White paper - Integrated Cyber Security Defense Strategies

Multi vector Smart Airgap Defenses for Unstructured Data

Overview

Unstructured data attacks are increasing with an attack every 11 seconds. The nature and type of attacks is getting more sophisticated, with attacks using multi-vector attacks that look for vulnerabilities across OS's, networks and storage devices.

The target of these attacks is predominantly file data. This means enterprises need to invest in multi vector defense strategies that are tightly integrated with capabilities to detect, identify, respond, and recover.

This whitepaper explains how Ransomware Defender can extend into 3rd party solutions with API trigger support to protect your critical data and how a multi vector defense strategy can better protect your data.

How to improve your security posture with a comprehensive approach

The simple answer is an integrated approach that allows different security domains to share threat information with automated responses to threats. Without real-time automated responses, reaction times simply won't keep up with the active threats facing enterprises today, placing corporate data at risk.

Superna security products offer a complete solution that proactively protects data in production while also using information from external security tools to block replication into the cyber vault and maintain a clean good copy of data.

Ransomware Defender's Smart Airgap API allows leveraging sensor knowledge at multiple layers (network,

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

storage, IDS, perimeter, endpoint protection) combined with an integrated Smart Airgap Cyber vault using Dell EMC Powerscale.

Superna security products offer a complete solution combining Ransomware Defenders threat knowledge, Easy Auditor's real-time triggers for Data Loss Prevention, Mass Data Delete detection, custom security triggers and long term audit data retention for forensic analysis.

What are Multi Vector Defenses?

A detection vector is a type of security monitoring focused on a particular layer of the application stack, example Operating systems, file systems, network packet flows, application logs, firewalls, email logs, syslog events from switches and routers are all areas where security products can detect malicious behavior.

Many attacks use the network to probe defenses and look for vulnerabilities along with machines listening on common ports like SMB and NFS. During this phase the attacker would be using tools to scan the network and using the vulnerabilities identified to build an attack plan against the intended targets. This is an example of a detection vector that can uncover this malicious activity just prior to the attack being launched.

By leveraging network detection solutions that observe networking device flows, this activity can be flagged as an early detection of suspicious activity. This is a key point in the attack that can be leveraged to prepare for the attack and protect data.

From a timeline perspective this window of time when devices are being probed could be very small and preparing for this impending attack requires a real-time response.

superna®

White paper - Integrated Cyber Security Defense Strategies

Multi vector Smart Airgap Defenses for Unstructured Data

Operations staff monitoring alerts from networking security devices may be too slow to be of any value since the attacker could launch the attack before the alerts are reviewed by security staff.

Many customers are not able to staff 7/24 security personnel to monitor network security events allowing an attacker the ability to launch an attack when no one is available to review and respond to the security alert.

Detecting at the network layer with an alert does not offer any proactive protection at the storage layer which is the target of the attack.

These challenges can be overcome with an automated multi vector integrated defense solution that automates the process between the network layer defenses and the storage layer defenses. Even low level suspicious activity flagged as a warning could be used to prepare an automated response action.

Let's review the components of this solution.

The solution components:

1. Ransomware Defender is a storage layer protection solution for file and object data that monitors user behavior and protects data in real time with user file system lockouts, snapshots, file and object tracking and infected host IP tracking, along with fully integrated Cyber vault automation for offline data management.
2. Ransomware Defender Smart AirGap API to enable bidirectional integration with 3rd party security platforms

Network Monitoring solution

A network security device with anomaly

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

detection, flow analysis that is able to detect suspicious activity and send and receive trigger notifications to cause an action to be taken within the network. This type of network security device offers maximum data protection by integrating with Superna's Smart AirGap API to protect data.

The next section discusses how this integration works.

Security Domain Integration between the Network and Storage layer

In order to integrate defense layers from network to storage, API's are required to automate decision making and responses.

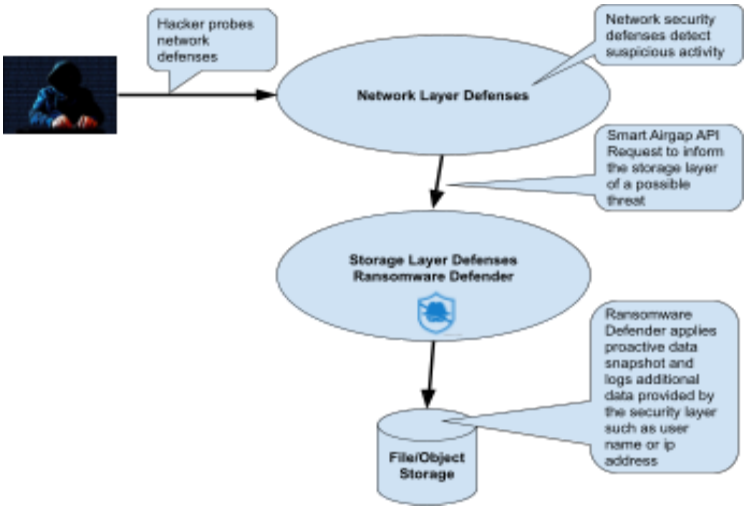
Superna Ransomware Defender exposes the Smart Airgap API to 3rd parties. This API provides an integration point to connect detection systems at the network layer or other layers, for example email gateways, Intrusion detection system, Firewalls, SIEM tools, endpoint protection etc. By connecting network detection threat warnings to the Intelligent storage layer defenses the SmartAirGap API can provide a hand off for decisions and responses to the storage layer to take proactive actions to safeguard the data before the impending attack begins.

The following diagram shows the integration at the network security layer that notifies Ransomware Defender of a network warning. This API request can be a generic warning or pass in more specific information like user name and host ip address.

superna®

White paper - Integrated Cyber Security Defense Strategies

Multi vector Smart Airgap Defenses for Unstructured Data



Smart Airgap API Features

1. **Inbound Notifications**
   a. Threat warning notification from external devices allows Ransomware Defender to snapshot critical data proactively.
   b. OR Block replication into the the cyber vault to ensure data integrity in the vault
   c. OR User lockout request from the network layer. This can enable the network layer to request a user to be banned from access to storage using Ransomware Defenders unique user aware storage lockout.

2. **Outbound Notifications**
   a. Storage layer detection of suspicious user behavior allows the user name and host IP address to be sent to external security tools. This allows network layer devices to monitor a host or potentially disconnect the host from the network, disable AD account, or quarantine email as an automated action after receiving a notification from the Smart AirGap API.

Cyber Vault Integration

Cyber Security Frameworks suggest

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

that offline data or a cyber vault is a key component of a security strategy. The Ransomware Defender solution offers a complete range of options for Cyber vaulting data including Airgap automation, data replication reporting, data safe replication, inband management of vault storage to lower the administrative overhead and most of all **Intelligence**.

How does Intelligence speed the recovery of data in a Cyber Vault?

Ensuring suspect or compromised data does not reach the secure cyber vault is the number one objective. This is how recovery times are reduced by having file level audit logs to determine what data was compromised and when it occurred. Ransomware Defender and Easy Auditor provide full traceability of where, when and who compromised the data.

Any solution without user and file level historical traceability from production systems prior to the attack will extend recovery times since data selection from the vault will be trial and error.

False positive identification of clean data only adds to the cost and time to restart a large recovery effort using a previous version of the data in the vault. This trial and error increases recovery time dramatically. This is why full user audit log historical data is so important to quickly and accurately identify the beginning of the attack, The Superna Easy Auditor product provides long term audit data for forensic analysis.

It is important to note that a vault solution by itself does not improve your security posture, it only addresses cleaning up after a cyber disaster has occured.

Enterprises should focus on the big picture which is to arm the infrastructure with detection and

response solutions and long term audit data retention that is **always** required for a forensic audit post cyber attack to assist in recovery of data with or without a cyber vault.

Conclusion

The rapid threat landscape requires an updated threat response system that removes humans from the response and allows rapid multi-vector detection responses regardless of where the threat originated in the infrastructure.

Ransomware Defender, Easy Auditor and the Smart Airgap API provides the ability to integrate security with Intelligent, proactive data protection to keep pace with the evolving sophistication and speed of today's cyber attacks.

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