Lab Insight Report

Validation of Dell PowerProtect Cyber Recovery

Enhanced Ransomware Resiliency with Managed Data Isolation

By Krista Macomber, Senior Analyst

March 2023

Evaluator Group

Enabling you to make the best technology decisions

Introduction

Creating an isolated, or “air-gapped” storage environment has long been a best practice for enterprise data protection, following the “3-2-1” rule that calls for an off-site data copy. Today, it becomes even more important, as ransomware attackers target backup environments in an effort to inhibit companies from being able to recover from compromised data.

In fact, **recent Evaluator Group research** found that, while in 2019, approximately 22% of enterprises had an air gap in place, today, more than 30% have implemented an air gap over the past year in response to ransomware resiliency requirements, and another 27% plan to implement or to expand their usage of air-gapped storage for cyber-resiliency.

The problem is that IT Operations teams are struggling against the constraints of limited staffing and headcount resources. They are steadily running out of time to be able to manage the physically air-gapped tape storage implementations that have traditionally been used to achieve the isolated storage environment. As a result, they are looking to the public cloud and managed services for streamlined consumption. However, achieving isolation requires more than just shipping data to the cloud.

This paper reviews the capabilities of Dell PowerProtect Cyber Recovery, a solution for vaulting data to an isolated storage environment. In addition to detailing the specific capabilities of this solution, it includes items for IT Operations to consider as they are evaluating all such data vault solutions.

Dell PowerProtect Cyber Recovery: Key Differentiators

- Foundation based on Dell PowerProtect DD appliances
- Flexible deployments - on-premises, in cloud, Dell-managed or combination
- Isolated network and management interface
- Policy-driven, non-persistent access to vault
- CyberSense integration inspects full content of databases and files
    - 99.5% confident to detect corruption based on ~200 million file operations
    - Identify most recent non-corrupt recovery point

Background for Dell Data Vaulting

Dell PowerProtect Cyber Recovery provides an isolated environment that can be used as a vault for storing immutable and encrypted data copies, and as a sandbox environment for creating writeable copies for data validation and analytics (e.g., checking for signs of tampering). The solution is available on-premises and can be deployed in AWS, Azure and Google Cloud Platform. It’s also available as a managed service offering through Dell

APEX Cyber Recovery Services. Evaluator Group validated the on-premises, customer-managed deployment option that is based on Dell PowerProtect Data Manager running version 19.12 of Dell's PowerProtect Cyber Recovery software and CyberSense 8.0, which was developed by Index Engines.

Validation of Dell PowerProtect Cyber Recovery

Solution Overview

PowerProtect Cyber Recovery functions by replicating data from a primary backup storage system to the Cyber Recovery environment. Data is transferred over an isolated, secure network that is severed following the conclusion of the data transfer job (a detailed validation of these functionalities follows). If desired, customers have the option to vault to multiple Cyber Recovery targets. Cyber Recovery data copies can be used to create independent, full backup copies for recovery, or they can be migrated from the data vault environment back into production. The solution integrates with Index Engines CyberSense for scanning and analysis capabilities (most notably, to support ransomware recovery).

Solution Architecture

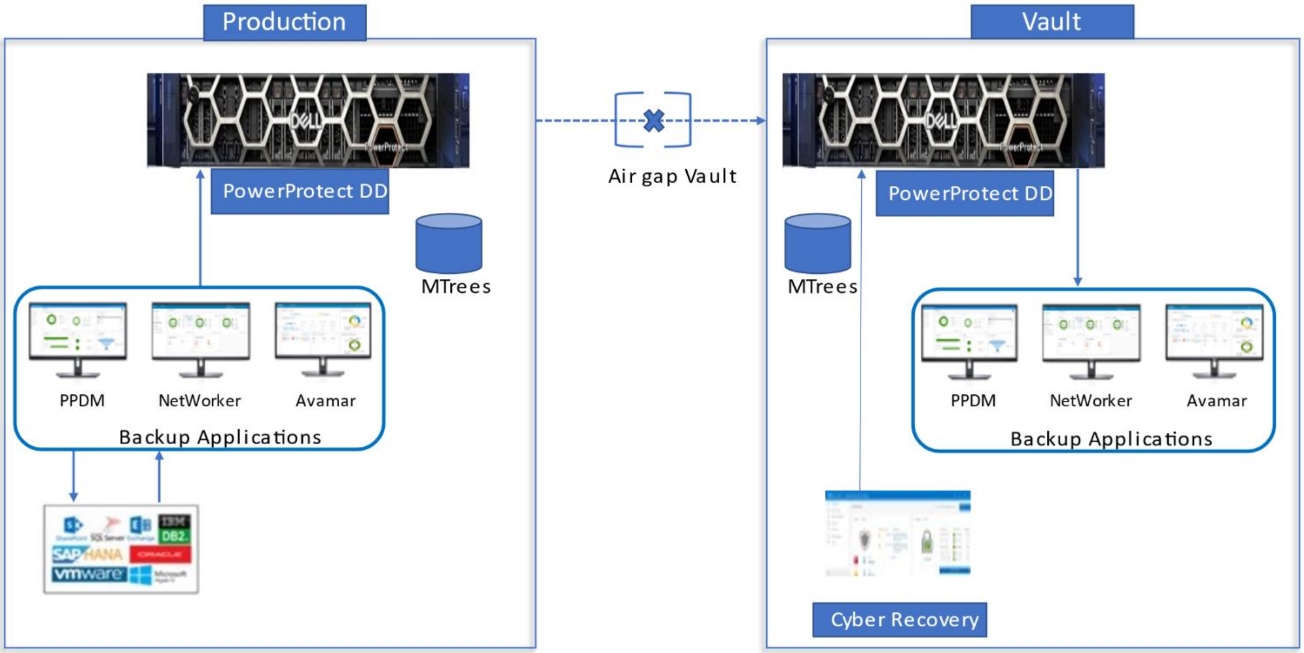

Figure 1: Dell PowerProtect Cyber Recovery Architecture (Source: Dell)

Dell PowerProtect Cyber Recovery encompasses a "production" and a "vault" environment. The production environment consists of a backup application (namely Dell PowerProtect Data Manager, Avamar, or NetWorker) that runs core backup operations. Specifically, the backup data must be stored on PowerProtect DD Systems that sit on premises in the customer's data center. The production

PowerProtect DD system replicates the data over an isolated network to a PowerProtect DD system that is deployed in the Cyber Recovery vault environment. Evaluator Group validated a PowerProtect Cyber Recovery solution that used an on-premises vault environment; in the event that the vault environment is hosted in the public cloud, the solution uses a PowerProtect DD Virtual Edition that is deployed in front of the cloud object store. In addition to the PowerProtect DD target, the vault environment includes the Cyber Recovery software, which controls vaulting operations. It also may include an instance of the backup software, if it is required for application recovery operations, as well as any other required applications (namely, CyberSense).

Validation Overview

The following is a summary of the key capabilities encompassed in this Lab Validation. The validation stages included isolating production data to the vault and confirming immutability, allowing ransomware to be copied into the vault and detected, and finally restoring uncorrupted backup data from the vault to production.

Stage I: Isolation and Immutability

- Isolate production data by copying into the vault with the sync operation
- Confirm air gapping functionality
    - Test network isolation capabilities, and the ability to sever connection when data is not being transferred.
    - Verify that the management interface cannot be accessed from production/public-facing portions of the environment.
    - Test the ability to access via CLI and API
    - Verify access control capabilities (MFA, etc.)
    - From production, sync to vault, lock, and demonstrate that the vaulted copy cannot be changed.
- Attempt to delete the protected copies that are synced to the vault, without privileged access
- Immutability functionality
    - Observe the control over retention periods.
    - Attempt to:
        - Delete immutable backup copies in the vault
            - Use various roles (backup, cluster, general admin, etc.) to change retention period on the backups.
            - Attempt to trigger the end of the retention period by tampering with the PowerProtect DD system clock.

Stage II: Ransomware Detection

- From production, simulate corruption, copy corrupted data to the vault.

- Demonstrate detection of corruption.
- Testing of Index Engines' CyberSense scanning and analytics (backup integrity, indicators of attack), including:
    - ML-based analysis for suspicious activity indicating an attack
    - Scanning of incremental backups in the Cyber Recovery Vault and comparisons to the previous state
    - ID of last known good recovery point
    - Forensic reporting and analysis to ID corrupted files (requires CyberSense dashboard)

Stage III: Recovery

- Ability to recover uncompromised backups and granular files within the vault as well as back to the production PowerProtect DD

Evaluation: Policy-Based Operations

Cyber Recovery operations are policy-based and controlled through the Cyber Recovery user interface (UI), command line interface (CLI), or REST API. The following list encompasses the operations that are possible – and that Evaluator Group witnessed – for vaulted data:

- Copy – Creates a point-in-time copy to be stored in the vault.
- Secure Copy – Adds a retention lock to the data copy that is created under the Sync Copy operation.
- Copy Lock – Locks the vault copy with a retention hold.
- Secure Copy Analyze – Invokes CyberSense to analyze the data copy that is created under the Secure Copy operation.
- Sync Copy – Combines the Copy and Sync operations; data is synchronously replicated, and then another copy is created.
- Sync – synchronous replication of data from the production environment to the vault
    - Via the CyberRecovery CLI, data can be synced to a system other than the PowerProtect DD system in the vault, for out-of-place recovery scenarios.

Evaluation: Replication Processes and the Vaulting Window

Evaluator Group observed that the designation of what data is vaulted is controlled through the production backup application (e.g., Dell PowerProtect Data Manager), and that the vaulting window – that is, the period of time in which data is synced – is controlled through policies that are set in the Cyber Recovery user interface. The validation exercise confirmed that the vault is only unlocked when data is being synced to it; not only is transferred over an isolated network that is secured with the TLS 1.2 cryptographic protocol, the network connection is only established during the vaulting period. Additionally, the ability for security officers or admins to manually secure the Cyber Recovery vault environment was verified. Replication jobs in progress at the end of the vaulting window are paused. For security reasons, a policy can be set up by the administrator to cancel jobs automatically if they are not resumed after a designated period of time. The administrator automatically receives an alert after 24 hours if the job is not resumed.

Evaluation: Access Control

Access to the vault and subsequent user privileges are role-based. The solution includes three core, default roles. Evaluator Group witnessed the following user roles and functions.

- Dashboard
    - Can view the Cyber Recovery dashboard.
        - Can view the status but cannot alter policies.
        - Cannot secure or de-secure the vault environment.
        - Cannot change passwords belonging to other users.
- Admin
    - Can perform all Cyber Recovery operational tasks.
    - Can change their own passwords, but not the passwords belonging to other admins.
- Security Officer
    - The Cyber Recovery security officer (crso) is created during installation and is assigned the security office role. This user can be considered the “super user” and creates other users.
    - Can create, modify, enable, disable, and delete all user accounts, with the exception of the “crso” “super user” (more details on this role below). Functions include:
        - Setting password expiration. This is applied for all users, with a minimum of 30 days and a maximum of 180 days.
        - Disabling multifactor authentication (MFA – this can be applied by users via an external application) for admins or for other security officers.
    - Can perform all Cyber Recovery operational tasks.
        - Including administrative settings and activity reports.
    - More than one security officer can be designated, but there can only be one crso super user per Cyber Recovery installation.

Authentication is token-based, and it occurs via the Cyber Recovery REST API with the Hypertext Transfer Protocol Secure (HTTPS) used for secure communications with client-side components.

For PowerProtect Cyber Recovery implementations using an on-premises vault environment – such as that validated by Evaluator Group – Dell advises customers to require an administrator to physically go into the data center to access the terminal controlling the vault environment. Dell does not advise customers to deploy a “jump server” as the host on the production side, in order to keep the two security domains separate. Dell furthermore advises the use of firewalls and providing as few users as possible with access to the vault’s subnet.

Evaluation: Maintenance, Monitoring and Reporting

Evaluator Group observed the Dell PowerProtect Cyber Recovery solution’s various UI, dashboarding and reporting capabilities.

The Cyber Recovery UI indicates the status of the vault:

- Locked – Network connections are closed; replication to the vault is not occurring.
- Unlocked – One or more network connections are open; replication to the vault is occurring.
- Secured – A Security Officer or Admin user has manually locked the connection.

There is also a Cyber Recovery dashboard view, and a tab displaying Alerts and Events. These provide users with visibility into:

- System/server issues, storage issues, and security issues.
- Updated user information, completion of retention locks, and other key activities.
- From there, users can take any action as might be required.

The Cyber Recovery UI also provides job monitoring (Running, Successful, Completed with Exceptions, or Failed). These include:

- Protection jobs
- System jobs (e.g., cleaning operations)
  - The Maintenance/Cleaning schedule is set by default to occur once every seven days, and it is configurable via the UI.
- Recovery jobs (including creating and deleting sandbox environments)

The UI provides alerts, and users can receive email notifications. They also can run and export system and job reports that are based on full logging capabilities.

Evaluation: Immutability and Encryption

Once the data reaches the vault, users have the ability to “Lock” a data copy for a designated retention period, through the Cyber Recovery User Interface. Evaluator Group observed that, during this period, the copy is immutable; it can be viewed, but it cannot be modified or deleted. Once set, the retention lock can be extended, but it cannot be decreased or removed without the credentials of a Security Officer. Dell recommends the use of Retention Lock Compliance. If Compliance Mode is applied, no user can alter the retention lock settings, including through tampering with the system clock of the vault PowerProtect DD.

As data is being replicated from the production environment to the vault, it needs to be secure. Backup data is encrypted in flight as it is replicated to the cyber vault. Once it lands on the PowerProtect DD in the vault, it is encrypted at rest.

Evaluation: Index Engines' CyberSense

CyberSense, which was developed by Index Engines, can be added as an application to PowerProtect Cyber Recovery. It allows the vaulted copies to be used for forensic analytics and recovery following a cyberattack such as a ransomware attack. This helps not only to discover malware attacks by identifying suspicious or unusual activity, but also to uncover the closest available recovery point prior to the attack (a key challenge for IT Operations when recovering from ransomware) to mitigate the amount of data loss.In execution, CyberSense is fully integrated with the Dell Cyber Recovery host server, allowing Cyber Recovery to control the replication to the vault, and the orchestration of CyberSense analysis via RESTful API. CyberSense reads files in the backup images without needing to rehydrate them. It then indexes the files and analyzes them. The index size itself is less than 1% of the data indexed, making it capable of supporting enterprise scale.

While most ransomware analytics tools in use in data protection environments focus on inspectng file metadata, CyberSense goes a step further, inspecting the content of files (for instance inspecting the content of file headers and database structural integrity). This is a differentiator because ransomware variants are evolving to only encrypt part of the file in order to avoid detection. Intermittent and partial encryption falls behind the threshold analysis that is used by most tools to indicate potentially malicious activity. This approach also could help to detect if a file has been

CyberSense
Machine Learning Model Training

- Based on anonymized structured datasets containing >150 features representing file content or metadata changes.
- Datasets are created by analyzing controlled detonation of live ransomware obtained from public subscription services, and by simulating attacks using detailed descriptions of ransomware from a network of dozens of global researchers.
- Also uses customer-submitted, real-world datasets representing clean data, data that has been attacked, and data suspected of being attacked. As of March 2023, Index Engines has collected approximately 70 million customer samples, which is increasing over 5 million per month.
- The datasets are organized into behavioral classes (indicators of compromise). Representative samples from each class are decomposed into ~200 million fundamental file operations that are statistically combined to generate millions of different simulated attack and non-attack scenarios which are then used to train the MLM.
- Iterative data augmentation process is used for quality improvement.

wiped or emptied – such as in an instance of cyber warfare. Another benefit is that, because application-based encryption encrypts the user content of files but retains the structure of the file itself, it can distinguish between application-based and malicious encryption.

To detect potentially nefarious activity, CyberSense looks at randomness of change to files, to build an entropy and similarity score that indicates the likelihood that the behavior indicates an attack. The tool has a 99.5% confidence in alerts, based on testing that Index Engines conducts in its labs. Index Engines has trained the CyberSense Machine Learning Model (MLM) based on datasets representing over 5,500 ransomware variants to date, with about 80 new variants being added each month.

The clean data vault copy can then be replicated back into production by the backup software, replacing the compromised copy. Optionally, data can be replicated and recovered to a PowerProtect DD system other than the one deployed in the Cyber Recovery vault, such as into a sandbox environment for forensics, and to confirm that the source of the malware has been eradicated before the suspicious data is recovered back into production.

As observed by Evaluator Group, users receive an alert in the Cyber Recovery UI and in email of potentially nefarious activity. The Lab Validation verified that usage reporting, including on suspect files and hosts is available, helps pinpoint attack vectors and impacted servers. There is also the ability to export system logs and event outputs for integration with Security Information and Event Management (SIEM) tools such as Splunk, which many larger enterprises are using for broader visibility and response to cyber-attacks, across their IT environments.

Summary

Customers have more options than ever before when it comes to data vaulting solutions. Managed offerings are of interest to a growing number of customers, as they seek to isolate a growing number of data copies for enhanced ransomware resiliency, but as they simultaneously struggle with staffing shortages. Dell PowerProtect Cyber Recovery covers a number of important checkboxes, including its ability to control replication processes and the vaulting window, role-based access to the vault environment, and the ability to recover to an alternate PowerProtect DD implementation as a sandbox environment for forensics and testing. Its deployment flexibility is a value-add, and its close integration of CyberSense is a notable differentiator.

About Evaluator Group

Evaluator Group LLC., an Information management and data storage analyst firm, has been covering systems for over 20 years. Executives and IT Managers rely upon us to help make informed decisions to architect and purchase systems supporting their data management objectives. We surpass the current technology landscape by defining requirements and providing an in-depth knowledge of the products as well as the intricacies that dictate long-term successful strategies.