superna®

Ransomware Defender for AWS S3

Product Datasheet

Secure cloud storage in Real-time

Superna Eyeglass© Ransomware Defender for AWS S3

Amazon AWS S3 Storage Protection

Cloud Storage available from AWS S3 service exposes your corporate data to Internet based attacks on your data.

Enhancing 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. The solution offers real time detection, alerts, attack mitigation and recovering from the attack with a precise list of infected files.

Deployed with Cloud formation templates and leverages AWS services for scaling and simplicity. Automatically learns behaviors and customizes configuration with Learning mode.

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

Key Features

1. Real time threat detection, alerting, mitigation with attacker account lockout, infected files are logged for recovery

United States
225 Cedar Hill Street, Suite 200
Marlborough, Massachusetts 01752

superna®

Ransomware Defender for AWS S3

Product Datasheet

Secure cloud storage in Real-time

2. Capable of defending against encryption, high rate deletes, suspicious IO behavior
3. Native AWS deployment leveraging native AWS services (cloud trails, Kafka MSK, SNS, EC2 Auto Scaling Groups)
4. Role based Access Controls
5. Mass delete detection to alert when a high rate of deleted objects are detected
6. Automated learning system that baselines normal bucket access patterns and self configures to detect real attacks vs normal IO patterns
7. Per bucket protection configuration
8. Multi region support from a central location
9. Alerting via email, syslog, web hooks
10. Dynamic scaling to match processing to any sized workload using Scale Groups in EC2 and MKS service to scale event processing
11. Event rate graphing to manage performance overtime
12. Historical event tracking
13. Flag as false positive feature if required for manual overrides
14. Ignore list to suppress monitoring by bucket or object key path wildcard
15. Monitor list to disable user account lockout function and enable only detection, object tracking and alerting with per bucket or object key path with wildcard support
16. Smart Airgap API support for integration with AWS Cyber vault replication solution
17. License model is a subscription based on S3 buckets
18. Integration with 3rd party IDS, IPS security solutions monitoring your EC2 instances. Integration uses the smart Airgap API that allows inbound notifications of application server or network traffic detections to inform that storage layer to take actions against a user

United States
225 Cedar Hill Street, Suite 200
Marlborough, Massachusetts 01752

or source IP address of an attacker.

Visit the product page at
https://www.supernaeyeglass.com/cyber-scanner
Contact us at sales@superna.net

United States
225 Cedar Hill Street, Suite 200
Marlborough, Massachusetts 01752