PowerScale Cyber Protection Suite Reference Architecture

April 2024

H19777.2

White Paper

Abstract

This document describes the PowerScale cyber protection advanced software suite to secure OneFS clusters proactively and store data in a separate air-gapped repository.

Copyright

Contents

Executive summary

Overview

Organizations continue to make strides towards digital transformation with the explosion of unstructured data. As more data is generated, it has become one of the most valuable assets of an organization. Anytime an asset becomes valuable, the malicious actors and organizations begin to take notice. The malicious actors may be individuals, but the organizations could be state-sponsored groups or other criminal organizations.

Protecting data in the current environment is paramount. In fact, cybersecurity governance is the top priority for business leaders. According to the International Data Corporation (IDC), worldwide security investments will grow 12.1% in 2023 to $219 Billion[1]. Furthermore, 88% of board members classified cybersecurity as a business risk[2]. Additionally, cyber risk or cybersecurity insurance policies require a documented cybersecurity plan.

Of the malicious threats, ransomware is the most concerning. In the form of software or malware, ransomware encrypts data and sensitive data is exfiltrated, rendering systems unusable. The cybercriminal holds the data and systems hostage until a ransom is paid.

Revisions

Date	Part number/ revision	Description
September 2023	H19777	Initial release
November 2023	H19777.1	• Updated *Zero Trust API* section • Added *Progress Flowmon ADS* section
April 2024	H19777.2	Minor updates

We value your feedback

Dell Technologies and the authors of this document welcome your feedback on this document. Contact the Dell Technologies team by email.

Author: Aqib Kazi

Note: For links to other documentation for this topic, see the PowerScale Info Hub.

[1] IDC Spending Guide, August 2023.

[2] Gartner Board of Directors Survey 2022, October 2021.

Introduction

Cyber protection and cybersecurity spending continues to increase as it is prioritized by organizations. In recent years, ransomware attacks have been gaining national attention as a result of their ability to disrupt an organization’s ability to operate. An organization’s intellectual property, reputation, and revenues are all at stake in the current environment. The revenue impacts are far greater, given the data privacy laws enacted in recent years. The first recorded cyberattack occurred in 1989. Since then, attacks have become more sophisticated, using malware, ransomware, and phishing attacks.

PowerScale offers cyber protection to secure OneFS clusters proactively and to store data in a separate air-gapped repository. This paper describes the cyber protection components available for a PowerScale cluster.

Cyberattacks

Malicious parties use cyberattacks to gain unauthorized access to corporate networks with a common goal of total control over an organization’s data. From a corporate view, data can be protected through traditional Disaster Recovery (DR) measures, allowing business continuity in the event of a disaster. DR measures focus on the administrative Recovery Point Objective (RPO) and Recovery Time Objective (RTO) requirements for the specified datasets. However, the concepts of DR differ from cyber protection in that cyber protection focuses on data fidelity to address the malicious use of an organization’s data.

Cyberattacks include malware, phishing, and ransomware:

- Phishing is a scam attempt, where users are convinced to provide credentials or personal details through various campaigns.
- Malware is a type of software allowing malicious parties unfettered access to IT systems for data theft and service disruptions.
- Ransomware is a form of malware that encrypts data and allows the malicious parties to exfiltrate sensitive data, rendering files and dependent systems unusable and held captive until a ransom is fulfilled.

Ransomware

Ransomware is the largest cyber threat to organizations. Ransomware completely cripples an organization’s ability to function. All necessary data is encrypted or exfiltrated, and the various systems that depend on the data to function are rendered useless. The organization is no longer able to function as a business. At this point, the malicious party makes a ransom request. If the request is not fulfilled in the specified period, the data is either permanently deleted, dumped online, or is sold to the highest bidder.

Given ransomware’s ability to completely debilitate a business’s primary function, the damage from a typical ransomware attack is often very costly. Ransomware can also cause businesses to lose access to important data through encryption and exfiltration, leading to further financial losses. It is important for organizations to prepare for and mitigate the risks associated with ransomware attacks. Ransomware has become extremely prevalent with constant attacks, as shown in the following figure, mapping ransomware attacks in the United States since 2018.

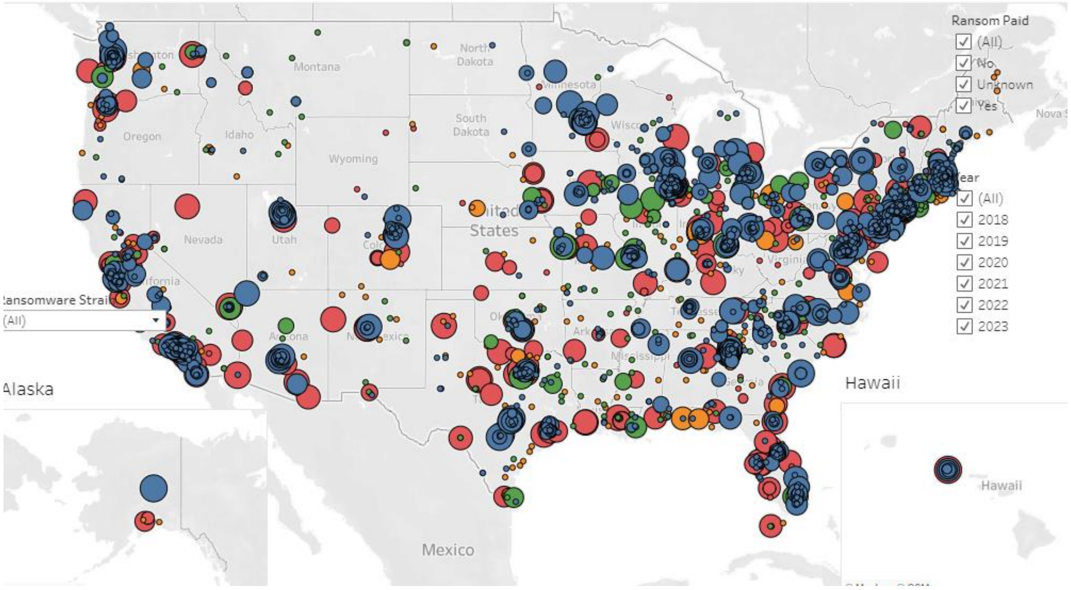


Figure 1. Heat map of US ransomware attacks since 2018
Credit: https://www.comparitech.com/ransomware-attack-map

Top ransomware attacks by payout

A ransom is not always paid out by organizations and there is not always a guarantee that data will be decrypted. In some cases, even after the ransom is paid, the data is not decrypted, or simply the decrypting key does not work as promised. The decrypting key may not work at all, or it may only work for certain file types. Malicious parties target larger organizations that depend on extensive operations, allowing the ransomware to have the greatest impact on the critical functioning of the company. The largest ransomware payouts, as of April 2023, are listed in the following table.

Table 1. Largest ransomware payouts

Company	Payout	Source
CNA Financial	$40 million	CNA Financial Paid Hackers $40 Million in Ransom After Cyberattack (businessinsider.com)
JBS	$11 million	JBS: Cyber-attack hits world's largest meat supplier - BBC News
CWT Global	$4.5 million	'Payment sent' - travel giant CWT pays $4.5 million ransom to cyber criminals | Reuters
Colonial Pipeline	$4.4 million	Colonial Pipeline reportedly paid $5M to hackers after ransomware attack - CNET
Brenntag	$4.4 million	Chemical distributor pays $4.4 million to DarkSide ransomware (bleepingcomputer.com)

Ransomware evolution

The impacts of ransomware vary based on the type of ransomware and the attack vectors. Ransomware has gained significant notoriety recently, as it has evolved with modern attack vectors.

Recent forms of ransomware are developed using a subscription model for Ransomware as a Service (RaaS). The ransomware developers allow attackers to use the RaaS tools that are ready to deploy, and the developers get a percentage of the ransom payout. The general availability of these ready to deploy tools creates an environment with more widespread attacks and new vectors. Each attacker uses a unique vector, creating more attack variations.

Given the RaaS model, malicious parties now have access to ransomware that is already tested and ready to deploy. The attacker is now decoupled from the ransomware developer, multiplying the number of attackers. Each attacker provides a novel approach to infecting clients using different vectors. The increase in vectors and approaches creates a challenging cybersecurity environment for organizations.

Ransomware lifecycle

A ransomware attack starts with an infection and ultimately leads to extorting capital from an organization based on the value of the business operations or the data. The following figure summarizes the four stages in the ransomware lifecycle.

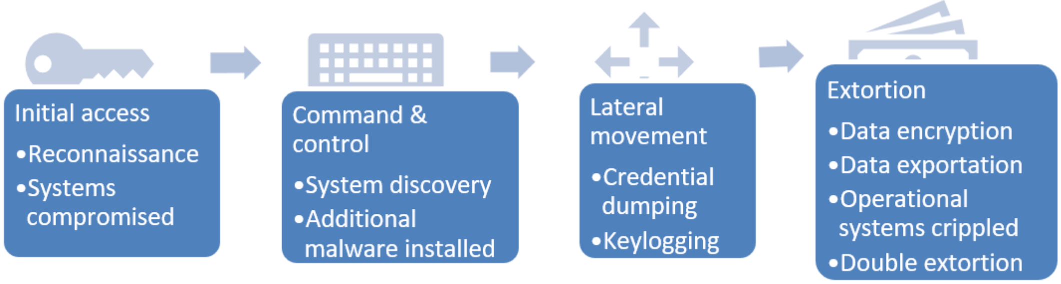


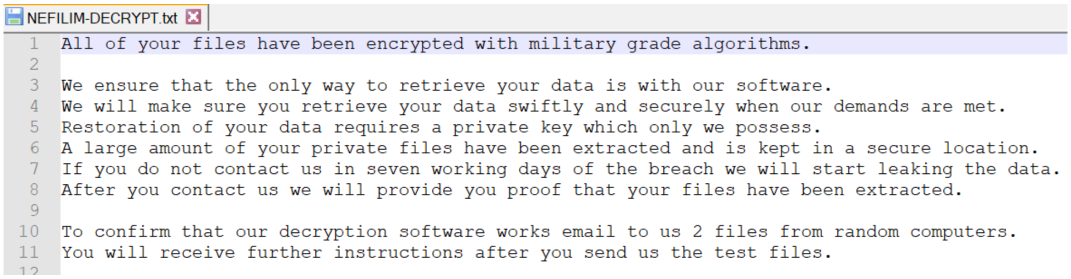
Figure 2. Ransomware lifecycle

During the Initial Access phase, the malicious parties gather information about the target network. The malicious parties look to exploit known vulnerabilities in software or devices on the target network. After a single system is compromised, the door is now open to spread the malware and begin the next phase.

In the Command & Control phase, the malicious party looks to collect detailed information about the target's network. The process includes understanding what data is valuable for the organization and what systems have the greatest dependencies. When the target systems are characterized, the malicious parties adapt the attack accordingly. Additional malware can be installed at this point.

After the target system's most valuable data and operations are identified, the next step is to thwart any potential system recovery. Gaining access to the most valuable data and systems requires credential access. The process of gaining access to these systems may be through credential dumping and keylogging.

The final phase is exfiltration and encryption of the organization's data. During this phase, any valuable data is encrypted and/or exported. If the ransomware party determines that the choke point of the target organization is daily operations, the operational systems are crippled. After the most valuable points are compromised, the ransomware party begins the demand process, as shown in the following figure. In modern ransomware attacks, malicious parties use double extortion, by not only encrypting data, but also by retaining a copy of the data offsite. The offsite data can be sold to the highest bidder or simply dumped online to damage the company's reputation.



```
All of your files have been encrypted with military grade algorithms.

We ensure that the only way to retrieve your data is with our software.
We will make sure you retrieve your data swiftly and securely when our demands are met.
Restoration of your data requires a private key which only we possess.
A large amount of your private files have been extracted and is kept in a secure location.
If you do not contact us in seven working days of the breach we will start leaking the data.
After you contact us we will provide you proof that your files have been extracted.

To confirm that our decryption software works email to us 2 files from random computers.
You will receive further instructions after you send us the test files.
```

Figure 3. Example ransomware note

PowerScale cyber protection solutions

Dell PowerScale offers two cyber protection solutions, PowerProtect Cyber Recovery, and the PowerScale Cyber Protection Suite.

PowerProtect Cyber Recovery

The Dell PowerProtect Cyber Recovery solution offers NAS protection for PowerStore, Dell Unity, PowerScale, and 3rd party NFS exports and SMB shares. The orchestration is controlled through the PowerProtect DD series appliance.

For more information about the PowerProtect solution, see:

- PowerProtect Data Manager for NAS overview | Dell PowerProtect Data Manager: Dynamic NAS Protection | Dell Technologies Info Hub
- Dell PowerProtect Cyber Recovery: Reference Architecture | Dell Technologies Info Hub.

PowerScale Cyber Protection Suite

Dell PowerScale offers a Cyber Protection Suite of advanced software to protect data throughout the lifecycle, as shown in the following figure. Considering the ransomware lifecycle, PowerScale's software suite ensures cyber protection at each phase, while also planning for a potential ransomware attack. Further, the Cyber Protection Suite does not require a full PowerScale backup. Administrators can select the data that is paramount for business continuity in the event of a ransomware attack. The PowerScale Cyber Protection Suite aligns with the cybersecurity framework defined by the National Institute of Standards and Technology (nist.gov).

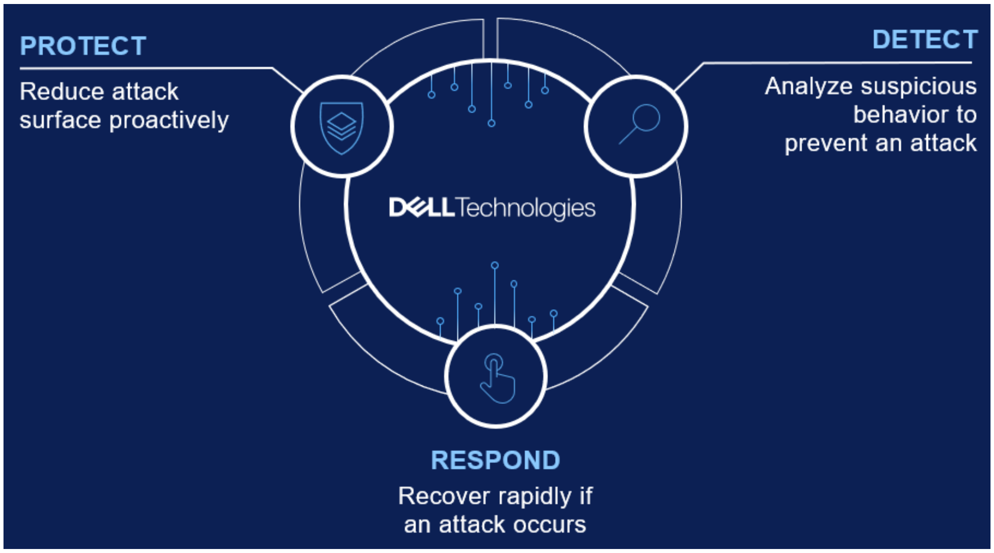

PROTECT
Reduce attack surface proactively
DETECT
Analyze suspicious behavior to prevent an attack
DELL Technologies
RESPOND
Recover rapidly if an attack occurs

Figure 4. PowerScale Cyber Protection Suite

PowerProtect Cyber Recovery vs PowerScale Cyber Protection Suite

The primary objective of the PowerProtect Cyber Recovery and the PowerScale Cyber Protection Suite differs in key areas. Although the primary focus of this paper is the PowerScale Cyber Protection Suite, it is important to understand the data protection impacts offered by each solution.

Full cluster vs business continuity dataset backup

The PowerProtect Cyber Recovery solution requires a full PowerScale cluster backup, which may be a time-consuming process depending on the overall cluster size. By contrast, the PowerScale Cyber Protection Suite does not require a full backup of the cluster, allowing administrators to define a business continuity dataset. The business continuity dataset is composed of specific directories, shares, exports, or snapshots. A smaller dataset, rather than a full cluster backup, also allows for quick recovery times, because only impacted datasets are restored.

Ransomware event interdiction

The PowerScale Cyber Protection Suite uses an audit trail, integration with 3rd party devices, and real-time monitoring for access anomalies to quickly disrupt a ransomware event. AI powered threat detection monitors the production clusters and sends alerts of any suspicious activity. The ransomware event interceptions include protection against data exfiltration early in the lifecycle, minimizing ransomware attack vectors and impacts.

Cyber Vault PowerScale cluster

The PowerScale Cyber Protection Suite offers replication of the business continuity datasets to a PowerScale cluster in a cyber vault. Because the cyber vault PowerScale cluster is a complete cluster, rather than a singular storage array, it offers all the options of a full PowerScale cluster. In the event of a ransomware attack, administrators have two options for restoring data:

- Copy the business continuity datasets from the cyber vault cluster to the production cluster
- Make the cyber vault PowerScale cluster the production cluster

Converting the cyber vault cluster to a production cluster offers minimal downtime rather than waiting for datasets to copy from the vault cluster to production cluster, providing a powerful last resort option.

Data exfiltration protection

If a ransomware attack occurs in which data is exfiltrated, administrators must restore data quickly to ensure minimal business impacts. Because the PowerProtect solution requires a full cluster backup, there is no option to selectively restore data. During the data exfiltration process, the malicious parties attempt to steal an organization's most sensitive data. If only some of the data has been exfiltrated, restoring an entire cluster is a time-consuming process. The Cyber Protection Suite allows administrators to restore only the datasets that were exfiltrated, minimizing down time.

Dell Professional Services for cyber planning and recovery

In addition to the PowerScale data protection solutions, Dell provides professional services for cyber planning and recovery. Dell Services enhances cyber resilience by bringing processes and technology together to form a holistic cyber recovery program to ensure that organizations are protected from cyber threats. The cyber planning and recovery service can be engaged at any time during the ransomware lifecycle. Engaging before an attack includes cyber planning. However, an incident response service is available to engage during or after a ransomware attack. For more information, see the Dell Response and Recovery datasheet at Incident Response and Recovery Data Sheet (delltechnologies.com).

PowerScale Cyber Protection Suite

The three core pillars of the PowerScale Cyber Protection Suite are based on Protect, Detect, and Respond:

- The Protect pillar reduces the attack surface proactively with built-in capabilities and automated environment hardening at the data storage layer.
- The Detect pillar analyzes suspicious behavior to prevent an attack from occurring and shares threat intelligence across the enterprise cybersecurity solution stack.
- The Respond pillar plans for the worst-case scenario, where a ransomware attack takes place, by providing the tools to respond and recover from an attack.

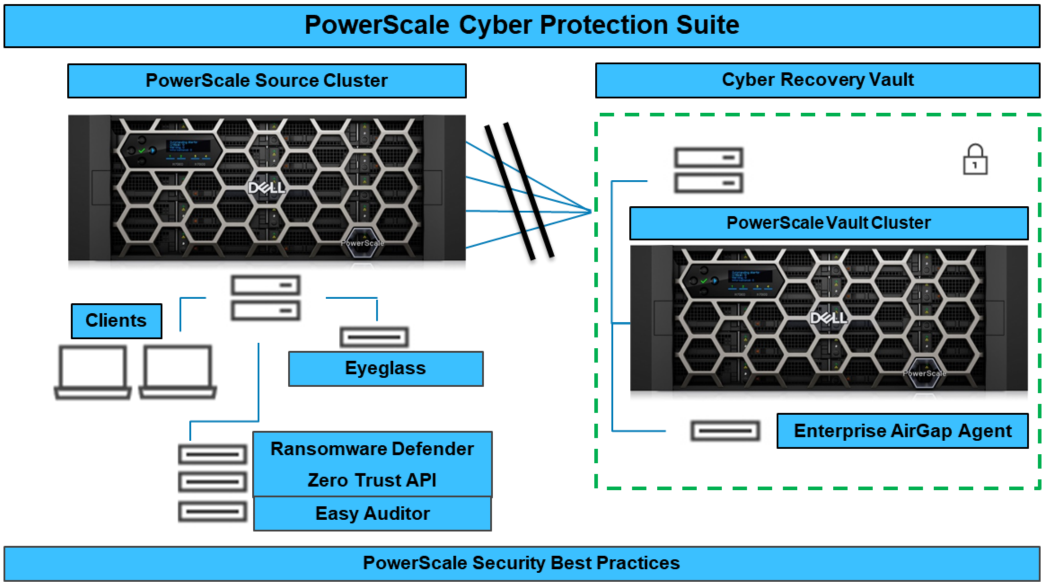


Figure 5. PowerScale Cyber Protection Suite

The PowerScale Cyber Protection Suite consists of modules that each perform a specific security function. When combined, the modules form a suite of advanced software to protect unstructured data from cyber threats.

Table 2. PowerScale Cyber Protection Suite

PowerScale Cyber Protection Suite	
Eyeglass	Management control plane for the Cyber Protection Suite
Ransomware Defender	Real-time user behavior detection to detect and halt a ransomware attack through user lockouts and trigger-based snapshots.
Zero Trust API	Enables Extended Detection and Response (XDR) and Security Information and Event Management (SIEM) telemetry sharing and collection across the data center.
Easy Auditor	Audits users and file activity to provide top active users, stale permissions, and login reports. Active auditing monitors mass deletes and bulk data copying.
Enterprise Airgap Agent	Manages replication of an offline business continuity dataset in an automated cyber vault
PowerScale Security Best Practices	

Eyeglass

Eyeglass serves as the management plane for the PowerScale Cyber Protection Suite. Administrators are provided a single pane of glass for managing the entire suite through Eyeglass as the launchpad for Ransomware Defender, Easy Auditor, and AirGap Enterprise. Event reporting, threat management, and policy configuration are all performed through Eyeglass.

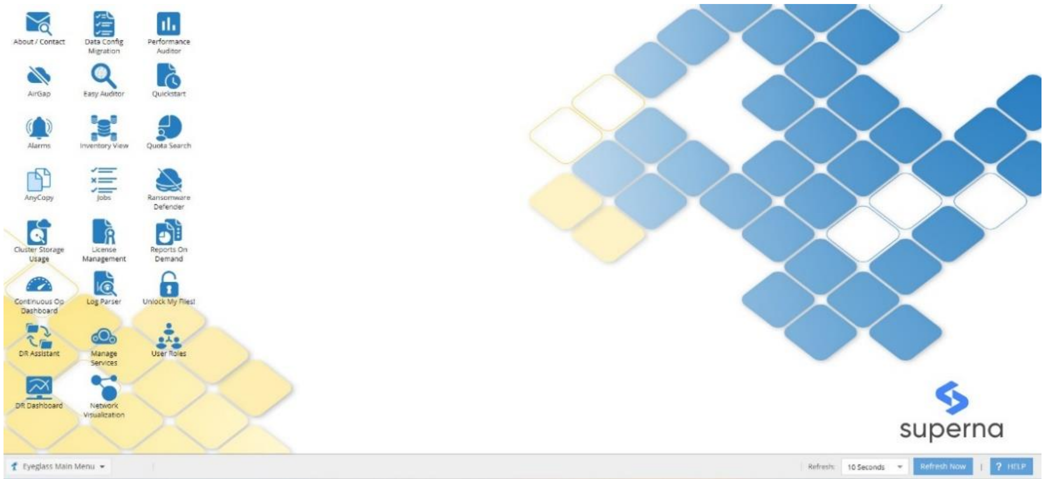


Figure 6. Eyeglass management console

Many administrators may already be familiar with Eyeglass because it is also used as the management plane for other Superna solutions.

PowerScale security configuration and considerations

Many of the concepts for cyber protection overlap with general PowerScale security best practices and considerations. These concepts are applicable to other security threats and have a broader envelope of protection. For information about PowerScale security considerations, see Dell PowerScale OneFS: Security Considerations | Dell Technologies Info Hub. For information about PowerScale security configuration controls and settings, see the *Security Configuration Guide* for the respective OneFS software release at PowerScale OneFS Info Hubs | Dell US.

Ransomware Defender

At the core of the PowerScale cybersecurity framework is Ransomware Defender. The solution combines scalability with real-time event processing to detect and stop ransomware attacks. Detecting changes to users' normal file system access patterns, Ransomware Defender can take defensive measures to prevent major damage and minimize recovery times when administrator-defined thresholds are met. If Ransomware Defender detects ransomware attack behavior, it initiates multiple defensive measures, including locking users from file shares, either immediately or over a period of time. Besides timed Auto Lockout rules, there is an automatic response escalation in case multiple infections are detected simultaneously, even if an administrator is not available. Further, the event triggers an automated snapshot creation upon initial detection for a ground-zero restore point.

User behavior detection is based on known consistent ransomware access patterns early in the attack lifecycle, as displayed in the following image. Historically, ransomware follows a specific pattern, as described in the section Ransomware lifecycle. Ransomware Defender monitors clusters for these specific events that are abnormal to typical user patterns. These include excessive encryption or movement of files that are not consistent with user behavior.

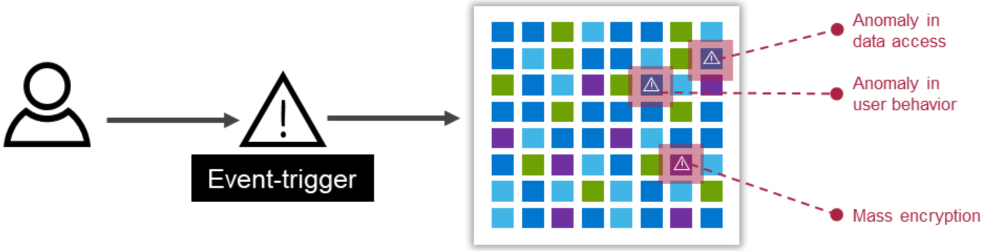
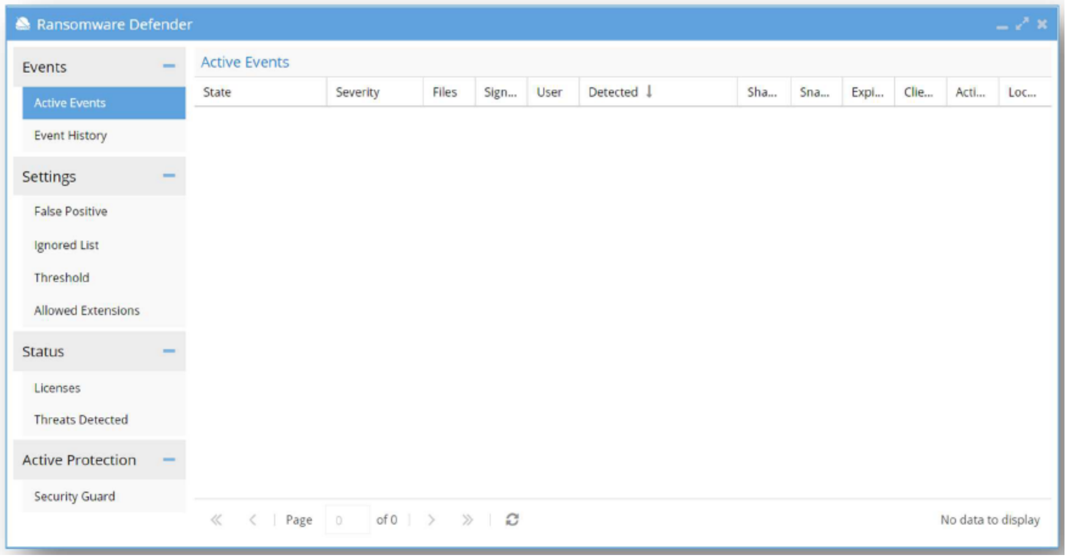


Figure 7. Ransomware Defender Event Triggers

Ransomware Defender is accessed through Eyeglass, as shown in the following figure. Alerts, configuration, and status are all managed through Eyeglass. Administrators may already be familiar with Eyeglass for its extensive data replication and failover capabilities.



Active Events

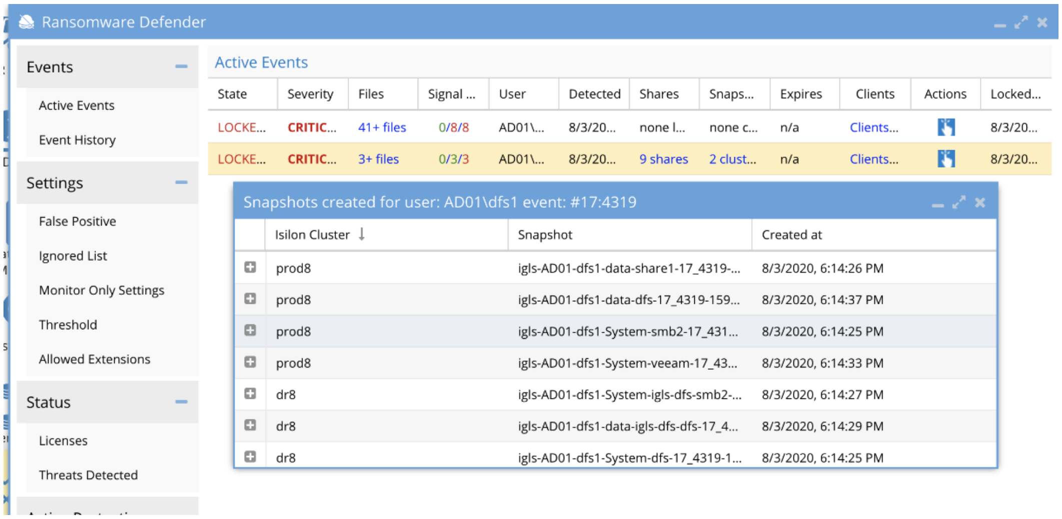
State	Severity	Files	Sign...	User	Detected	Sha...	Sna...	Expi...	Clie...	Acti...	Loc...

No data to display

Figure 8. Ransomware Defender

Ransomware Defender monitors PowerScale clusters constantly, for specific activity that indicates a ransomware attack, using a fully automated learning mode to monitor behavior and avoid false positives. Further refining the detection, protection can be customized for more sensitive data. When a ransomware event is detected, access from the infected user’s account to PowerScale is blocked. Ransomware Defender can manage multiple clusters, each with multiple shares. If ransomware activity is detected on one share in a cluster, the user loses access to all managed shares and clusters. As soon as ransomware activity has been detected and a user has been temporarily blocked, a notification is sent immediately to the administrator. Ransomware Defender only locks out the infected user, allowing other users to access the cluster. Because the security lockout is applied across the security stack, the locked-out user's other devices are also inaccessible.

When an active event occurs, Ransomware Defender displays the event state, severity, infected share, and other critical event information. In the following figure, a user is locked out and the associated snapshots are displayed.



Active Events

State	Severity	Files	Signal ...	User	Detected	Shares	Snaps...	Expires	Clients	Actions	Locked...
LOCKE...	CRITIC...	41+ files	0/8/8	AD01\...	8/3/20...	none l...	none c...	n/a	Clients...		8/3/20...
LOCKE...	CRITIC...	3+ files	0/3/3	AD01\...	8/3/20...	9 shares	2 clust...	n/a	Clients...		8/3/20...

Snapshots created for user: AD01\dfs1 event: #17:4319

Isilon Cluster ↓	Snapshot	Created at
prod8	igls-AD01-dfs1-data-share1-17_4319-...	8/3/2020, 6:14:26 PM
prod8	igls-AD01-dfs1-data-dfs-17_4319-159...	8/3/2020, 6:14:37 PM
prod8	igls-AD01-dfs1-System-smb2-17_431...	8/3/2020, 6:14:25 PM
prod8	igls-AD01-dfs1-System-veeam-17_43...	8/3/2020, 6:14:33 PM
dr8	igls-AD01-dfs1-System-igls-dfs-smb2-...	8/3/2020, 6:14:27 PM
dr8	igls-AD01-dfs1-data-igls-dfs-dfs-17_4...	8/3/2020, 6:14:29 PM
dr8	igls-AD01-dfs1-System-dfs-17_4319-1...	8/3/2020, 6:14:25 PM

Figure 9. Ransomware Defender locked out user event

If an active event is detected, Ransomware Defender's user behavior detection retains all associated security data, as shown in the following table.

Table 3. Active event security data

Active Event Data	Explanation
Actions	The history of all steps taken during the detection is listed with time stamps. All share lockout or snapshot creation tracking is logged. All future actions stay with the event history. If an event is archived, the history stays with the event in the "Event History" tab.
Client IP	The IP address of the user's PC that is infected.
File Event	A discrete event published by PowerScale's event stream based on a user action, for example: open file, close file, write or read to file.
Files	The list of files associated to the detection for the specified user.
Lock Out	The date and time of the security event
Ransomware Event	A collection of signals whose combined Signal Strengths exceeds the user-set threshold in Eyeglass.
Shares	List of shares that were locked out
Signal	Occurrence of one or more File Events that have been flagged by one or more threat detectors as a potential Ransomware Event.
Signal Strength	For a given Signal, the number of threat detectors that were triggered. A higher Signal Strength has a higher probability of being a Ransomware Event.
Snapshots	List of snapshots of SMB share paths taken during the lockout
Threat Detectors	Logic used by Eyeglass Ransomware Defender to determine if a group of File Events is potentially associated with a Ransomware attack. There are multiple independent threat detectors used by Eyeglass Ransomware Defender during analysis that are assessed in parallel.
User	The user or NFS IP of the locked-out account

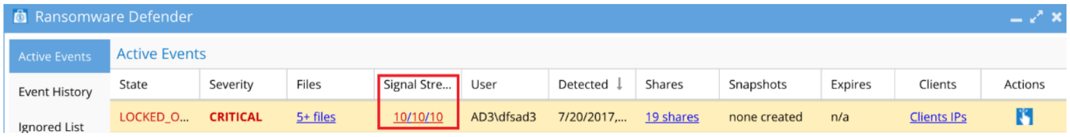
Ransomware events are based on signal strength thresholds. The threat level and associated action are listed in the following table.

Table 4. Ransomware Defender signal strength threshold

Threat Level	Ransomware Defender Action
Warning	Eyeglass sends an email to notify any subscribed administrator(s) of the threat but takes no direct action.
Major	Eyeglass begins a “delayed lockout” procedure. Notify the administrator(s) that a threat has been detected, and the user will be locked out after X minutes, unless the admin logs in and explicitly cancels the action. The grace period is configurable in Eyeglass settings.
Critical	The user lockout is immediate, and the administrator(s) are notified.

Administrators configure the threshold for detected ransomware events with an associated signal strength, interval, grace period, and an option to escalate the alerts based on the occurrence of events.

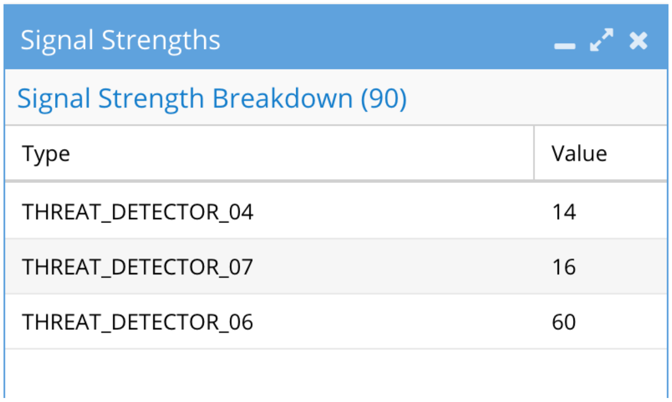
The threat detection Signal Strength measures the severity of a user's File Event behavior. A higher count indicates a more severe detection. A **Signal Strength** column can be found in the **Active Events** or **Event History** tab of the Eyeglass Ransomware Defender window, as highlighted in the following figure.



State	Severity	Files	Signal Stre...	User	Detected ↓	Shares	Snapshots	Expires	Clients	Actions
LOCKED_O...	CRITICAL	5+ files	10/10/10	AD3\dfsad3	7/20/2017,...	19 shares	none created	n/a	Clients IPs	

Figure 10. Active Events Signal Strength

Further, the signal strengths are based on specific threat detectors that contributed to the event, as displayed in the following figure.



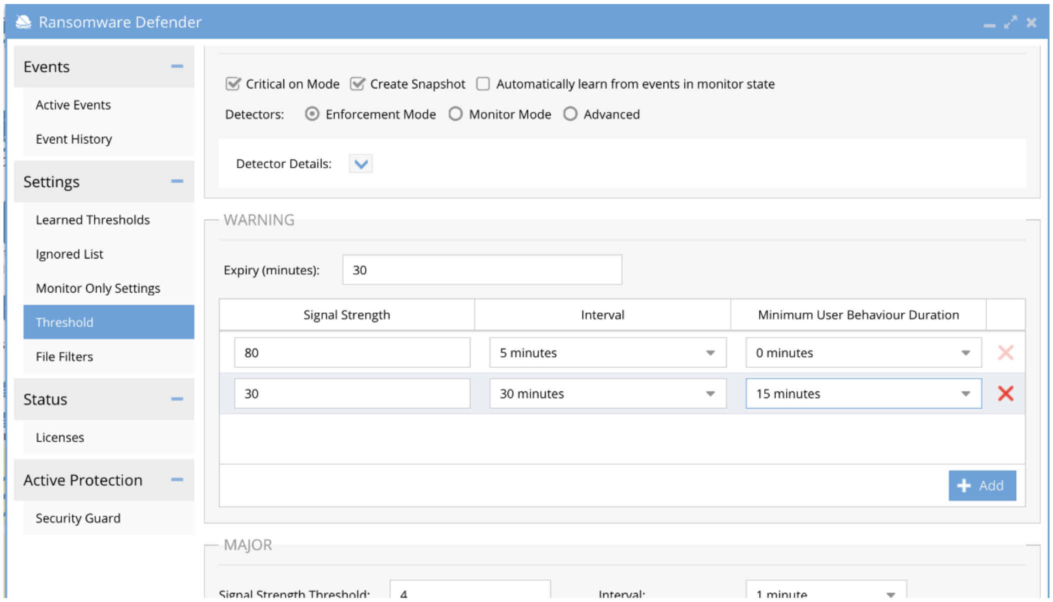
Signal Strength Breakdown (90)

Type	Value
THREAT_DETECTOR_04	14
THREAT_DETECTOR_07	16
THREAT_DETECTOR_06	60

Figure 11. Signal strength threat detectors

Note: The threat detectors are not documented for enhanced security and are for support only.

The **Threshold** menu also includes an option to **Automatically learn from events in monitor state** allowing administrators to use events for learning the normal access patterns. When a threshold is reached, administrators can take a snapshot and/or mark the event as **Critical on Mode**. The **Critical on Mode** option disables the automatic lockout feature for critical events and applies a major event delayed lockout. Furthermore, for each of the threshold levels, an event can be associated across multiple vectors, based on a combination of signal strength, interval, and duration, as shown in the following figure. The multiple vectors allow administrators to define varying combinations that could be indicative of an attack.



☑ Critical on Mode ☑ Create Snapshot ☐ Automatically learn from events in monitor state

Detectors: ● Enforcement Mode ○ Monitor Mode ○ Advanced

Detector Details:

WARNING

Expiry (minutes): 30

Signal Strength	Interval	Minimum User Behaviour Duration
80	5 minutes	0 minutes
30	30 minutes	15 minutes

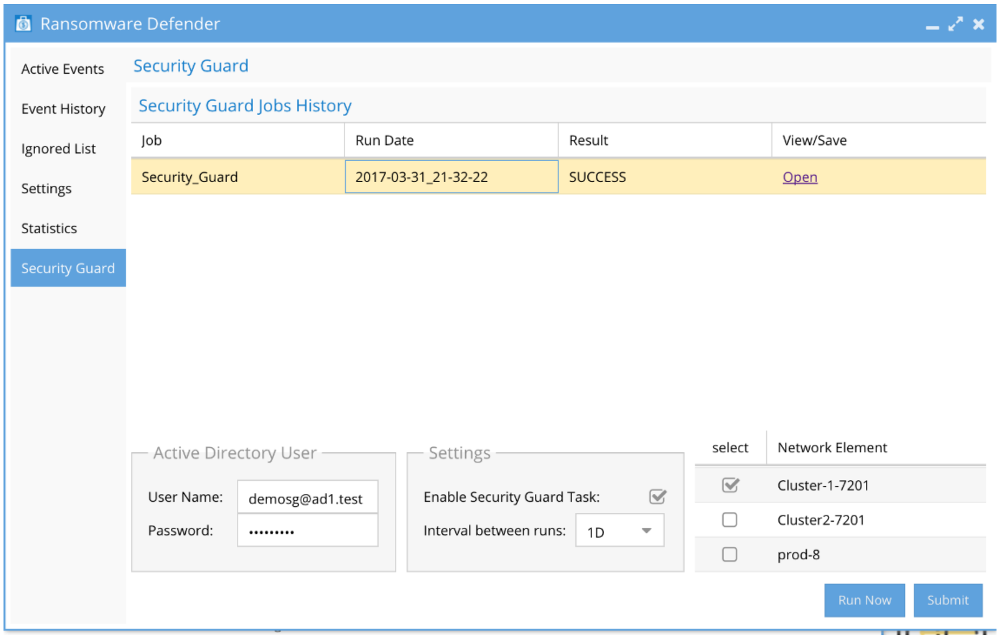
MAJOR

Signal Strength Threshold: 4 Interval: 1 minute

Figure 12. Ransomware Defender threshold options

Security guard

A critical part of security best practices is ensuring threat detection systems are active and ready. Ransomware Defender includes a “Security Guard” feature, which simulates a ransomware attack to validate all components are functioning, including alerting and lockout of user sessions. The feature can simulate an attack on demand or on a scheduled interval that may be required by regulatory security requirements. During the simulation, administrators are notified through the defined event thresholds, and a detailed log is available after the attack. The simulated attack includes options define the Active Directory user and specify a single or multiple clusters, as displayed in the following figure. Further customizing the attack, an option is also available for a custom file extension.



Security Guard

Security Guard Jobs History

Job	Run Date	Result	View/Save
Security_Guard	2017-03-31_21-32-22	SUCCESS	Open

Active Directory User

User Name: demosg@ad1.test

Password: •••••••••

Settings

Enable Security Guard Task: ☑

Interval between runs: 1D

select	Network Element
☑	Cluster-1-7201
□	Cluster2-7201
□	prod-8

Figure 13. Security Guard

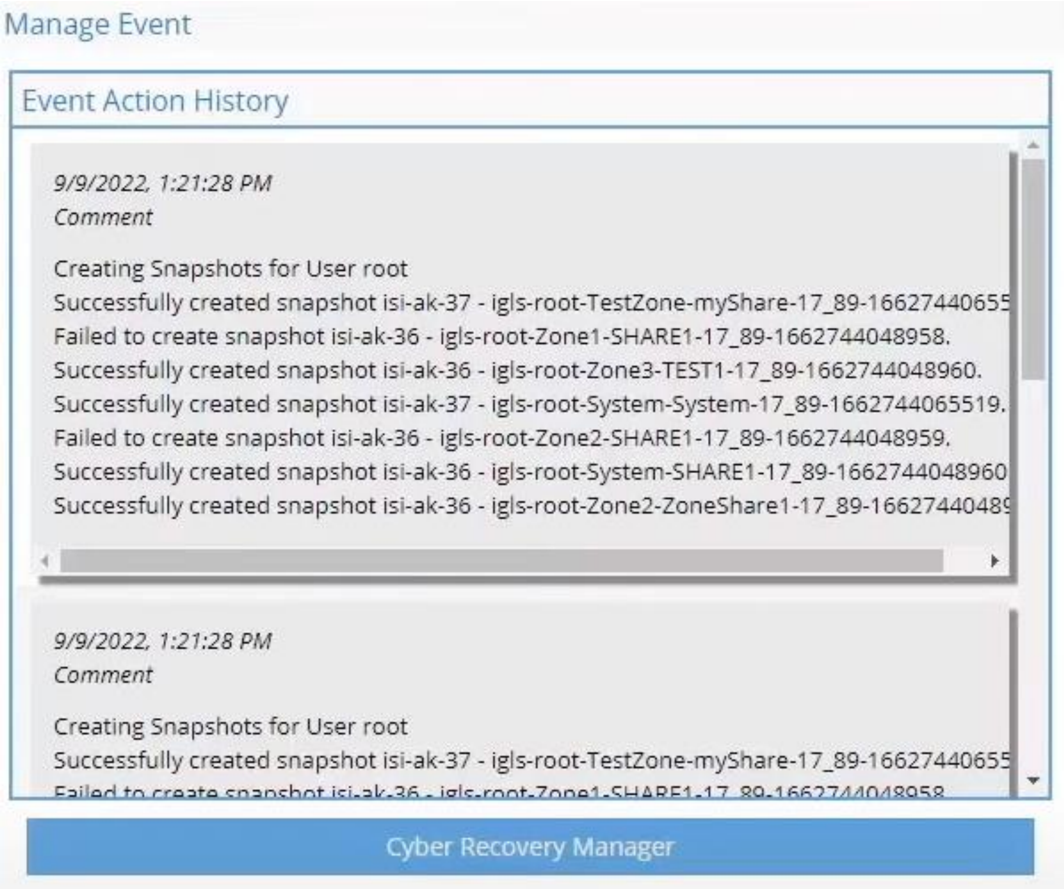
Honeypot tripwire

Honeypots are an important part of vulnerability management. It is essentially a “fake” share or file that mimics the original. The goal is that the hacker attacks the fake honeypot instead of the actual data, allowing the system to lock the user out early in the attack. Typically, a honeypot is used where sensitive data exists and allows for faster detection times at these locations in the file system. Ransomware Defender allows honeypots in as many locations as needed.

Cyber Recovery Manager

Ransomware Defender contains a Cyber Recovery Manager that automates data recovery using a OneFS snapshot after a ransomware attack. Based on information from audit events, Ransomware Defender is aware of the time an attack took place. Using this timestamp, the Cyber Recovery Manager, can then list the available snapshots to restore before the attack took place.

In the Ransomware Defender module, the event history information contains an “Action” option where the Cyber Recovery Manager option is available, as displayed in the following image.



Manage Event

Event Action History

9/9/2022, 1:21:28 PM
Comment

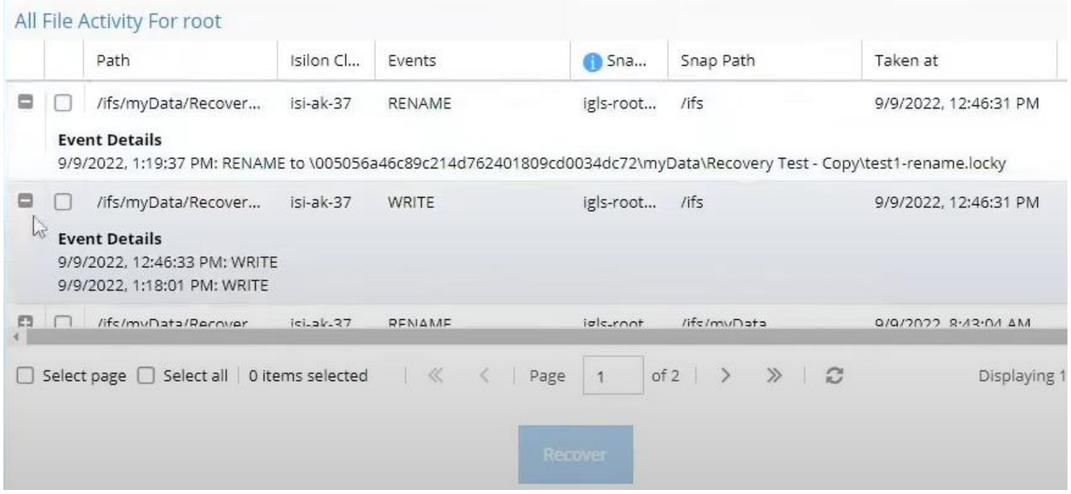
Creating Snapshots for User root
Successfully created snapshot isi-ak-37 - igls-root-TestZone-myShare-17_89-16627440655
Failed to create snapshot isi-ak-36 - igls-root-Zone1-SHARE1-17_89-1662744048958.
Successfully created snapshot isi-ak-36 - igls-root-Zone3-TEST1-17_89-1662744048960.
Successfully created snapshot isi-ak-37 - igls-root-System-System-17_89-1662744065519.
Failed to create snapshot isi-ak-36 - igls-root-Zone2-SHARE1-17_89-1662744048959.
Successfully created snapshot isi-ak-36 - igls-root-System-SHARE1-17_89-1662744048960
Successfully created snapshot isi-ak-36 - igls-root-Zone2-ZoneShare1-17_89-16627440489

9/9/2022, 1:21:28 PM
Comment

Creating Snapshots for User root
Successfully created snapshot isi-ak-37 - igls-root-TestZone-myShare-17_89-16627440655
Failed to create snapshot isi-ak-36 - igls-root-Zone1-SHARE1-17_89-1662744048958

Figure 14. Cyber Recovery Manager

Clicking the **Cyber Recovery Manager** option lists the files that have been compromised from a ransomware attack. The following figure shows the last known snapshots associated with the compromised files. Simply select the snapshot and click **Recover**.



All File Activity For root

		Path	Isilon Cl...	Events	Sna...	Snap Path	Taken at
⊟	□	/ifs/myData/Recover...	isi-ak-37	RENAME	igls-root...	/ifs	9/9/2022, 12:46:31 PM
		Event Details 9/9/2022, 1:19:37 PM: RENAME to \005056a46c89c214d762401809cd0034dc72\myData\Recovery Test - Copy\test1-rename.locky					
⊟	□	/ifs/myData/Recover...	isi-ak-37	WRITE	igls-root...	/ifs	9/9/2022, 12:46:31 PM
		Event Details 9/9/2022, 12:46:33 PM: WRITE 9/9/2022, 1:18:01 PM: WRITE					
⊞	□	/ifs/myData/Recover...	isi-ak-37	RENAME	igls-root...	/ifs/myData	9/9/2022, 8:43:04 AM

□ Select page □ Select all | 0 items selected | « ‹ | Page 1 of 2 | › » | Displaying 1

Figure 15. Cyber Recovery Manager file recovery

Because cyber incidents require a post-mortem analysis, the Cyber Recovery Manager assists in the analysis. An automated quarantine feature moves impacted files to a hidden location for inspection in the future. The quarantine also removes file visibility from users.

Zero Trust API

The Zero Trust API is an add-on component to Ransomware Defender and enables integration with third party SIEMs and XDRs. A Security Information and Event Management System, or SIEM, facilitates the identifying and addressing of potential vulnerabilities and threats before they disrupt a company's operations. Using SIEM technology, event log data is collected from different sources, analyzed in real-time, and action is taken by Ransomware Defender if abnormal behavior is spotted. Depending on the security stack implementation a SIEM may be sharing data with an XDR. However, the security stack implementation varies according to the environment.

An Extended Detection and Response (XDR) solution gathers and correlates data across multiple layers of security, including email, endpoint, server, cloud workload, and network. An XDR also collects data from other security systems, such as Endpoint Detection and Response (EDR), Network Detection and Response (NDR), SIEM, and other threat related data. Alternatively, some security implementations might have the EDR and NDR sharing data with the SIEM.

The Zero Trust API allows integration with XDRs and SIEMs, integrating with an organization’s security stack and further protecting PowerScale clusters. As a result, you can detect threats sooner, conduct investigations more quickly, and improve response times through security analysis. The integration provides a cohesive security approach across the corporate network by linking storage, network, endpoints, servers, and email domains using a bi-directional API, bridging the security intelligence gap at the storage domain.

Through the bi-directional API security event analysis spans across detection vectors through the data, application, and network layers, as displayed in the following figure. This allows the security system to identify suspicious activity quickly, because it can draw on data from multiple sources to identify potential threats. As a result, it can detect malicious activity earlier and take action to prevent it from escalating through the data center layers. For example, if a threat is detected from the security stack, this can be configured to trigger a user lockout across monitored PowerScale clusters and a SnapshotIQ snapshot.

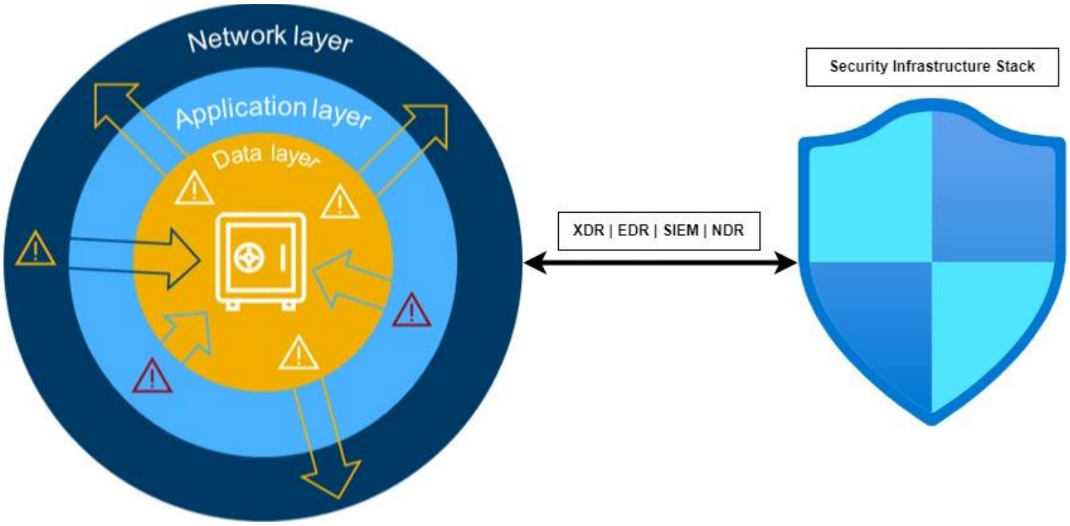


Figure 16. Zero Trust API

The Security Infrastructure Stack now correlates data across domains and through the layers, allowing Ransomware Defender to monitor current threat levels. Application Server threats trigger an API call for OneFS to create immutable SnapshotIQ snapshots of critical data. Compromised user threats trigger an access denial to PowerScale storage with AD & SMB share aware lockouts. Further, SyncIQ replication to the PowerScale Vault Cluster is blocked until the active threat is cleared.

Progress Flowmon ADS

A typical Enterprise Security Infrastructure Stack collects and analyzes threat data across all devices, endpoints, and network infrastructure. Network Detection and Response (NDR) is a critical part of the stack to detect suspicious network activity and unknown threats early in the attack lifecycle. NDRs monitor and analyze network traffic, alerting of suspicious network traffic patterns that deviate from a baseline or expected characteristics.

Other components of network security monitoring are an Intrusion Detection System (IDS) and Threat Intelligence feeds (TI). IDS is a passive monitoring system, that detects known threats using a database of signatures. Altogether, NDR and IDS secure network infrastructure and the alerts allow security administrators to respond to an attack before it reaches a PowerScale cluster.

The Progress Flowmon Anomaly Detection System (ADS) detects anomalies in network traffic to expose malicious behavior and indicators of compromise through NDR, IDS, TI, and other detection methods. Flowmon ADS shares the network status with Ransomware Defender through the bi-directional Zero Trust API. If a network anomaly occurs, Flowmon ADS notifies Ransomware Defender, triggering a OneFS snapshot and stopping replication to the Cyber Recovery Vault, as illustrated in the figure below.

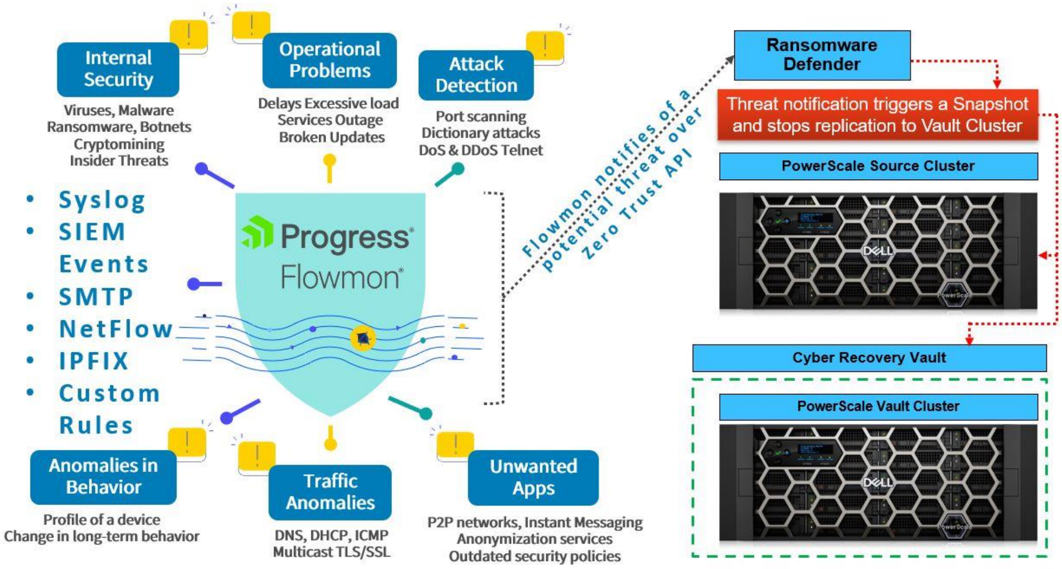
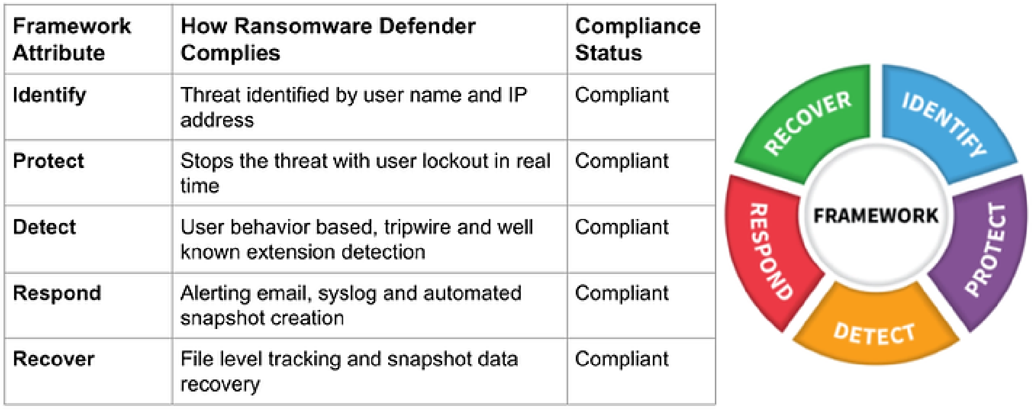


Figure 17. Flowmon ADS event flow with Ransomware Defender

Threats are detected through Flowmon's end-to-end network security, including Network Performance Monitoring and Diagnostics (NPMD) and Application Performance Monitoring (APM). Further, Flowmon assists with meeting the regulation requirements for the NIS2 cybersecurity directive. For more information on the Progress Flowmon integration with the Zero Trust API, see the Progress Flowmon and Zero Trust API Datasheet.

AirGap Enterprise

The AirGap Enterprise module add-on to Ransomware Defender retains an offline copy of a dataset in an automated cyber vault. The offline dataset copy is logically segmented from the production network, providing two critical advantages. First, the dataset is stored in a secure offline vault, protecting it from enterprise network threats. A second advantage is planning for a ransomware attack that cripples business operations. By using an offline dataset, you can quickly restore operations to the point in time when the last copy of the dataset was made, thus minimizing the impact and damage associated with the ransomware attack as a whole. Further, if a dataset is readily available to restore, payment of the ransom is not a consideration, potentially saving millions of dollars. The AirGap cyber vault also complies with the NIST cybersecurity framework best practices.

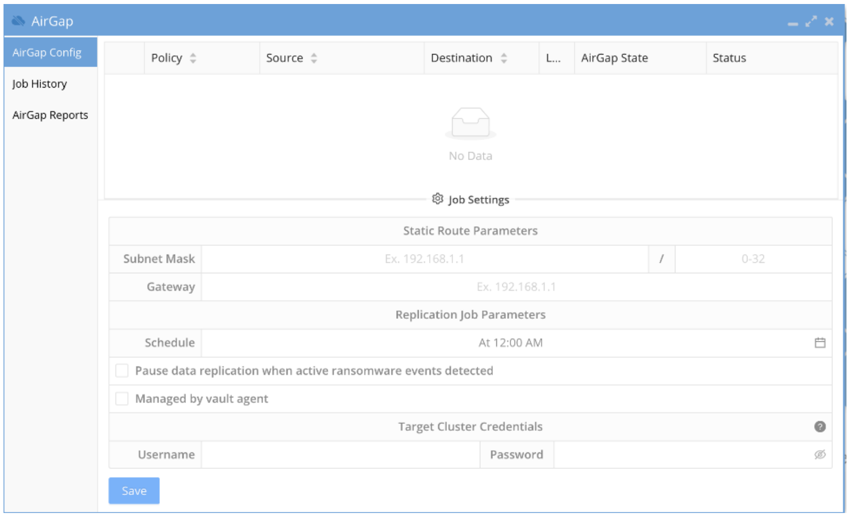


Framework Attribute	How Ransomware Defender Complies	Compliance Status
Identify	Threat identified by user name and IP address	Compliant
Protect	Stops the threat with user lockout in real time	Compliant
Detect	User behavior based, tripwire and well known extension detection	Compliant
Respond	Alerting email, syslog and automated snapshot creation	Compliant
Recover	File level tracking and snapshot data recovery	Compliant

Figure 18. Ransomware Defender compliance with NIST cybersecurity framework

As part of the inside-the-vault hardened solution, full automation and in-band management allow access through a virtual machine within the cyber vault. The Smart Airgap technology ensures that data is only replicated when it is safe to do so. Further, the airgap mode provides a low-cost, fully automated solution. Optionally, a physical fiber cutter and firewall are available for the cyber vault.

Similar to the other modules in the PowerScale Cyber Protection Suite, you can access and manage the AirGap Agent through Eyeglass, as shown in the following figure.



Policy	Source	Destination	L...	AirGap State	Status

No Data

Job Settings

Static Route Parameters

Subnet Mask	Ex. 192.168.1.1	/	0-32
Gateway	Ex. 192.168.1.1		

Replication Job Parameters

Schedule	At 12:00 AM

□ Pause data replication when active ransomware events detected

□ Managed by vault agent

Target Cluster Credentials

Username		Password	

Figure 19. AirGap configuration

By only allowing data replication after a security clearance has been granted, the Cyber Recovery Vault is completely protected from unauthorized access. Note that under normal operating conditions, the PowerScale Vault Cluster does not have network access outside of the Cyber Recovery Vault and stores the business continuity dataset. The Enterprise AirGap Agent performs data and security checks periodically, at a frequency defined by an administrator. If a security clearance is granted, the Enterprise AirGap Agent replicates only the changed data blocks to the PowerScale vault cluster's business continuity dataset.

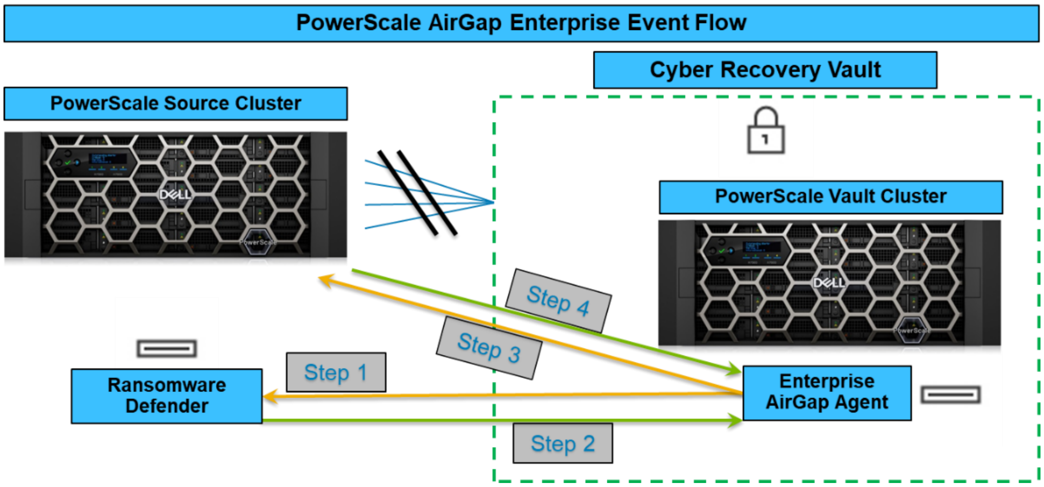


Figure 20. PowerScale AirGap Enterprise Event Flow

The AirGap Enterprise module runs through the following logical flow of steps, corresponding to the steps in Figure 20, to perform a security check and replicate changed data blocks:

1. At an administrator-specified frequency, the Enterprise AirGap agent adds network interfaces to query the Ransomware Defender agent outside the vault, for any active ransomware events. If active ransomware events are found, the process stops here, and the Enterprise AirGap agent removes the network interfaces, securing the Cyber Recovery Vault.

2. If no active ransomware events are detected, Ransomware Defender grants a security clearance to the Enterprise AirGap agent to proceed.
3. The Enterprise AirGap agent then queries the PowerScale source cluster to start replication to the PowerScale vault cluster. The PowerScale source cluster checks for updates to the business continuity dataset. If the PowerScale source cluster reports no changes to the business continuity dataset, the process stops here and the Enterprise AirGap Agent removes the network interfaces, securing the Cyber Recovery Vault.
4. If the PowerScale source cluster reports updates to the business continuity dataset, data replication may commence, only copying the changed data blocks. The Enterprise AirGap agent monitors the replication process.
5. Finally, when the replication is complete, the Enterprise AirGap Agent removes the network interfaces, securing the Cyber Recovery Vault. In the future, the process starts again at Step 1, based on the configured frequency.

Easy Auditor

Easy Auditor protects and secures PowerScale clusters by simplifying auditing operations for compliance, security, and other daily checks. Through real-time auditing capabilities, proactive data protection can be achieved by automating responses to security events using SnapshotIQ snapshots and enabling real-time locking out of user data access. With support for billions of audit records, Easy Auditor scales to clusters of any size. The PowerScale Cyber Protection Suite uses Easy Auditor for security features that complement the other modules in the suite, enhancing the overall suite's security posture. Audit and security data is shared with Ransomware Defender for analysis and actionable threats.

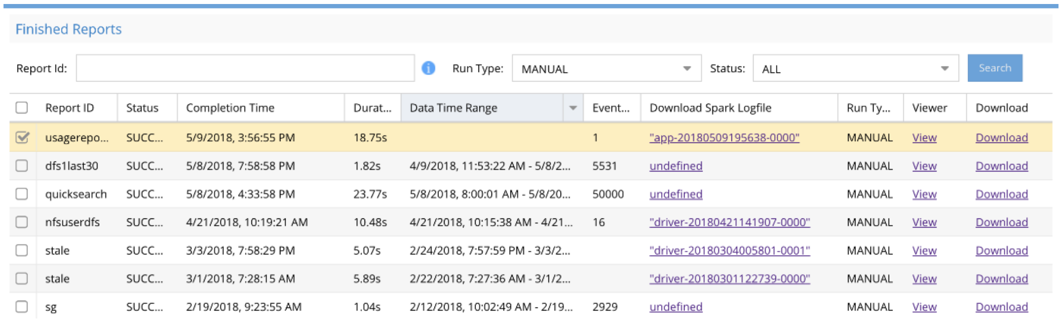
Similar to Ransomware Defender, Easy Auditor is also accessed through Eyeglass. Alerts, configuration, and status are all managed through Eyeglass.

Easy Auditor provides default reports and customizable reports to meet all auditing and security requirements. The default reports can be refined to meet regulatory or security requirements. The default reports include the following:

- Stale User Access Report: This report is used to determine which users might not require access to SMB shares based on access patterns. This is a security report that can be shared with departments that manage SMB share access. The report lists users that have accessed data using SMB shares and calculates the last read or write of each share the user has access to, based on AD group membership. The report also lists users that can mount shares and whether users have accessed data during the reporting time period.
- Access User Report: The report maps user to share access, detecting users with excessive permissions and confirming existing share access that may not align with security policies. The report generates a list of shares and a list of Active Directory (AD) users and groups that have access to a SMB share. The AD groups can be expanded to a list of users for administrators that do not have access to AD. Typically, this report is used to determine which users may not require access to SMB shares, based AD group membership. This is a security report that can be shared with departments that manage SMB share access.
- Login Monitor Report: This is a compliance report that satisfies HIPAA and PCI Requirements to track login to systems that store compliance data.

- Employee Exit Report: This report would be run prior to an employee leaving an organization and provides a view of all files the user accessed in any way over the last 30 days. The report is typically part of an HR process, displaying user activity by day over the last 30 days.

Reports are sent through email on a specified frequency and are available to view at any time in the “Finished Reports” tab, as shown in the following figure.



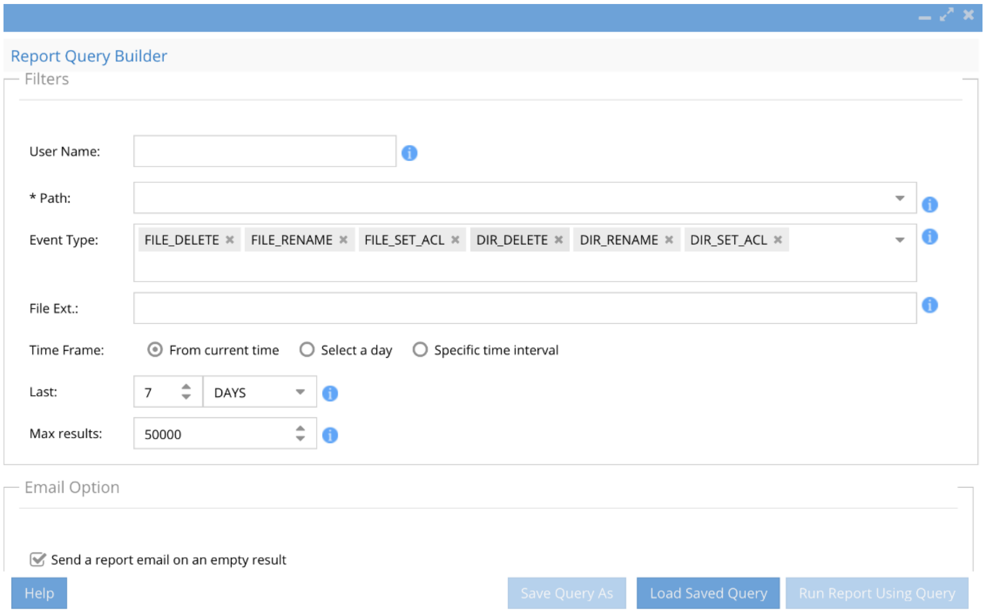
Finished Reports

Report Id: ____ Run Type: MANUAL Status: ALL

□	Report ID	Status	Completion Time	Durat...	Data Time Range	Event...	Download Spark Logfile	Run Ty...	Viewer	Download
☑	usagerepo...	SUCC...	5/9/2018, 3:56:55 PM	18.75s		1	"app-20180509195638-0000"	MANUAL	View	Download
□	dfs1last30	SUCC...	5/8/2018, 7:58:58 PM	1.82s	4/9/2018, 11:53:22 AM - 5/8/2...	5531	undefined	MANUAL	View	Download
□	quicksearch	SUCC...	5/8/2018, 4:33:58 PM	23.77s	5/8/2018, 8:00:01 AM - 5/8/20...	50000	undefined	MANUAL	View	Download
□	nfsuserdfs	SUCC...	4/21/2018, 10:19:21 AM	10.48s	4/21/2018, 10:15:38 AM - 4/21...	16	"driver-20180421141907-0000"	MANUAL	View	Download
□	stale	SUCC...	3/3/2018, 7:58:29 PM	5.07s	2/24/2018, 7:57:59 PM - 3/3/2...		"driver-20180304005801-0001"	MANUAL	View	Download
□	stale	SUCC...	3/1/2018, 7:28:15 AM	5.89s	2/22/2018, 7:27:36 AM - 3/1/2...		"driver-20180301122739-0000"	MANUAL	View	Download
□	sg	SUCC...	2/19/2018, 9:23:55 AM	1.04s	2/12/2018, 10:02:49 AM - 2/19...	2929	undefined	MANUAL	View	Download

Figure 21. Finished Reports

The customizable reports are based on user, paths, files extension, file action, and a date range as shown in the following figure.



Report Query Builder

Filters

User Name:

* Path:

Event Type: FILE_DELETE ✕ FILE_RENAME ✕ FILE_SET_ACL ✕ DIR_DELETE ✕ DIR_RENAME ✕ DIR_SET_ACL ✕

File Ext.:

Time Frame: ● From current time ○ Select a day ○ Specific time interval

Last: 7 DAYS

Max results: 50000

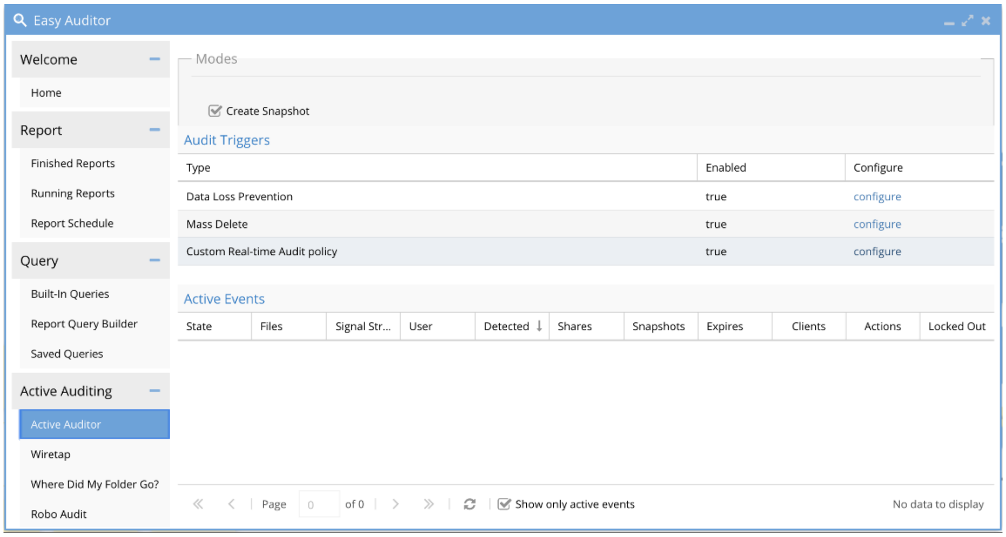
Email Option

☑ Send a report email on an empty result

Figure 22. Report Query Builder

Active Auditor

Rather than simply reporting threats to administrators and creating additional workload for administrators to read through lengthy reports, Active Auditor automates security through real-time audit triggers. For example, if two associated event triggers occur, send an alert. The triggers are fully customizable policies based on user, path, file extension, source IP address and more, to detect any condition in real time. The Active Auditor configuration window is shown in the following figure.



Modes

☑ Create Snapshot

Audit Triggers

Type	Enabled	Configure
Data Loss Prevention	true	configure
Mass Delete	true	configure
Custom Real-time Audit policy	true	configure

Active Events

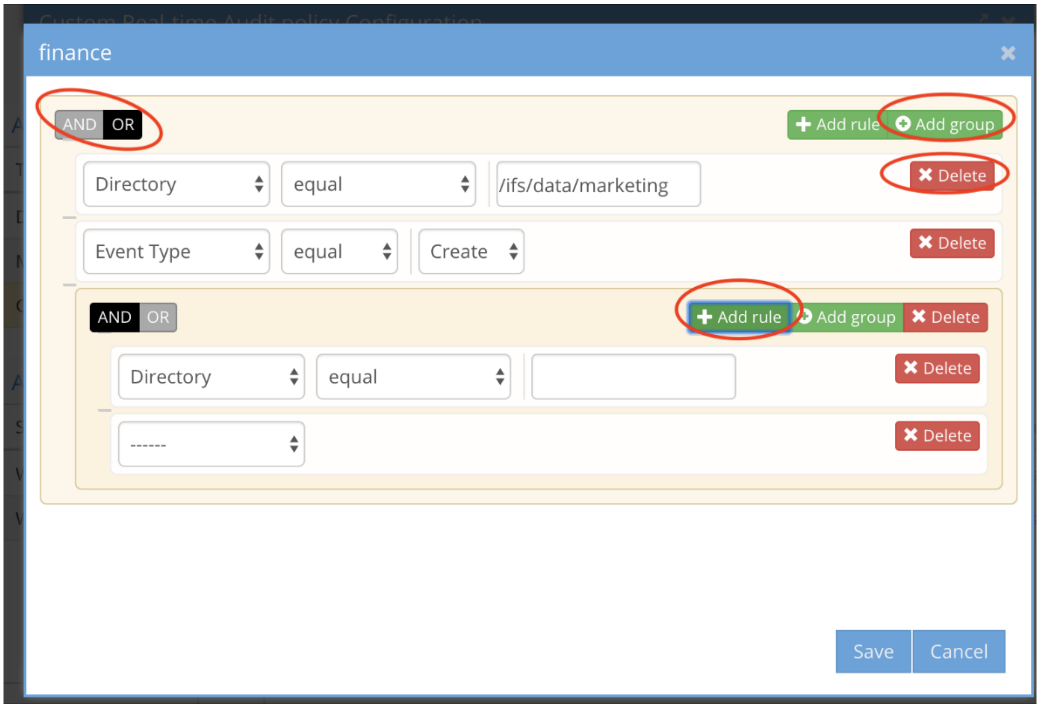
State	Files	Signal Str...	User	Detected ↓	Shares	Snapshots	Expires	Clients	Actions	Locked Out

☑ Show only active events

No data to display

Figure 23. Active Auditor configuration

The real-time auditing triggers include a fully customizable set of and/or rules, allowing administrators to configure extremely granular triggers, as shown in the following figure.



AND OR

Directory | equal | /ifs/data/marketing

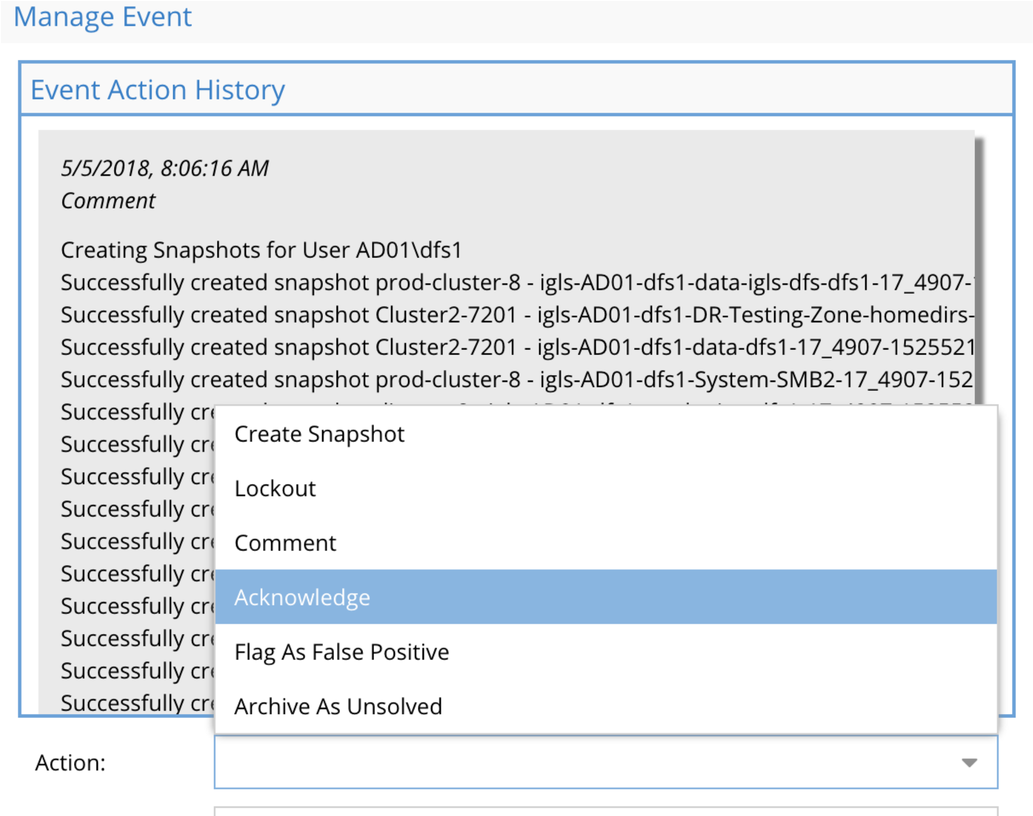
Event Type | equal | Create

AND OR

Directory | equal |

Figure 24. Granular real-time auditing triggers

When an active event occurs with Active Auditor, administrators are provided a detailed log of the event and are provided a set of actions to select, as shown in the following figure.



5/5/2018, 8:06:16 AM
Comment

Creating Snapshots for User AD01\dfs1
Successfully created snapshot prod-cluster-8 - igls-AD01-dfs1-data-igls-dfs-dfs1-17_4907-
Successfully created snapshot Cluster2-7201 - igls-AD01-dfs1-DR-Testing-Zone-homedirs-
Successfully created snapshot Cluster2-7201 - igls-AD01-dfs1-data-dfs1-17_4907-1525521
Successfully created snapshot prod-cluster-8 - igls-AD01-dfs1-System-SMB2-17_4907-152
Successfully cr
Successfully cr
Successfully cr
Successfully cr
Successfully cr
Successfully cr
Successfully cr
Successfully cr
Successfully cr
Successfully cr

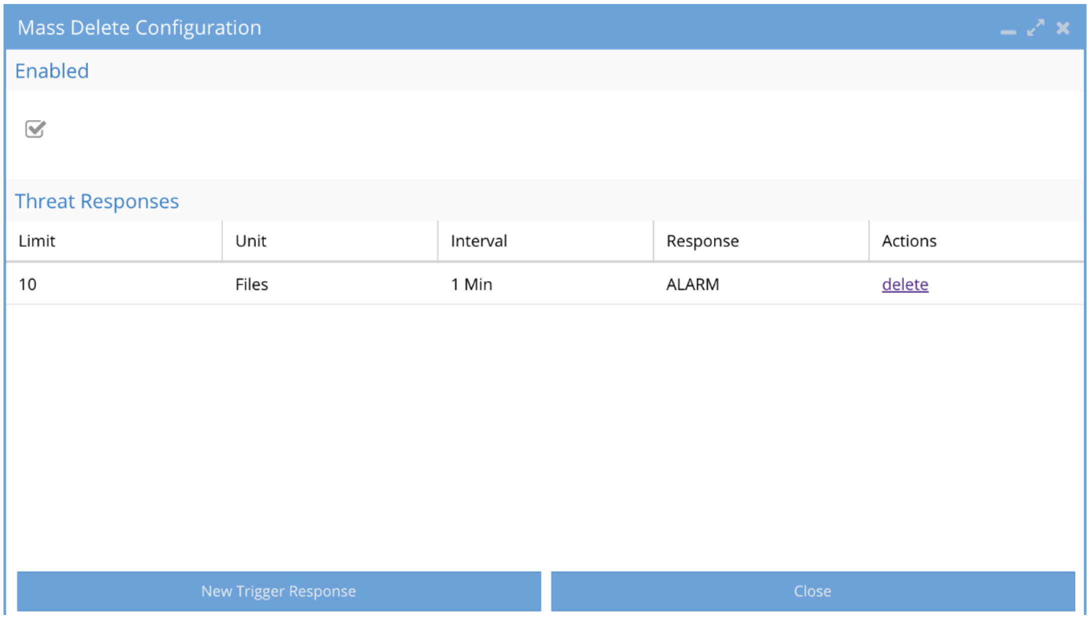
Figure 25. Event Action History

Honeypot

Active Auditor can be configured for honeypot detection, to detect an insider threat looking for open shares to read data. The trigger is configured to activate any time the honeypot directory is accessed.

Mass delete protection

Active Auditor's mass delete protection feature monitors users who delete files on any share or export up to a threshold defined by an administrator over a specified period of time. Real-time detectors count deletions made by a user and raise alerts when policies are violated. A built-in protection option takes a snapshot of SMB shares if the user is suspected of destroying data. Furthermore, snapshots are created for all SMB shares to which the suspected user has access. In the event of accidental deletions, recovery is simplified through automatically applied snapshots. The following figure displays the Mass Delete Configuration window.



Mass Delete Configuration

Enabled

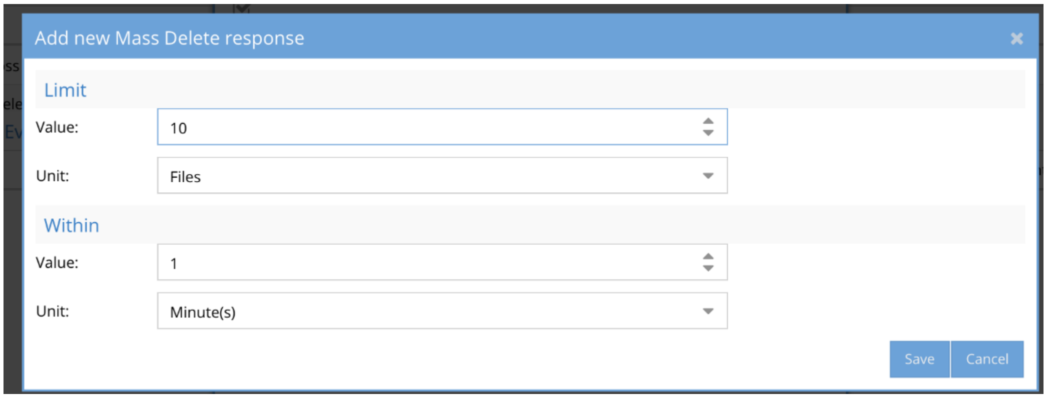
☑

Threat Responses

Limit	Unit	Interval	Response	Actions
10	Files	1 Min	ALARM	delete

Figure 26. Mass Delete Configuration

Additionally, Mass Delete responses can be configured, as shown in the following figure.



Add new Mass Delete response

Limit

Value: 10

Unit: Files

Within

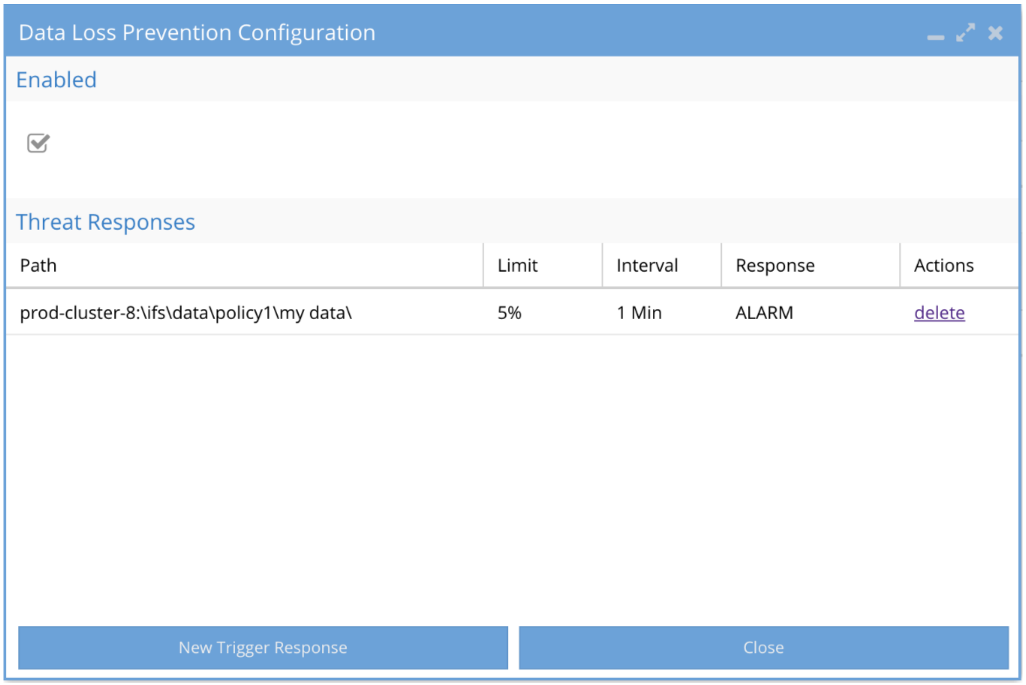
Value: 1

Unit: Minute(s)

Figure 27. Mass Delete Response

Data loss prevention

Active Auditor’s data loss prevention feature monitors users who copy files on any secure share or path. The feature provides real-time monitoring of secured data from bulk copy operations that are not authorized or an indication of a potential data loss scenario. An auto applied accounting quota is used to monitor the capacity of the file system path. Administrators specify a percentage of the data any user can read from the path before the audit trigger is detected. The triggers create an alert that includes the date, time, and IP address of the event. The Data Loss Prevent Configuration window is shown in the following figure.



Data Loss Prevention Configuration

Enabled

☑

Threat Responses

Path	Limit	Interval	Response	Actions
prod-cluster-8:\ifs\data\policy1\my data\	5%	1 Min	ALARM	delete

Figure 28. Data Loss Prevent Configuration window

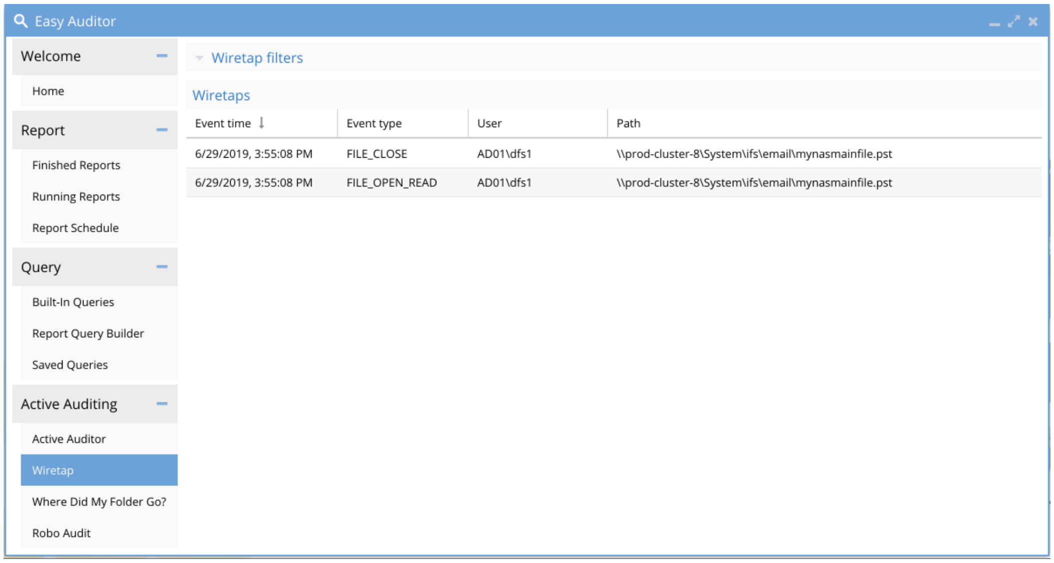
WireTap

Administrators or security personnel can view a live feed of events in real-time using WireTap. The events are triggered by user actions. Rather than examining events independently, the captured events provide security staff with a comprehensive overview of the incident. Audit events are processed in real-time to stream the events directly to the WireTap UI.

Some real-time scenarios where a WireTap would be beneficial are:

- Specified path to monitor multiple users
- Monitor only a specific user
- Monitor a folder – with or without sub-folders

The WireTap UI displays the live events in real-time, as shown in the following figure.



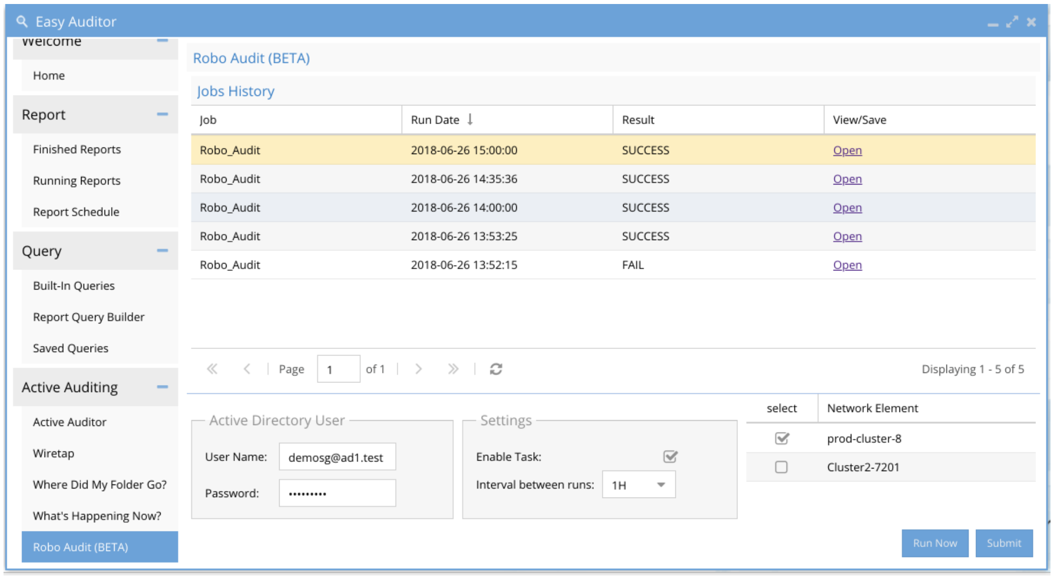
Wiretaps

Event time	Event type	User	Path
6/29/2019, 3:55:08 PM	FILE_CLOSE	AD01\dfs1	\\prod-cluster-8\System\ifs\email\mynasmainfile.pst
6/29/2019, 3:55:08 PM	FILE_OPEN_READ	AD01\dfs1	\\prod-cluster-8\System\ifs\email\mynasmainfile.pst

Figure 29. WireTap UI

Robo Audit

The Robo Audit feature allows administrators to test the cluster for audit events, to ensure that the audit and security features are functioning correctly. The feature creates an SMB connected user to create events, allowing verification of file and directory events. A complete report is generated logging the user functions to matching audit events. The Robo Audit jobs are also displayed in the UI, as shown in the following figure.



Jobs History

Job	Run Date	Result	View/Save
Robo_Audit	2018-06-26 15:00:00	SUCCESS	Open
Robo_Audit	2018-06-26 14:35:36	SUCCESS	Open
Robo_Audit	2018-06-26 14:00:00	SUCCESS	Open
Robo_Audit	2018-06-26 13:53:25	SUCCESS	Open
Robo_Audit	2018-06-26 13:52:15	FAIL	Open

Active Directory User

User Name: demosg@ad1.test

Password: •••••••••

Settings

Enable Task: ☑

Interval between runs: 1H

select	Network Element
☑	prod-cluster-8
☐	Cluster2-7201

Figure 30. Robo Audit history

Ransomware Defender vs Easy Auditor

Together, Ransomware Defender and Easy Auditor provide powerful cyber protection. However, it is important to note that each module's cybersecurity features, and coverage areas are unique. The following table summarizes the key attributes of each module.

Table 5. Ransomware Defender vs Easy Auditor cybersecurity coverage

Ransomware Defender	Easy Auditor
Real-time per-user behavior-based detection: Displays user, IP, shares, and files affected	Top active users (files created, deleted, renamed, and so on)
Automated snapshot creation upon initial detection for ground-zero restore point	Least accessed shares by user (Stale permissions report)
Per user lockout automated response and file system data protection	Share access report
Cyber recovery manager streamlines recovery from snapshots, automating the process to determine the best available restore point for each file affected	Login reports
In-Eyeglass alerts plus email, syslog, or webhook forwarding of events to a SIEM (Zero Trust API) tool or slack channel	Helps administrators find who deleted or moved a file
Honeypot tripwire feature for enhanced protection	Mass Delete feature: Detect, react, and prevent a number of files deleted from a specified folder
Automated security penetration testing ensures that defenses are fully operational by testing detection and lockout on a scheduled basis	Data Loss Prevention: Detect and prevent bulk data copying of sensitive data
Access to data itself is not required because Ransomware Defender is not in the client access path	Wiretap feature used to monitor all IO to a path or a user for security monitoring, or excess permissions to a path, share, or export
Zero Trust API Integration provides: • XDR/SIEM without input & response capabilities based on the storage domain • Initiate Ransomware Defender automated response for Critical Path Snapshot or User Lockout - Protects data on the PowerScale cluster based on suspicious activity detected by another component in the data center	Create custom policies that alert when a specific behavior occurs on the filesystem

Deployment and configuration considerations

The modules in the PowerScale Cyber Protection Suite have unique deployment and configuration considerations. This section describes module dependencies, interactions, considerations, and hardware requirements.

Module dependencies

The PowerScale Cyber Protection Suite is composed of advanced software modules that form a barrier of cyber protection throughout the ransomware lifecycle and across the data center. The best practice for PowerScale cyber protection is to deploy all of the modules. However, depending on the environment, budget constraints, and IT administration requirements, not all the modules may be applicable. In this case, consider the dependencies for each of the modules in the following table. Eyeglass is required for managing the cyber protection modules.

Table 6. Cyber Protection Suite module dependencies

Module	Required modules for deployment
Ransomware Defender	Eyeglass
Easy Auditor	Eyeglass
AirGap Enterprise	Ransomware Defender, Eyeglass

Module interactions

Although it is possible to only deploy select modules in the PowerScale Cyber Protection Suite, it is important to understand how each module enhances the other modules in the suite.

Ransomware Defender and AirGap Enterprise

Ransomware Defender is a required module for the AirGap Enterprise module. The AirGap Enterprise Agent communicates with Ransomware Defender for active security events before starting replication.

Easy Auditor and Ransomware Defender

Easy Auditor shares audit data with Ransomware Defender to warn of any security events. Ransomware Defender can then use the audit events as a basis for further inspection for anomalies in access patterns. Deploying Easy Auditor enhances Ransomware Defender's overall security coverage.

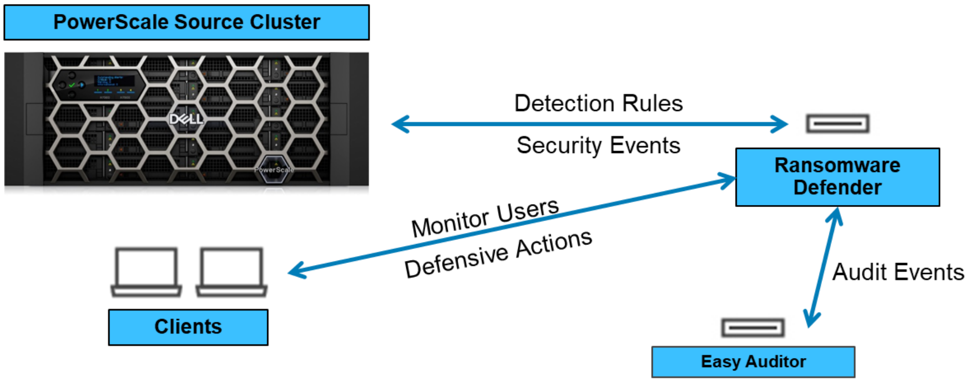


Figure 31. Easy Auditor and Ransomware Defender interaction

AirGap Enterprise and Easy Auditor

Easy Auditor's active auditing features can be extended to the PowerScale vault cluster. The vault's security is further enhanced with triggers for data loss prevention, mass deletes, and other custom triggers. Easy Auditor's user and network aware policies are used to stop replication to the vault cluster if active events occur.

AirGap Enterprise design considerations

This section describes design considerations for AirGap Enterprise.

Network design

On the PowerScale Source Cluster, some of the nodes are connected through a Vault L3 Switch, located in the Cyber Recovery Vault, to the PowerScale Vault Cluster. Although the number of nodes connected to the Vault L3 Switch varies based on cluster size and workflow requirements, it is recommended to have at least two of the nodes' front-end network ports connect through the Vault L3 Switch. The rest of the nodes on the source cluster connect to the production network. All the PowerScale Vault Cluster nodes connect to the Vault L3 Switch as shown in the following figure.

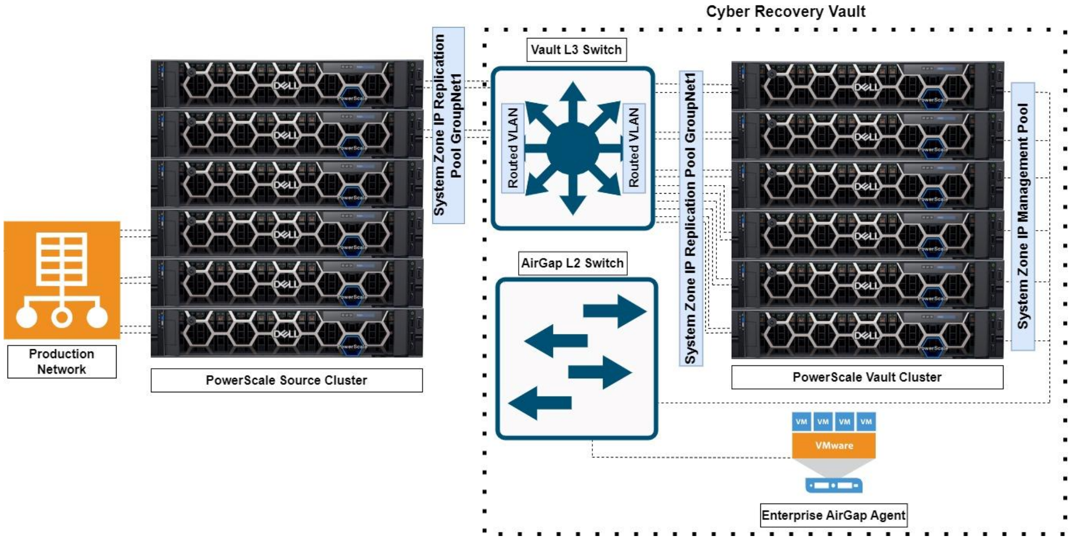


Figure 32. PowerScale Source Cluster to Vault Cluster topology

The source cluster nodes that connect to the Vault L3 Switch require a direct connection without any additional network hops for optimal security. The source and vault cluster nodes connect to the Vault L3 Switch through their respective System Zone IP Replication Pool Groupnet1. The Vault L3 Switch routes the VLAN from the source cluster to the VLAN for the vault cluster.

Inside the Cyber Recovery Vault, the PowerScale Vault Cluster management ports connect through a System Zone IP Management Pool to the AirGap L2 Switch. The AirGap L2 Switch also connects to the VMware ESXi host running the AirGap Enterprise vault agent.

Considering that each node on the source cluster can only connect to either the Vault L3 Switch or the production network, a common question is how to split the nodes between the networks. The best practice is for at least two of the source cluster nodes to connect to the Vault L3 Switch. Additional source cluster nodes can connect to the Vault L3 Switch, depending on the source cluster size, workflow, and recovery requirements.

Firewall

Adding a firewall to the Cyber Recovery Vault is an optional configuration. The minimum best practice is having the Vault L3 Switch manage replication into the Cyber Recovery Vault as explained in the section Network design. A firewall could be used in place of the Vault L3 Switch routing between the source cluster and the vault cluster as shown in the following figure.

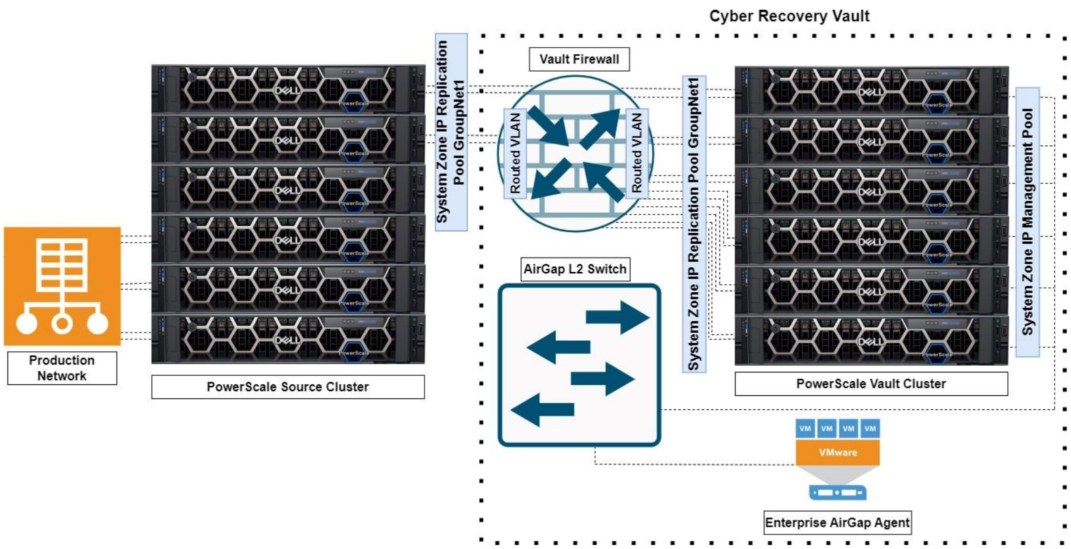


Figure 33. Cyber Recovery Vault with Vault Firewall

Depending on the Vault L3 Switch vendor, configuration, and release, a firewall provides additional protection in most cases. The level of additional protection is difficult to gauge because each switch and firewall vendor implements different security functions. Consider how the specific Vault L3 Switch compares with the specific firewall.

Traditionally, firewalls provide additional security over an L3 switch. If a firewall is configured to block all incoming traffic, any host requesting data from outside the Cyber Recovery Vault would be denied. An Access Control List (ACL) could be configured to allow traffic only from the source cluster. Another option would be a reflexive ACL that could see an outbound connection, and it can be configured to reflect outbound connections, allowing traffic back on that connection. The stateful behavior of firewalls maintains a connection state, up to a timeout period of inactivity, blocking traffic when the connection is closed.

A Next-Generation Firewall (NGFW) would provide an added layer of security with deep packet inspection to determine what type of data heuristically is passing through, or which application is communicating. The NGFW provides flexibility to block or allow data with granular options. For example, the NGFW could detect and block malware in a data stream. Traffic could be limited to and from a single application or host. Considering that the NGFW would be in the Cyber Recovery Vault, a maintenance window would have to be planned for to ensure that the software is current against threats.

Another factor to consider with a firewall are the impacts on data replication speed. The additional packet filtering does consume time, but the impacts vary, and are minimal with the new generation firewalls, depending on the firewall version and vendor.

Adding a firewall to the Cyber Recovery Vault can also create additional management overhead. The device must be configured and updated in a cadence. Access roles must be configured, and other overhead should be considered during the design phase.

It is important to understand that the network interfaces on the vault cluster are added only for replication and then removed when not in use. Further, OneFS release 9.5 and later include a built-in firewall. For more information about the OneFS firewall, see the white paper PowerScale: Network Design Considerations | Dell Technologies Info Hub.

Accelerator nodes

Given that not all the source and vault cluster nodes are connected through the Vault L3 Switch, adding accelerator nodes to both the source and vault clusters provides additional replication throughput. If accelerator nodes are to be used, as a best practice add them to both the source and vault clusters. Further, ensure that they are both part of the nodes participating in the replication and connected through the Vault L3 Switch as shown in the following figure.

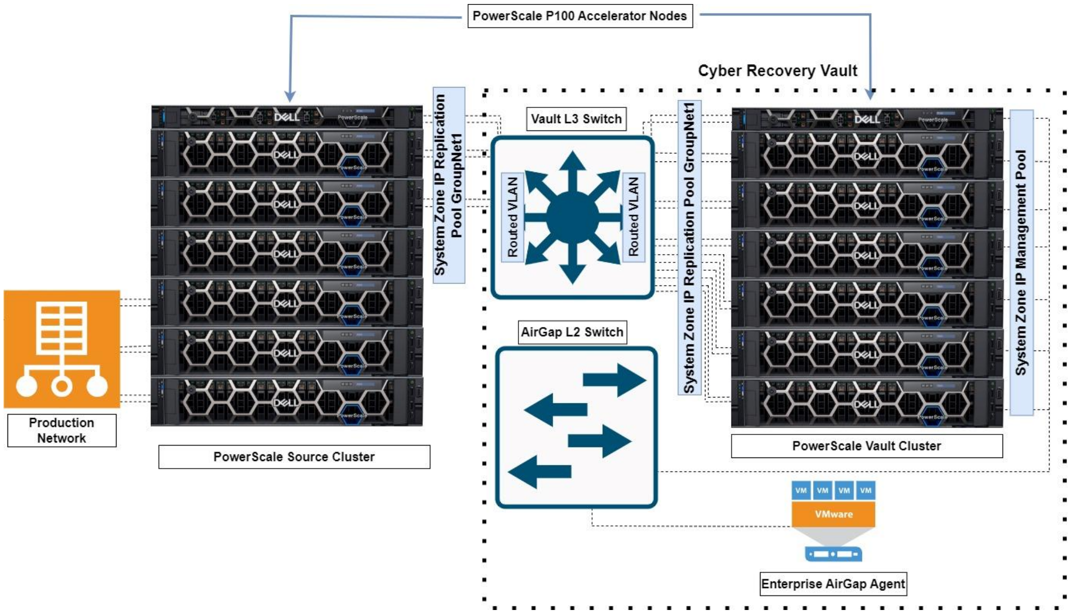

PowerScale P100 Accelerator Nodes
Cyber Recovery Vault
System Zone IP Replication Pool GroupNet1
Vault L3 Switch
Routed VLAN
Routed VLAN
System Zone IP Replication Pool GroupNet1
System Zone IP Management Pool
AirGap L2 Switch
Production Network
PowerScale Source Cluster
PowerScale Vault Cluster
VM
VM
VM
VM
VMware
Enterprise AirGap Agent

Figure 34. PowerScale Source to Vault Cluster Topology with Accelerator Nodes

During SyncIQ replication, the nodes generate worker streams between the clusters. The accelerator nodes read and write data from other nodes in the cluster. This optimizes the overall cluster throughput, considering all of the source cluster nodes are not connected through the Vault L3 Switch.

Fiber-cut switch

The Cyber Recovery Vault can be further isolated using a fiber-cut kill switch, simulating a real-world fiber-cut scenario. The fiber-cut switch provides electrical and electromagnetic isolation as an optional part of the Cyber Recovery Vault. An out-of-band management channel is used to isolate the network using fiber-cut simulation and REST APIs/CLIs. Further, it can also function as a kill switch for better containment by blocking the lateral movement of ransomware. Using the fiber-cut switch still allows for the choice of either the Vault L3 Switch or the Vault Firewall because it is physically placed outside the vault, as shown in the following figure.

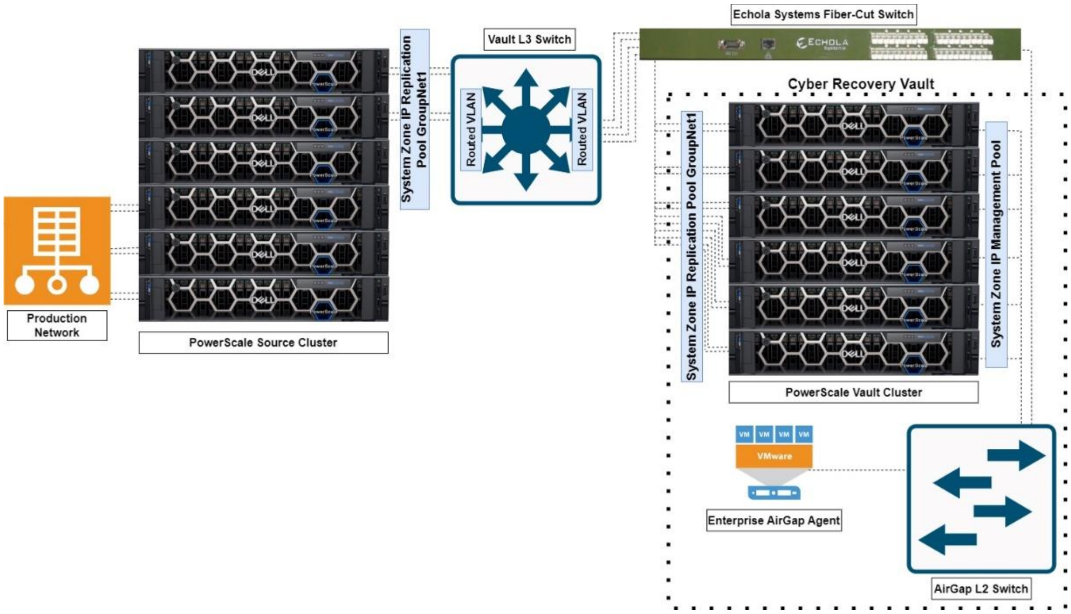

Echola Systems Fiber-Cut Switch
Vault L3 Switch
Routed VLAN
Routed VLAN
System Zone IP Replication Pool GroupNet1
Cyber Recovery Vault
System Zone IP Replication Pool GroupNet1
System Zone IP Management Pool
Production Network
PowerScale Source Cluster
PowerScale Vault Cluster
VM
VM
VM
VM
VMware
Enterprise AirGap Agent
AirGap L2 Switch

Figure 35. PowerScale Source to Vault Cluster Topology with Echola fiber-cut switch

For more information about the Echola Systems fiber-cut switch, see Echola Systems Optical switch products.

SyncIQ considerations

Although the considerations here are specific to a source and vault cluster, the general SyncIQ design considerations for a source and target cluster are applicable. For more information about SyncIQ design considerations, see Dell PowerScale SyncIQ: Architecture, Configuration, and Considerations | Dell Technologies Info Hub.

Vault cluster license requirements

The vault cluster requires SmartConnect Advanced, SyncIQ, and SnapshotIQ licenses. SmartDedupe and SmartLock are optional, depending on the data requirements.

Source and vault cluster node platforms

During the design phase, consider how the node platforms on the source and vault cluster affect the overall data replication performance. When a performance node on the source cluster is replicating to archive nodes on the vault cluster, the overall data replication performance is compromised based on the limited performance of the vault cluster’s nodes. For example, if a source cluster is composed of F900 nodes and the vault cluster is composed of A3000 nodes, the replication performance reaches a threshold because the A3000 CPUs cannot perform at the same level as the F900 CPUs.

Depending on the workflow and replication requirements, the longer replication times may not be a concern. However, if replication performance is time sensitive, consider the node types and associated CPUs on the source and target clusters, because this could bottleneck the overall data replication times.

For maximum SyncIQ efficiency, a matching node platform for both clusters is recommended, because the number of SyncIQ workers is based on the node’s CPU. If the vault cluster has a lower performance node, it would not be able to maintain the source cluster’s stream throughput.

Business continuity dataset and cluster node platforms

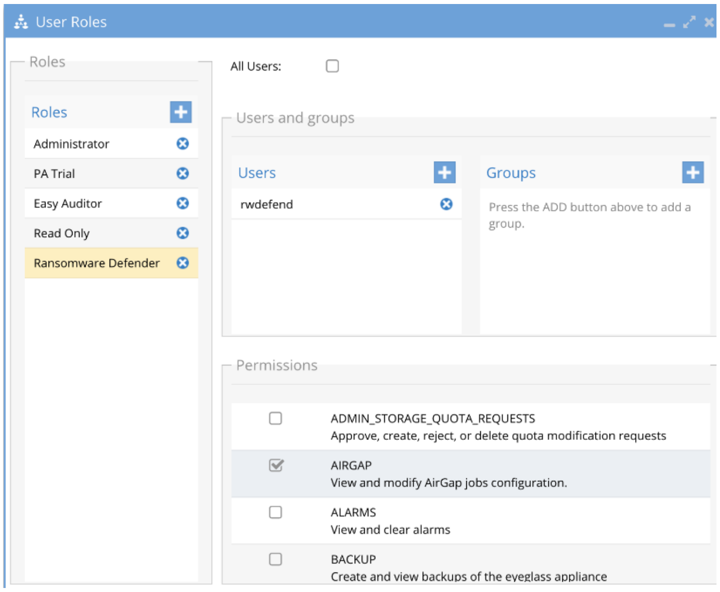
During the design phase, consider how the business continuity dataset that is stored on the PowerScale Vault Cluster impacts the node quantity and platform of the source and vault cluster. The first step is identifying the business continuity dataset, because several departments must agree on the business continuity dataset.

When the dataset is defined, the next step is to consider how quickly the dataset is changing. Based on the frequency of dataset changes, from a business continuity perspective, organizations must consider the stale data that occurs as the dataset ages from the last update. From this data point, extract the size and frequency of the dataset changes. If the dataset has significant changes in a short time span, this will impact how quickly the dataset can be replicated from the source to vault cluster. The dataset replication speed depends on many factors, but mainly the source and vault cluster sizes, available bandwidth, node platforms, and overall cluster resources. If the source and vault cluster are composed of a larger quantity of nodes, data replication is faster. Further, if the source and vault cluster nodes are performance nodes, more SyncIQ streams are created between the clusters, increasing replication throughput.

Access control and management

On the source cluster, administrators should be assigned with the minimum required Role Based Access Control (RBAC). On the vault cluster, only the Chief Security Officer (CSO) or other senior security management staff should have access. For more information about configuring RBAC for OneFS, see Introduction to Role Based Access Control | PowerScale OneFS Authentication, Identity Management, and Authorization | Dell Technologies Info Hub.

The Cyber Recovery Vault should follow a similar access permission as the source and vault cluster. Although AirGap Enterprise is part of the Ransomware Defender module, it allows for a separate user role to manage the AirGap function. Similar to the vault cluster access, it is also best practice to have the CSO or other senior security management assigned the role of managing AirGap Enterprise. The administrators managing Ransomware Defender must be separate from the staff managing the AirGap function. Ransomware Defender has a role specifically for AirGap. In the following figure, a dedicated role option is available in Ransomware Defender for AirGap.



Roles: Administrator, PA Trial, Easy Auditor, Read Only, Ransomware Defender

All Users: □

Users: rwdefend

Groups: Press the ADD button above to add a group.

Permissions:

- □ ADMIN_STORAGE_QUOTA_REQUESTS
  Approve, create, reject, or delete quota modification requests
- ☑ AIRGAP
  View and modify AirGap jobs configuration.
- □ ALARMS
  View and clear alarms
- □ BACKUP
  Create and view backups of the eyeglass appliance

Figure 36. AirGap user role in Ransomware Defender

Jump server

Optionally, a jump server can be configured to reside inside the Cyber Recovery Vault, providing an option for access into the Cyber Recovery Vault. Although, the jump server eases the administration of the Cyber Recovery Vault, consider the security impacts because it is a device with access outside the vault. Ensure that the jump server is configured similarly to the Vault Cluster, where only the Chief Security Officer (CSO) or other senior security management staff have access. The applications on the jump server must also be limited and configured for minimal access.

Hardware requirements

This section provides the hardware deployment requirements for each of the modules in the PowerScale Cyber Protection Suite.

Eyeglass

The Eyeglass module deployment requirements are the following:

- vSphere 6.0 ESX host or higher or Hyper-V with VHDX appliance requires
  - vCenter supported deployment clients
    - vCenter 6.5 Flex or html5
    - vCenter 6.7 Flex client (VMware bug broke OVF with html WebUI)
    - vCenter 7.0.1 Build: 17491160

Note: All other hypervisor options are unsupported. Support for Eyeglass requires using a vApp.

- 4 vCPU
- 16 GB RAM (RAM must be upgraded based on the scalability table here)
- 30G OS partition plus 80 GB disk total disk size in VMware 110 GB
- IP Port Requirements: Eyeglass Ports Requirements , Scalability Limits and Phone Home Requirements (supernaeyeglass.com)

Ransomware Defender and Easy Auditor

Ransomware Defender and Easy Auditor share a VM instance that form a stack to process audit data. The stack is referred to as the Eyeglass Clustered Agent (ECA). For deployment requirements, see the ECA Cluster Sizing and Performance Considerations at Eyeglass Clustered Agent vAPP Install and Upgrade Guide (Ransomware Defender, Easy Auditor, Performance Auditor) (supernaeyeglass.com).

AirGap Enterprise

AirGap Enterprise is a licensed module for Ransomware Defender. AirGap Enterprise is a single VM instance that resides in the secure AirGap vault ESX host. The module has the following requirements:

- Dedicated AirGap management switch (L2/L3): S3048-ON
- Optional fiber-cut switch
- Optional firewall
- Optional jump server: Dell R240
- ToR Switches: Dell S5248F-ON
- Dell PowerEdge R450 vSphere 6.0 or higher appliance requires:
  - 4 vCPU
  - 16 GB RAM
  - 30G OS partition plus 80 GB disk total disk size in VMware 110 GB

Further reading

For more information about PowerScale's cyber protection advanced software suite, see the following interactive demos and Hands-On Labs:

- Be a Cyber Hero with the PowerScale Cyber Resiliency Solution Powered by Ransomware Defender | Demo Center (dell.com)
- Be a PowerScale Pro with Superna EyeGlass | Demo Center (dell.com)
- PowerScale Cyber Protection solution powered by Ransomware Defender Getting Started | Demo Center (dell.com)
- Setup and management of DR for PowerScale, powered by Superna Eyeglass | Demo Center (dell.com)

References

Dell Technologies documentation

The following Dell Technologies documentation provides other information related to this document. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

- PowerScale (Isilon) | Dell Technologies Info Hub Dell PowerScale SyncIQ: Architecture, Configuration, and Considerations | Dell Technologies Info Hub
- Dell PowerProtect Data Manager: Dynamic NAS Protection | Dell Technologies Info Hub
- Incident Response and Recovery Data Sheet (delltechnologies.com)
- Dell PowerScale OneFS: Security Considerations | Dell Technologies Info Hub.
- PowerScale OneFS 9.6.0.0 Security Configuration Guide (dell.com)
- PowerScale (Isilon) | Dell Technologies Info Hub

Other documentation

- Worldwide Security Spending Guide (idc.com)
- 2022 Gartner Board of Directors Survey
- CNA Financial Paid Hackers $40 Million in Ransom After Cyberattack (businessinsider.com)
- JBS: Cyber-attack hits world's largest meat supplier - BBC News
- 'Payment sent' - travel giant CWT pays $4.5 million ransom to cyber criminals | Reuters
- Colonial Pipeline reportedly paid $5M to hackers after ransomware attack - CNET
- Chemical distributor pays $4.4 million to DarkSide ransomware (bleepingcomputer.com)
- National Institute of Standards and Technology (nist.gov)
- Eyeglass Datasheet (supernaeyeglass.com)
- Ransomware Defender Datasheet (supernaeyeglass.com)
- Ransomware Defender Zero Trust API Datasheet (supernaeyeglass.com)
- Progress Flowmon and Zero Trust API Datasheet
- Protect Data from Ransomware with Flowmon & Superna - YouTube
- Zero Trust with Veeam Backup Solution and PowerScale (supernaeyeglass.com)
- Easy Auditor Datasheet (supernaeyeglass.com)
- Subscription Service - Monitored Security Service (supernaeyeglass.com)

- Ransomware Defender AirGap 2.0 Datasheet v6 (supernaeyeglass.com)
- Cyber Recovery Manager (supernaeyeglass.com)
- Eyeglass Clustered Agent vAPP Install and Upgrade Guide (Ransomware Defender, Easy Auditor, Performance Auditor) (supernaeyeglass.com)
- Eyeglass Ports Requirements, Scalability Limits and Phone Home Requirements (supernaeyeglass.com)