DATASHEET

superna

Superna Defender™ For AWS

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

OVERVIEW

Organizations are moving more data and applications to the public cloud, in order to take advantage of the scalability, performance, and cost efficiencies it can provide. While cloud vendors are responsible for maintaining the physical network, infrastructure and hypervisors, securing and protecting that data falls under a "shared responsibility" model. In this model, the customer owns the workload OS, apps, virtual network, access to their tenant environment, and the data. And while the cloud vendor will provide some basic security, the ultimate responsibility for securing and protecting the data falls to the organization. Bottom line? Public cloud storage can expose your data to cyberthreats.

SUPERNA DEFENDER™ FOR AWS

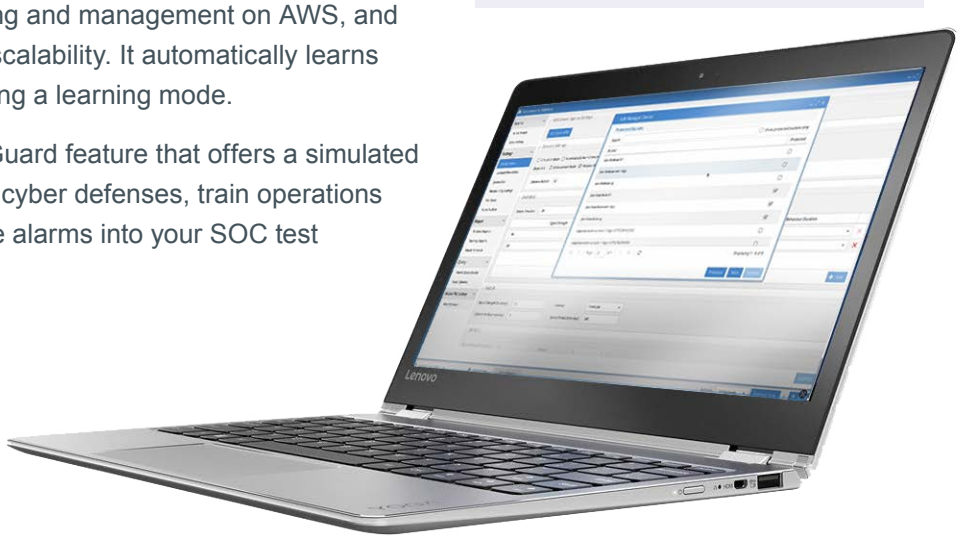
When unstructured data moves to the cloud, security needs to move with it. Superna Defender for AWS enhances the security of cloud data stored in S3 with an adaptive security solution that monitors storage IO and separates normal from suspicious or malicious IO. It offers real time detection, alerts,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

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

HIGHLIGHTS

- Superna 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
- Post-databreach analysis for compliance and forensics
- Based on best practices established by the National Institute of Standards and Technology (NIST)



KEY FEATURES

- Real time threat detection, alerting, mitigation with attacker lockout; infected files logged for recovery
- Defends against encryption, high-rate/ mass deletes, suspicious IO behavior
- 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
- 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
- Smart Air Gap API for integration with AWS Cyber Vault replication
- Subscription licensing based on S3 buckets
- Integration with 3rd party IDS, IPS security solutions for monitoring EC2 instances

USE CASES

Auditing

- Who did what and when to your Amazon S3 data?
- Idenifying stale data in S3 buckets; data with no access IO

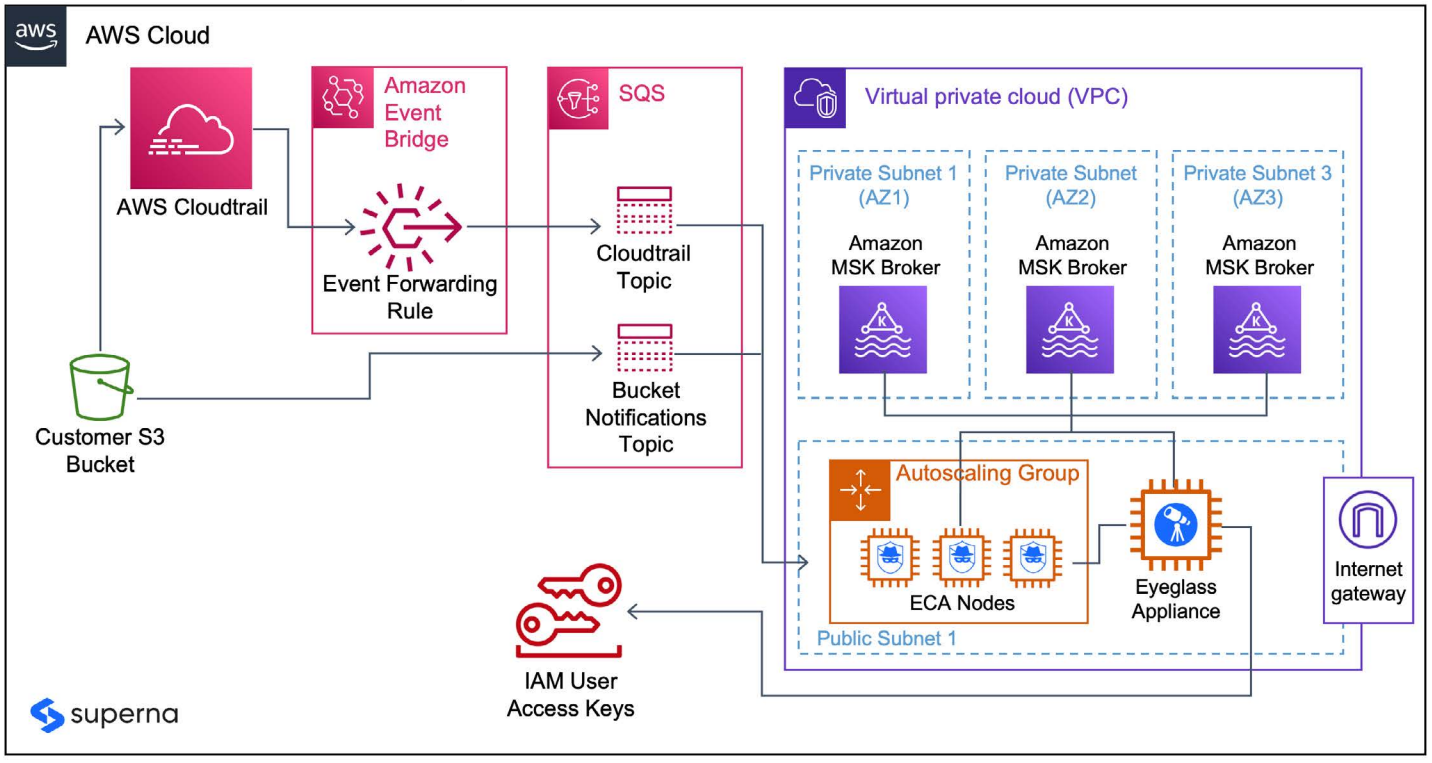
Forensic audit of S3 data acess

- 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 Defender™ for AWS



SUMMARY

Superna 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 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 you achieve better business results. Superna Defender for AWS is licensed per tb within protected buckets and is available as a subscription service, with bucket bundle pricing available.

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

20230308