Whitepaper

Best Practices and Day 2 Operations to Fortify Critical Data from Cyberattacks

Dell PowerProtect Cyber Recovery Best Practices and Day 2 Operations

Abstract

Dell PowerProtect Cyber Recovery is a secure data vaulting solution that protects and enables the recovery of an organization's most critical applications and data. The implementation and day-to-day operation of Cyber Recovery is flexible to meet both stringent and more flexible requirements.

This white paper discusses certain best practices and other considerations related to the day-to-day operation and maintenance ("Day 2 Operations") for the solution.

July 2022

Table of Contents

Introduction

The modern threat of cyberattacks and the importance of maintaining the confidentiality, availability and integrity of data require modern solutions and strategies to protect vital data and systems. Understanding the stakes involved in today's data-driven world, progressive organizations are adopting cyber resiliency strategies to identify, protect, detect, respond, and recover from ransomware and other cyberattacks. Achieving a cyber resiliency strategy, incorporates people, process and technology into a holistic framework that protects an entire organization or entity.

The Dell PowerProtect Cyber Recovery Solution (Cyber Recovery) is a powerful tool to enhance an organization's cyber resilience. By protecting critical applications and data in an isolated, immutable, and intelligent data vault, Cyber Recovery enables a safe and efficient recovery after a ransomware or destructive attack is successful.

Cyber Recovery is designed to run autonomously, based upon defined policies, in a physically and logically isolated environment. However, information provided by Cyber Recovery to the production environment should be monitored to validate proper operation and ensure that security remains intact. In addition, testing may need to be performed to comply with certain regulatory or organization-specific policies; and other maintenance and upgrades are required at certain intervals.

This white paper provides guidance and best practices to consider in related to these "Day 2" operations and ongoing maintenance and upgrading of Cyber Recovery.

Daily Tasks

Each policy configured in the Cyber Recovery console creates a job process – typically a “sync” plus a “copy”, “lock” and an optional “analyze” via CyberSense analytics. Normally these policies run run on a scheduled basis, as specified within Cyber Recovery. The normal interval for a policy is once each day, timed to begin after the related backup or other production process / copy has been completed. Policies can also be run manually via access to the Cyber Recovery console.

Policy monitoring. Upon the completion or failure of a job, Cyber Recovery logs the information to the internal console and sends a basic report via the SMTP server configured in the Cyber Recovery console. This information should be monitored or reviewed for the following issues:

- **Time to sync completion.** Syncs are based upon PowerProtect DD mTree replication, and as such involve the transfer only of data that has changed since the last sync. Organizations may desire to review the time for completion of the sync on a regular basis to determine whether any anomalies are occurring. For example:
    - Is the sync operation taking much longer than expected, perhaps meaning a larger amount of data is changing or portions of production have been encrypted (this will also be indicated by CyberSense if running for that specific job)
    - Is the sync operation taking much shorter, possibly meaning that data in production has been reduced. This could mean backup jobs are failing, data has been lost or deleted, etc.
- **Job failures.** If policy jobs are failing to complete, the reason should be investigated.

Target (Vault) Data Domain capacity monitoring. The standard best practice is to add capacity to a PowerProtect DD when it reaches 80% of capacity. Given lead times for planning, budgeting, ordering and implementation, the capacity of the vault PowerProtect DD(s) should be monitored on a regular basis. Currently, PowerProtect DD telemetry information can be securely sent from the vault if configured. Upcoming releases of Cyber Recovery will deliver more information about capacity for the PowerProtect DD targets.

Production based monitoring. It is a best practice to also monitor the completion of jobs that are writing data to the source mTrees in production. For example, if a backup job in production is failing or taking too much time, this may impact the proper completion of the vault-based policy job related to that production backup. Similarly, production exceptions impacting the sources of data for the vault should be monitored. This should include failed hosts, backup job warnings, client backup jobs not completing in expected timeframes, etc.

CyberSense. CyberSense provides the “intelligence” or analytics capability for data in the vault, delivering detailed information about whether data sets may have been corrupted. CyberSense is optionally configured to run within a policy, so it may not be running for all policies. Upon completion of its work, CyberSense registers detailed information to the CyberSense console in the vault and delivers a summary email and CSV attachment regarding its scan (per job) through the SMTP channel.

A “suspicious” alert from CyberSense should be handled immediately and carefully. Although false positives can occur, the CyberSense machine learning model is tuned to avoid these issues. Immediate information about the job, possible attack vector and other information is available in the messaging and CSV file and help to immediately begin the triage process. More information on CyberSense is available here.

Other vault components. Cyber Recovery can be configured with additional servers, networking, clean rooms, landing rooms, etc. Due to the vault's isolation, monitoring of these components would not necessarily integrate seamlessly with the production enterprise monitoring solution. Monitoring of individual components may be as simple as logging in to individual systems, or by configuring a centralized syslog repository within the vault. A data diode could potentially be used to securely send syslog messages from the vault to the production environment.

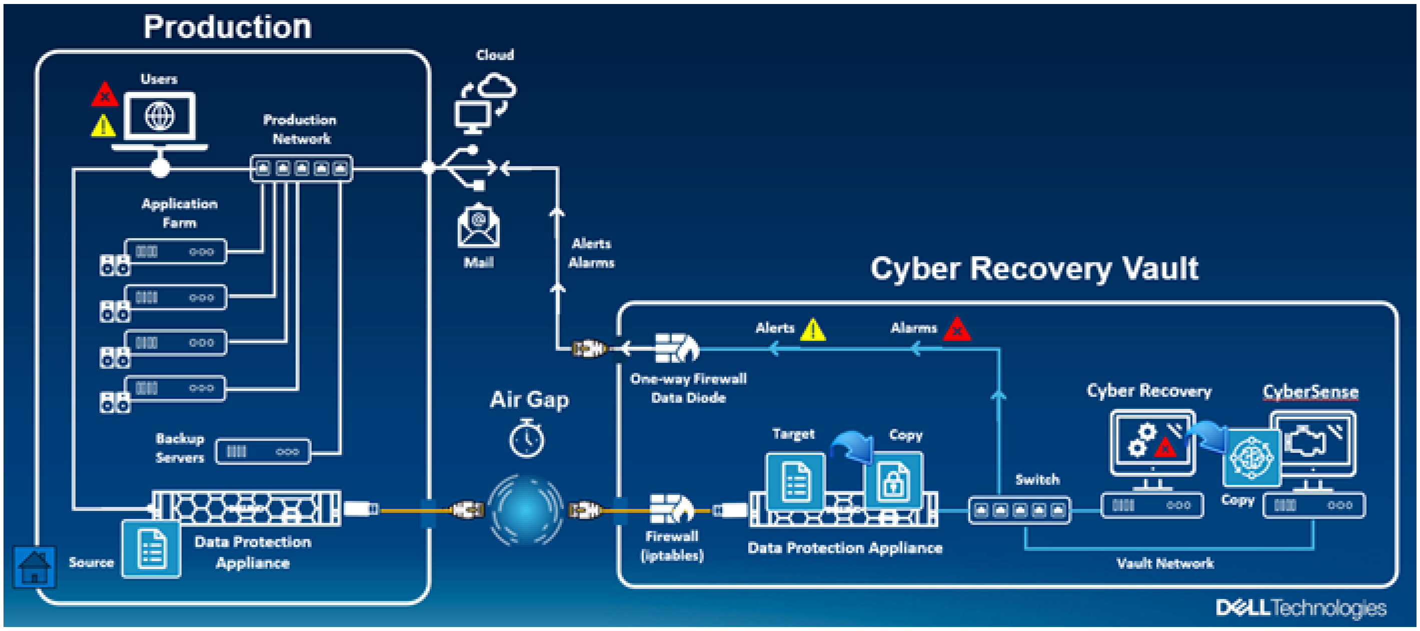
In addition to the PowerProtect DD, some of the components to consider monitoring include:

- Cyber Recovery server / host
- Cyber Sense Server(s)
- Jump Server
- ESXi infrastructure
- Network infrastructure (switches, diodes, firewalls, etc.)
- Compute for clean rooms, testing, etc.

Some of the issues to monitor include:

- System Availability
- Hardware Errors
- Capacity Thresholds
- CPU Thresholds
- Memory Thresholds

Below you will see some of the common components for Cyber Recovery that need to be managed and monitored. Alerts and alarms can be configured to help maintain efficient operations and management of the vault.



Weekly and Monthly Tasks

Patching and Upgrades. Just as in production, the compute, software and other components in the vault may have regular patches and upgrades that should be applied. Normally, patches do not have to be applied with the speed required in production due to the isolation of the vault. The following may require patching and upgrades, normally completed on a monthly or quarterly basis (depending upon organizational policies):

- Cyber Recovery software
- CyberSense software
- Firmware (compute, storage, switches, networking, firewall),
- OS upgrades
- Backup software (if present)

Process. The best practice recommendation is to designate a production mTree, with an associated policy in the vault, used only to stage patches and upgrades for transfer into the vault. When required, the production mTree can be temporarily mounted via CIFS or NFS, patches and upgrades copied to the mTree, and then the mount disabled. The associated policy in the vault can be run manually to securely copy that content into the vault environment. Upon completion, the mTree should be scanned by CyberSense. The hashes for each file should also be validated before application.

Hardening validation. It’s best practice to regularly validate the security configuration and validate that the required services are running properly:

- Services (if present)
  - **Active Directory.** Some implementations include a vault-only AD implementation for ease of operation (there is no link to production or other external source). AD should be validated to include only authorized accounts.
  - **DNS.** A base DNS implementation is optionally implemented for larger vault configurations (again with no linkage to production). This is less of a security concern, but the DNS should be validated to include only proper entries.

NTP. An NTP source is usually recommended for the vault although the stratum level and reliance on an external source can create security concerns. Regardless, NTP should be validated as working properly and securely, with time adjusted as needed if set to local / Stratum 0. Careful consideration should be taken if NTP time requires a change because it can impact PowerProtect DD's operation of compliance retention locking, particularly if the additional hardening capabilities have been applied (they may not accept any changes to NTP depending on the hardening level). Regardless of the source of time synchronization, the clocks of the vault components should be checked for synchronization with the proper source, as well as a sanity check that the time is reasonably accurate (i.e., within a few minutes of actual time). Any drift beyond a few minutes does not necessarily mean the vault will cease to function but should be investigated as to the cause of the drift and corrective action taken as appropriate.

Audit checks. Some organizations evaluate logging information contained within the vault for security and operational purposes.

Data Domain retention lock. Validate that the PowerProtect DD remains configured to operate at the desired retention lock level (Compliance v Governance v Hardened Compliance).

Policy validation. Policies are also a potential security concern and should be validated to match the agreed upon configuration. For example, an insider could maliciously or mistakenly:

- Change or delete the schedule for a policy (e.g., a policy schedule to run each day might be changed to run every 30 days)
- Modify the replication window for the completion of the sync process. Setting a short replication window and enabling enforcement of the windows could result in failed jobs. Conversely, disabling enforcement or lengthening windows could also result in undesirable behaviors.
- Change the level of retention locking in the policy. Note that this is a separate consideration from the retention lock configuration on the PowerProtect DD itself.
- Change the retention duration. Although this would not have an impact on data previously stored and retention locked, it would impact policies run after the change. An increase in retention could cause storage to reach capacity while a decrease could allow early deletion of data sets.

Performance and capacity Monitoring. As the data within a vault grows, it is necessary to ensure that the underlying infrastructure within the vault is suited to scale to the growth of data, and future requirements can be reasonably predicted. Additionally, having a good performance baseline (CPU, memory, disk, network usage) can help detect anomalies indicative of issues such as a software bug. A simple step such as tracking the time a CyberSense scan normally completes can provide valuable information regarding overall system performance. Similarly, tracking disk capacity over time can help determine if a filesystem has been growing steadliy over a longer period of time as opposed to an unexplained overnight jump in utilization.

Additional Tasks

There are a variety of other operations that an organization may need or require.

Recovery testing. Many organizations are required to test recovery capabilities on a regular basis. This testing can take many forms and must meet organizational requirements. The following is provided for illustration and example purposes:

- **Single application or component (e.g., a database) recovery.** This testing can be performed with the following basic steps:
    - Recover backup software instance in-vault, with backup catalog corresponding to selected date / dataset
    - Recover backup contents to sandbox area (this should be a small dataset representative of the data in the vault)
    - Isolate sandbox area
    - Perform application validation
    - Clean-up
- **Backup catalog recovery.** This is a simplified version of the process above, ending with the first step (recovery only to backup catalog)
- **Table top.** Many organizations run table top recoveries, with key constituents and interested parties discussing the recovery process without accessing the vault (i.e. in a conference room or call). This can assist in improving lines of communication and responsibility but is not as effective as a “hands-on” exercise and may be used in coordination with other testing.

Password changes. Passwords can be required to change on a regular basis, usually in keeping with the organization’s security policies. However, the time for changes might be extended based upon an understanding of the isolation and the “cost” of accessing the vault to make the changes on a regular basis. Separate consideration should be given if an employee with access to or credentials within the vault has a role change or leaves the organization.

Organizational audit. Many organizations protect only their critical applications and related data in the vault. As the business changes, the criticality of existing and perhaps new applications may also change. Care should be given to review these concerns on a regular basis. Policies may need to be modified to ingest additional content, modify retention periods or incorporate additional testing capabilities.

Physical locks / logs. Physical security concerns, including (where appliable) keys, locks, biometrics, written and electronic access logs, etc. should be monitored and checked on a regular basis consistent with the organization’s security requirements.

Capacity planning. Organizations must plan for infrastructure and data growth. As critical data increases or expands across distributed infrastructures, thresholds of the current deployment could be exceeded. Exceeding the thresholds could require additional vaults, cyber recovery management software and PowerProtect DD’s.

Vault hardening. Periodically, the vault's hardening configuration should be reviewed for:

- Configuration has not drifted from the original configuration
- Any new best practices for hardening should be implemented
- Hardening review should be inclusive of all vault components, including:
    - Validate PowerProtect DD side hardening, e.g., locking down replication, etc.
    - Network components
    - Jumpbox
    - CR Server
    - CS Servers
    - ESXi infrastructure
    - Physical components (i.e., nobody has improperly or mistakenly cabled something into the vault)

Information Management. In the event of a compromise of the production environment, knowledge of the location of critical data in the vault, along with procedures covering the process of recovering from a compromise, are essential.

Mtree contents. Particularly in a multi-Mtree environment, the contents of each Mtree should be known and available offline. As changes are made to the production environment, those changes which impact the location of critical backup data should be recorded. Documentation / Runbooks. As changes are made to production environment it is important to ensure recovery documentation is up-to-date, readily accessible, and the right personnel know where to find this information.

Conclusion

In the rapidly evolving threat landscape, organizations are looking for effective recovery strategies to maintain cyber resilience. Dell PowerProtect Cyber Recovery provides an effective recovery solution to resume normal business operations in case of a cyberattack. Utilizing best practices for day-to-day operations to maintain the protection of critical data will allow for the most confident and efficient recovery from a cyberattack. Whether a simple deployment or one more advanced, cyber resilience can be achieved with Dell PowerProtect Cyber Recovery.

Learn more about
Dell PowerProtect
Cyber Recovery

Contact a
Dell Technologies Expert

View more
Security Solutions
Resources

Join the conversation
with #PowerProtect