Integrated Cyber Security Defense Strategy

Against Multi-vector Attacks for PowerScale Data

Introduction

Cyber attacks have become a serious and continuous threat to businesses of all sizes and verticals. A cyber attack is happening every 11 seconds and the average cost of one is $13M and growing. Cyber-attacks are also getting increasingly sophisticated to break through even fairly modern security setups. In fact there are sophisticated DevOps processes that "attack innovations" go through to break even the latest security stances. Attackers are using multi-vector attacks that look for vulnerabilities across end-user devices, applications and operating systems, networks as well as data storage infrastructure. While there are point solutions for these multiple layers of IT ecosystem it is crucial to link these layers to minimize the time to detect and respond to these attacks.

This whitepaper explains how Dell PowerScale Cyber Protection Solution powered by Superna's Ransomware Defender and Smart Airgap technologies, can leverage security intelligence coming from different layers of the IT ecosystem using API integration. The API integration can trigger automated response like replication termination to the cyber vault, blocking suspicious users, tagging corrupt data etc. even while the attackers are still trying to break through the security layers. This approach can drastically cut down the detection and response timelines and put IT teams a step ahead of the attackers.

Overview of Dell Technologies Cyber Protection Solution for PowerScale/Isilon

The Dell PowerScale Cyber Protection Solution has two main components:

Data Isolation with Smart Airgap

The Smart Airgap solution isolates a copy of the data from all internal and external network paths and is the recovery copy of last resort. After the initial replication of data to the cyber vault, an airgap is maintained between the production environment and the vault copy. Any further incremental replication is done only intermittently by closing the airgap after ensuring there are no known events that indicate a security breach on the production site.

Detection of suspicious patterns of data access and trigger a wide range of responses

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.

Multi-vector Attacks and Multi-layer Detection

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. Here are two security layers that are responsible for most of the attacks.

Network layer

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.

Application layer

The saying goes: "In today's world, attackers don't really need to hack in; they just log in." The area of Identity and access management technologies are a key component of cyber security strategy. These technologies use artificial intelligence and machine learning to look for suspicious activity from authorized users. Distributed Denial of Service (DDoS) attacks are another type of application layer attack where heavy traffic overwhelms web services and leads to server crashes. There are tools both at the content delivery networks (CDNs) as well as tools that are embedded on the web servers to detect and avert such attacks.

While there are detection mechanisms at multiple layers of the IT ecosystem the key is to minimize the time to detect and respond and here are some of the challenges involved:

- ✓ 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.
- ✓ 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.
- ✓ Not all organizations are 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.
- ✓ Moreover, 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.

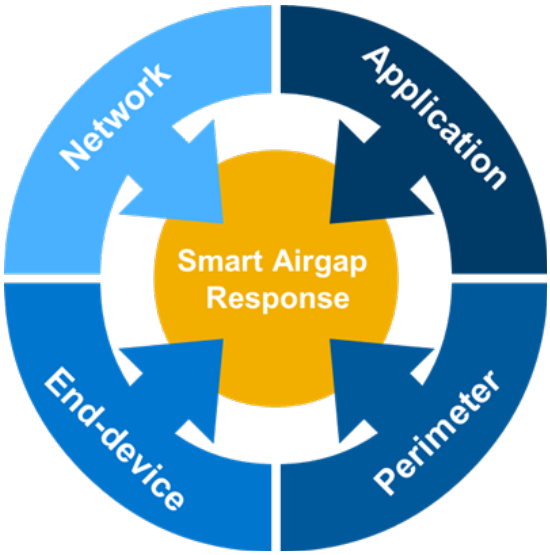
These challenges can be overcome with an automated multi vector integrated defense solution that automates the process between the network layer defenses and the storage layer defenses. Even low-level suspicious activity flagged as a warning could be used to prepare an automated response action.

Smart Airgap API for Integrated Detection and Response

Dell PowerScale Cyber Protection Solution offers 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. The Smart Airgap API allows leveraging sensor knowledge at multiple layers combined with an integrated Smart Airgap Cyber vault using Dell Powerscale.

The Smart Airgap 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 Smart AirGap 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.



Smart Airgap API Features

Following are ways the inbound API triggers can be used to increase the speed of response:

- ✓ Threat warning notification from external devices allows Ransomware Defender to snapshot critical data proactively.
- ✓ OR Block replication into the cyber vault to ensure data integrity in the vault.
- ✓ 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.

In addition to the inbound API calls Smart Aigap also provides outbound triggers:

- ✓ 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.

Smart Airgap's Comprehensive Audit Logs

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.

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.

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 occurred.

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.

Superna's Ransomware Defender, Easy Auditor and the Smart Airgap API for Dell PowerScale provide the ability to integrate security with intelligent, proactive data protection to keep pace with the evolving sophistication and speed of today's cyber-attacks.