DELL Technologies

Whitepaper

Recover Your Critical Data in Case of Cyberattack

Recovering from a Cyber Event

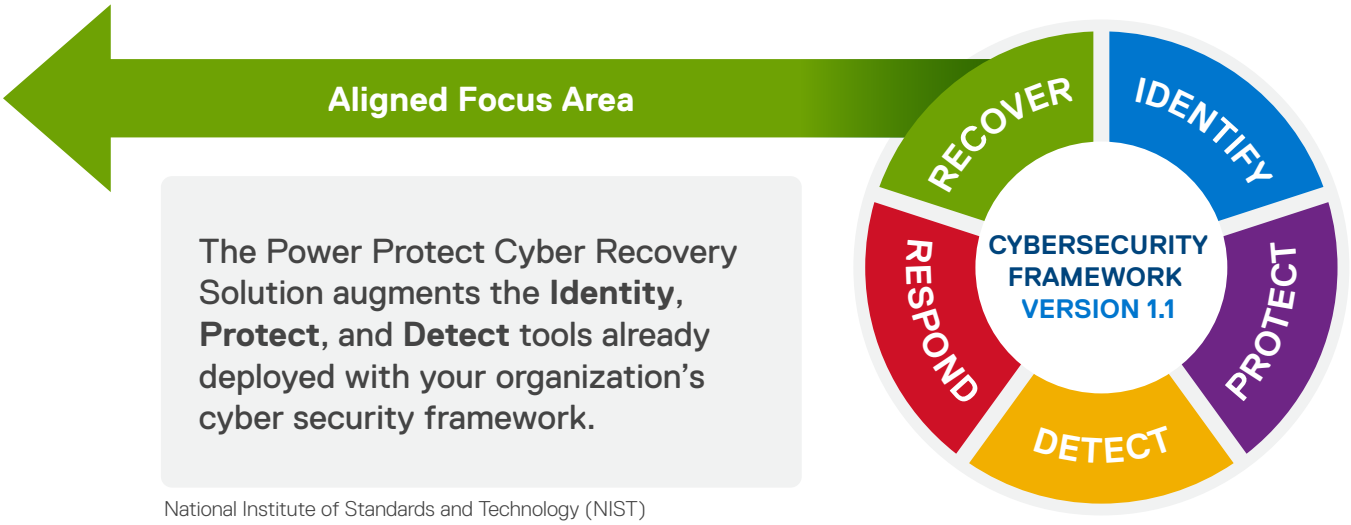
Leverage Dell PowerProtect Cyber Recovery to Recover from a Cyber Event

Obviously, there are many factors that come into play to determine the best recovery option(s) for each event. When faced with an attack, recovery option flexibility is paramount. It is also very important to remember that active cyber resilience measures available to the incident response team, and the applications affected by the attack will drive the Incident Response Team (IRT) to select the most appropriate recovery plan. This white paper will focus on how PowerProtect Cyber Recovery enables the different recovery paths as well as the usefulness and indications of each recovery path option. Additionally, this paper will also document the steps in determining root cause and cleansing, how the "blast radius" may drive your recovery options and why a clean room/landing zone may be important.

July 2022

Table of Contents

The NIST Cybersecurity Framework



The Power Protect Cyber Recovery Solution augments the **Identity**, **Protect**, and **Detect** tools already deployed with your organization's cyber security framework.

National Institute of Standards and Technology (NIST)

The modern threat of cyberattacks require modern solutions and strategies to protect vital data, systems, and infrastructure. Relying on traditional data protection methods, workflows, and technologies to ensure the confidentiality, availability, and integrity of data has proved costly for many organizations. Beginning with the watershed event in 2015 when Sony Pictures was attacked by North Korea the stakes changed drastically. Gone was the reliance on the venerable 3:2:1 data protection model (3 copies, 2 media types, 1 copy off site) to protect our critical data from any event. Understanding the stakes in today's data driven world is paramount.

Organizations today rely on the adoption of the NIST Cybersecurity Framework to increase resilience. Resilience strategies to identify, protect, detect, respond, and recover from ransomware and cyberattacks. Achieving a resilience strategy requires defense in depth, and incorporates people, process and technology into a holistic framework that will protect the entire organization.

Ensuring cyber resiliency requires a data vault that incorporates 3 major elements:

1. **Isolation** - the components of the data vault must be physically and logically isolated. Logical isolation has similarities to an air-gapped network, except that limited connectivity for replication of data into the vault.
2. **Immutability** - all data written to the data vault must be secured in a manner that electronically prohibits deletion or modification until the expiration of the retention period, which is typically a couple of weeks to a month. At a minimum, the overall requirements of immutability should block administrative overrides, or any virtual based or software defined components that can be destroyed with administrative credentials.
3. **Intelligence** - data in the vault should be analyzed or interrogated in a manner that ensures the data has not been manipulated or corrupted. While the focus of isolation and immutability is to protect anything that goes into the vault, Intelligence validates that the data in the vault is not corrupt.

Dell PowerProtect Cyber Recovery provides the highest level of protection, integrity, and confidentiality for your most valuable data. This assurance will allow organizations to quickly recover their most valuable data and systems after a cyber event and resume normal operations.

The ultimate goal of the Dell PowerProtect Cyber Recovery solution is to provide an organization with the quickest and most reliable path to recovery of business-critical data and systems. Therefore, it is critical to establish a cyber-attack recovery plan.

Responding to an Incident

At a high level these are the steps that need to be taken after the invoking of an incident response.

1. Preparation

a. Training

b. Develop business impact analysis

c. Run books

2. Declaration of Event

a. Incident Response plan

i. Act

ii. Plan

iii. Check

iv. Do

3. Identification/ Detection

a. Analytics

b. Forensics

c. Damage Assessment

d. Reporting

4. Mitigation/Remediation

a. Containment

b. Eradication

5. Recovery

a. Determine the most appropriate recovery technique based on confidence of data integrity and prioritize sequence. It is important to note that cyber restore and cyber recovery are not the same. Cyber restore does not rebuild a service, it simply restores data to existing infrastructure. Cyber recovery includes the rebuilding of a service and all the required underlying components and dependencies invoking the correct people, process, and technology.

i. Restore

ii. Repair

iii. Rebuild

iv. Recover

6. Post Incident Activity/Lessons Learned

Please reference the NIST Incident Response Checklist found in NIST.SP.800-61r2 for more detailed information on their guidance.

NIST Incident Response Checklist

1. Determine whether an incident has occurred

1. Analyze the precursors and indicators
2. Look for correlating information
3. Perform Research
4. As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence

2. Prioritize handling the incident based on relevant factors (functional impact, information impact, recoverability effort, etc.)

3. Report the incident to the appropriate personnel and external organizations

4. Acquire, preserve, secure, and document evidence

5. Contain the incident

6. Eradicate the incident

1. Identify and mitigate all vulnerabilities that were exploited
2. Remove malware, inappropriate materials, and other components
3. If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps to identify all other affected hosts, then contain and eradicate them

7. Recover from incident

1. Return affected systems to an operationally ready state
2. Confirm the affected systems are functioning normally
3. If necessary, implement additional monitoring to look for future related activity

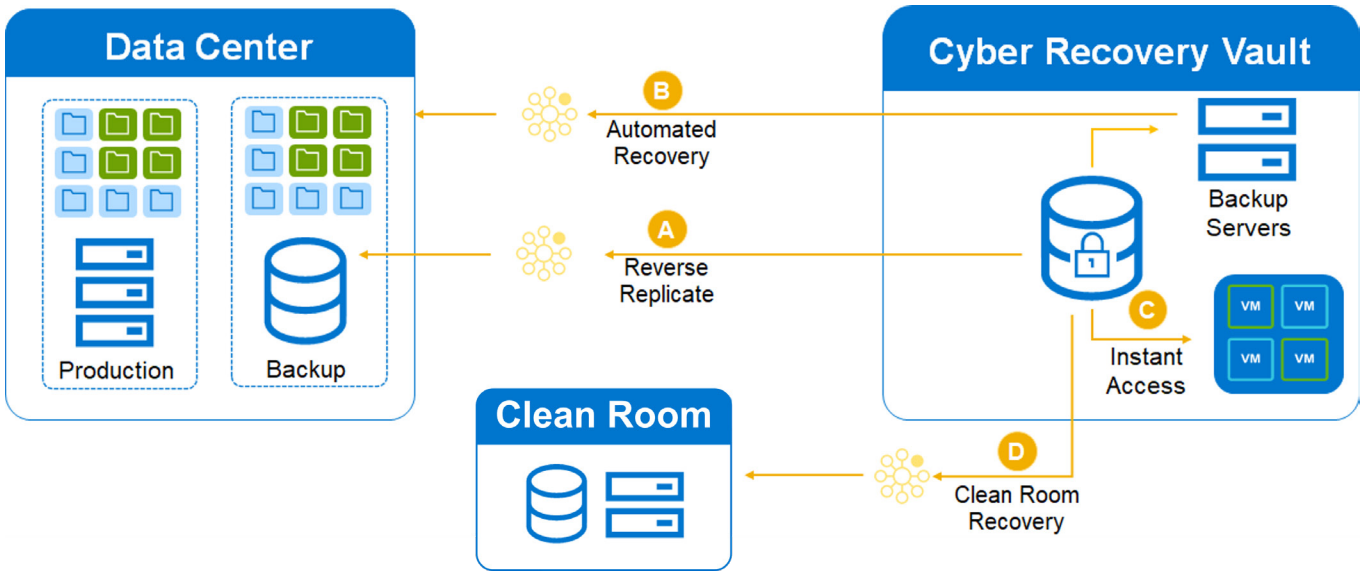
8. Create follow up report to summarize:

1. Threat and Risk
2. Investigate steps taken
3. Containment steps
4. Eradication steps

9. Hold a lessons learned meeting

1. Identifying where mistakes have been made for continuous improvement
2. Understand where problems occurred so that you can fill the voids
3. Recognize the success of what went well and what was effective
4. Retain organizational knowledge to understand the good, the bad and the ugly
5. Reduce future risk by keeping similar mistakes from happening
6. Improve future performance to be prepared for next attack

Recovery Methodology with PowerProtect Cyber Recovery



Automated Workflow

1. In the Cyber Recovery Vault, there will be multiple backup copies on the PowerProtect DD which you can chose from to restores your critical data.
2. Based on the assessment of the attack a backup catalog can either be restored fully, partially or imported.
3. Once the production environment is cleansed and validated the production environment can be brought back on-line or alternatively a limited subset of infrastructure to support hyper critical applications can be brought on-line.
4. Once the previous step is complete and there is compute, storage, and networking in place to restore to you have several recovery options based on the components deployed in the vault. See number 10 below.
5. Identify the restore points that were created before the attack occurred.
6. Using forensic findings, identify the malware or corrupt data and where it has been persisted.
7. Restore data and binaries as required. If binaries or OS images have been compromised, a decision as to whether to cleanse needs to be made.
8. Connect the vault to the production network by creating a temporary recovery path by connecting the backup infrastructure in the vault to the production network.
9. Determine the most appropriate recovery technique based on findings from analytics, forensics, damage assessments and reporting.
    a. **Reverse Replication** - This is the simplest, most straightforward recovery process. This entails recovering a complete known good backup and then restore the application from it. Workflow- Vault DD series to Production DD series then normal recovery process using your backup software. *This option is suggested for users who want to restore a complete known good backup and then restore the application data from it.*
    b. **A utomated Recovery** - allows you to recover directly from the vault backup server rather than moving everything to the backup server in the production environment. It requires the deployment of a backup server in the vault. The backup server in the vault would access data on the vault DD series to allow for dataset recovery directly to the production environment (please note, this option will also require the creation of network connectivity). *This option is most effective for organizations who want the ability to perform a complete recovery or selective recovery.*

c. **Instant Access** - Instant Access can be used as the sole recovery process or as a component of a larger recovery process. This option takes advantage of the PowerProtect DD instant access capability. VMs can instantly be brought up and used for testing, or you can use it the newly spun up VMs for production via vMotion. *This option is for organizations who want instantaneous access to the Virtual Machines.*

d. **Clean Room** - Clean Rooms are primarily used for testing, data sanitization, validation, and application recovery to expedite the recovery process.

   i. Option 1 - In this scenario, the clean room infrastructure would be sized to the largest application. Once the integrity of data is assured, you can recover from the clean room directly back to the production environment and then move on to the next application. This represents the most common process in which the incident response teams can ensure all data is clean before it is recovered back into production.

   ii. Option 2 - This option is used by organizations who want to recover application(s) and make them accessible right away. In this scenario, you would recover your application to the clean room and then run the application out of the clean room as though it was in the production environment.

10. Recovery Variations

    a. Bare Metal Recovery - A backup master server in the vault leverages the backup bare metal recovery functionality to recover physical clients thus making it unnecessary to reinstall operation system or configure hardware manually.

    b. Database Recovery - Native database utilities in production environment are used to trigger restores for database clients. Either DD Boost or CIFS/NFS can be used for a targeted restore.

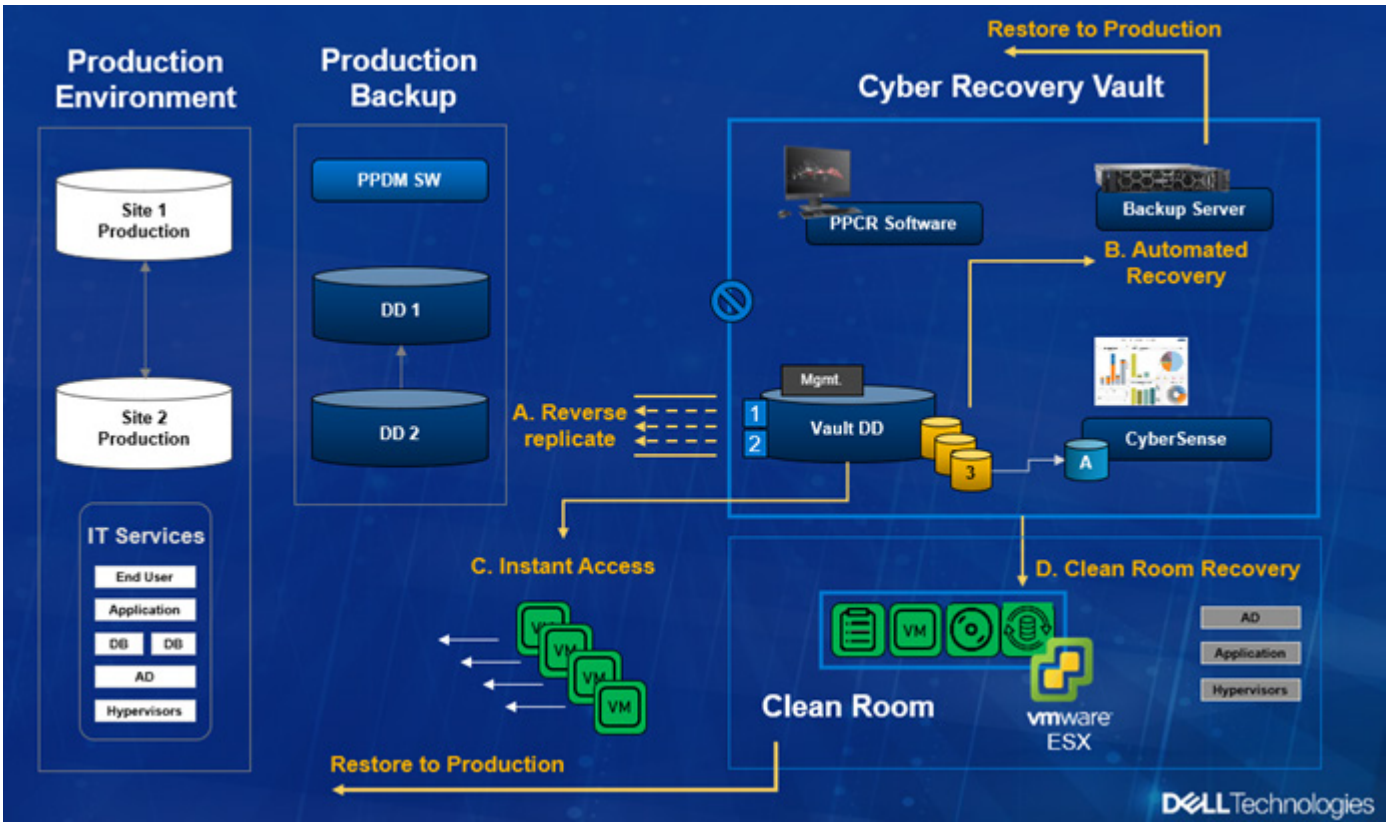
11. Resume Normal Operations. Once the critical applications have been re-established, the temporary recovery path can be disconnected. Ensure that all vault components are in place to resume normal daily vaulting operations.

Clean Room Use Case

Be aware that there will always be a window where the victim's cyber team and perhaps insurers and legal teams are going to limit access to the affected servers and assets. During this window they will take forensic images as they determine root cause. As noted previously, the NIST recovery guidelines are more specific and state recovery should not begin until there is an understanding of what happened and "high confidence" in understanding and eliminating any persistence or confirming non-persistence. Therefore, the reality is a locked-out period based upon the scope of the attack will need to be factored into any runbook or recovery plan.

The primary use case of a clean room is to decrease or eliminate down time even during a locked-out period. Best practice related to clean rooms is to begin at the business level. Identify and rank the critical services that are most important based on revenue, reputation, safety, ecosystem, etc. Then determine the downtime tolerances for those services. From the services that must be up within x window (when existing infrastructure is unlikely to be available), you will map those to the IT components (apps, databases, dependencies, etc.) and determine sizing and other requirements. Determining down time tolerances is a lot of work but must be defined based on each service, application, or database.

The picture below gives another view of the Cyber Recovery vault and the recovery options including a clean room.

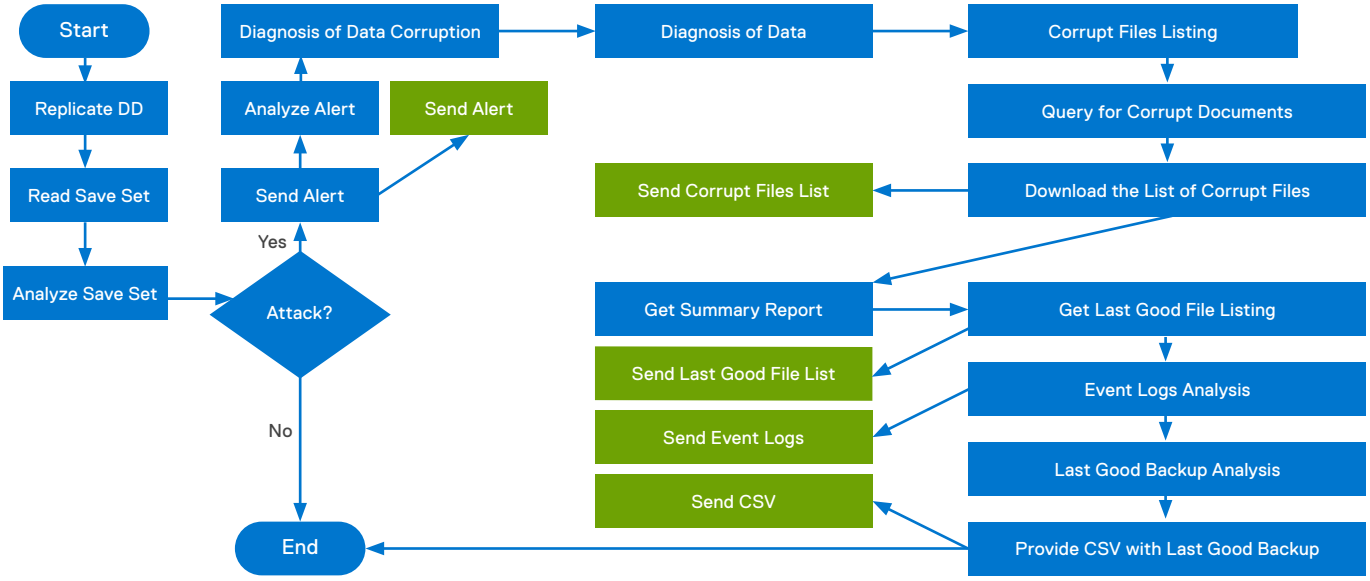


Sample Incident Response Workflow

Process Step Description	Application	Description
Start		
Replicate DD Series	Cyber Recovery Manager	The sync function replicates the backup data from the production environment DD series to the DD series in the vault.
Read Save Set	CyberSense	CyberSense reads new data content that has been replicated into the vault
Analyze Save Set	CyberSense	CyberSense provides two distinct capabilities: 1. CyberSense audits the data managed by Cyber Recovery to detect signs of corruption due to trojans and ransomware. Cyber Sense does this through it use of analytics and machine learning. When CyberSense detects any sign of corruption, it delivers an alert to the Cyber recovery dashboard. 2. When data is corrupted due to a cyberattack, CyberSense provides a number of post-attack forensic reports for diagnosis and recovery from the attack.
Attack Vector Found	CyberSense	CyberSense alerts appear as critical alerts in the Cyber Recovery Dashboard.
Send email alert	SMTP	The email includes an attached text file. The text file contains a full listing of all the statistics generated by CyberSense analytics. Also included is information on the specific attack vector that was detected.
Analyze Alert Mail	Human	If email alerts are enabled, CyberSense send an email alert stating that an infected backup set was detected. The email includes an attached text file. The text file contains a full listing of all the statistics generated by the CyberSense analytics. Also included is information on the specific attack vector that was detected.
Diagnosis of Data Corruption	CyberSense	CyberSense includes a number of reports that help in the diagnosis and recovery from a cyberattack. These reports are available through the CyberSense user interface. Once an alert is detected, the user can leverage the information to determine the steps for a recovery plan.
Corrupt Files Listing	CyberSense	A complete listing of likely corrupt files is displayed
Download the list of corrupt files	CyberSense	Download the complete listing of likely corrupt files.
Get summary reports	CyberSense	You can choose from a standard summary report for more detailed forensic analysis.
Investigate suspect files	CyberSense	Suspect files are provided to the forensics team for further investigation
Event logs Analysis	CyberSense	CyberSense provides event logs that indicate the last user account that modified a file as well as the executable that was used. For example, if 1,000 files were encrypted, 3rd party event log tools could determine which user account was utilized for the encryption and could identify the malware that was employed.
Send Event logs to the Incident Response Team	Human	Send the event logs to the IRT
Last Good backup copy analysis	CyberSense	CyberSense can report on the last good backup set. These backup sets can exist on several different incremental backups that were runover a period of time. CyberSense identifies the last good backup set based on analytics and machine learning. This good backup set will have no signs of corruption.
Provide CSV with last good backup sets to restore team	Human	Create a CSV file from the last good backup set analysis report to be viewed by the recovery team.
Send last good backup list to Incident Response Team	Human	Send the list of backup sets to the IRT
END		

How an Attack is Determined

Below is the workflow of how Cyber Recovery determines if an attack has occurred and what data to restore.



Post Event, What next?

After an event, you will need:

1. A clear description of the suspected attack vector
2. A process to determine the validity of the attack by verifying the alert was not a false positive
3. An estimate to the damage done by the attack
4. The listing of compromised hosts
5. Location and listing of last recoverable full backup for each of the compromised hosts

Determination of Root Cause

The PowerProtect Cyber Recovery Solution provides 4 mechanisms for being alerted:

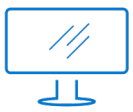
1. Cyber Recovery GUI
2. CyberSense Dashboard
3. Emailed alerts
4. Syslog Integration

Comprehensive indexing and security analytics provide critical information such as:

1. Who was impacted?
2. How much damage was done?
3. What was attacked?
4. Where is the source?
5. Listing of corrupt files
6. What user account was used?
7. When did the attack begin?
8. What backup sets contain the last known good copy of data?

Conclusion

Dell PowerProtect Cyber Recovery provides the industry's most effective recovery solution against common and advanced attack vectors, including dormant malware, data wiping and locking, data corruption, insider attacks, and the destruction of backup and storage assets. It provides your organization the assurance that you can quickly and confidently recover your most critical data and systems after a cyberattack and resume normal operations.



Learn more about Dell PowerProtect Cyber Recovery

Contact a Dell Technologies Expert

Demo Dell PowerProtect Cyber Recovery

Join the conversation with #PowerProtect