard support
- Subscription licensing based on S3 buckets

USE CASES

Auditing

- *Who* did *what* and *when* to your Amazon S3 data?
- Identifying stale data – or data with no access IO – in S3 buckets

Forensic audit of S3 data access

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

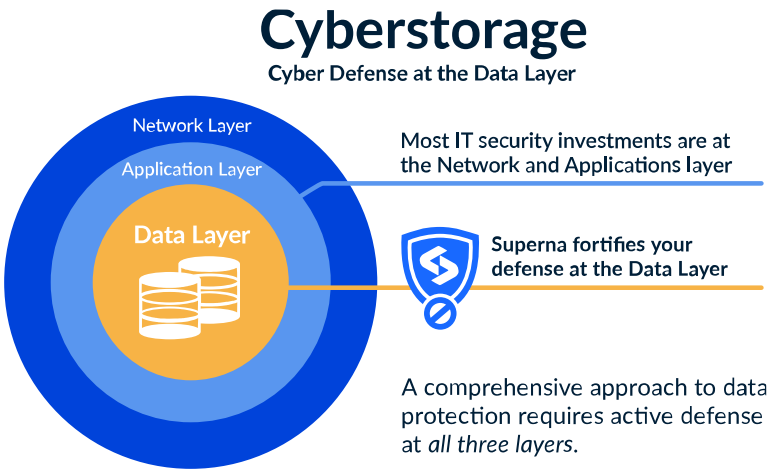
Defends against untrusted or malicious data behaviors

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

SUMMARY

Superna® Ransomware Defender™ for AWS provides real-time security for object data in AWS S3 services. It provides monitoring, alerting and automated lockout of accounts experiencing malicious object data IO patterns. It audits and monitors all access to S3 buckets and analyzes data access behavior for indications of undesired behaviors such as ransomware. Superna Defender for AWS 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 for AWS, you can:

- Audit and analyze data more extensively
- Protect data from leakage, ransomware, and cyberthreats more completely
- Defend against security threats
- Maintain regulatory compliance
- 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 for AWS is licensed per-terabyte within protected buckets and is available as a subscription service, with bucket bundle pricing available.

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!