DELL Technologies

Technical Whitepaper

Recovering from a Destructive Cyber Attack

Leveraging Dell PowerProtect Cyber Recovery to Recover the Lifeline of Your Business

Abstract

Cyberattacks are on the rise, and they are growing more sophisticated and devastating every day. In fact, $6 trillion is the estimated global impact of cyber crime in 2021[1]. Ransomware attacks not only cost organizations millions of dollars in lost revenue per day, they also inflict damage to reputation and negatively impact stock prices. Cyber threats are expected to continue to increase, especially as a result of working from home and distributed work environments.

Most organizations have strong data protection and detection capabilities in place already. But, could your organization recover if an attacker gets through the perimeter and encrypts or wipes your data? Additionally, how confident would you be in the integrity of that data that you were able to recover? Organizations need to consider recovery as part of their cyber resiliency and risk management strategies. This white paper highlights how Dell PowerProtect Cyber Recovery protects and isolates critical data from ransomware and other sophisticated threats.

February, 2022

[1] Cybersecurity Ventures: https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021

Table of contents

Executive Summary 3

Dell Cyber Recovery Overview 4

Use Case 1: Large Financial Institution 5

Use Case 2: School District 6

Use Case 3: Large State Government 6

Dell PowerProtect Cyber Recovery Details 7

Technology Components 7

Automated Workflow 7

Analytics In The Vault 9

Recovery Procedures 10

Scenario C: Reverse Replicate 11

Scenario D: Automated Recovery 11

Scenario C: Instant Access 12

Scenario D: Clean Room 12

Conclusion 12

Executive Summary

Across industries and among organizations of every size, cyberattacks are on the rise, in fact, Cyber Security Ventures estimates that every 11 seconds a cyber or ransomware attack occurs.[1] Attacks are virtually non-stop and the cost per attack continues to increase, with Accenture estimating that $13 million is the average cost to organizations resulting from cyber crime.[2] As organizations become increasingly aware of the cybersecurity risks that threaten their mission-critical operations as well as their reputation, IT security has become an essential part of enterprise digital strategy.

Protecting your organization starts with protecting your data — against ransomware and other sophisticated cyber threats. Yet, cyber threats are becoming more sophisticated, presenting ample opportunity for criminals using modern tools and tactics to leverage your critical data for a variety of purposes or destroy and ransom it for some agenda or benefit — and 64% of organizations are concerned that they will experience a disruptive event in the next twelve months.[3]

With cyber security, it's not a matter of "if" but "when" you will be faced with such an attack. In the wake of the most sophisticated cyber threats, rather than focusing on preventing ransomware or cyber attacks, organizations should focus on protecting critical data or apps that enable you to recover your critical assets with integrity so you can resume normal business operations with confidence. Yet, many organizations lack confidence in their data protection solutions, specifically the Global Data Protection Index reported that 67% of IT decision makers are not very confident that all business critical data can be recovered in the event of a destructive cyber attack[3].

The modern threat of cyber attacks 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 business, organization, or entity.

Having a Cyber Resiliency strategy is a mandate for all organizations and government leaders and can be seen as a competitive advantage in today's data-driven world. Ensuring cyber resiliency requires multiple layers of protection to ensure that critical data is protected and isolated from these attack surfaces so that it can be quickly recovered with confidence following a ransomware attack, to accelerate the restoration of the normal business operations.

Dell PowerProtect Cyber Recovery provides the highest levels of protection, integrity and confidentiality for your most valuable data and critical business systems and are a critical component of a comprehensive Cyber Resiliency strategy. This assurance that you can quickly recover your most critical data and systems after a cyber or other disruptive event is a critical step in resuming normal business operations. A modern and powerful cyber resilience strategy and Dell Data Protection are key to enabling our customers to increase business agility, accelerate time to market, improve their cloud economics, and reduce business risk.

[1]Cybersecurity Ventures: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021

[2]Accenture Insights, Ninth Annual Cost of Cyber crime Study March, 2019: https://www.accenture.com/us-en/insights/security/cost-cybercrime-study

[3]Gartner "Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware" report, January 2021: https://www.gartner.com/doc/reprints?id=1-25T81BQP&ct=210416&st=sb

Dell PowerProtect Cyber Recovery Overview

A robust and comprehensive cyber resiliency strategy should leverage frameworks like the National Institute of Standards and Technology (NIST Cybersecurity Framework (CSF)), which can help outline an end-to-end cyber-attack defense continuum. In short, Cyber Resiliency is a strategy that incorporates people, process and technology into a holistic framework that protects an entire business, organization or entity. This strategy allows you to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents. In our digital world with its reliance on data and real-time access on any device from any location it is more and more difficult to be resilient based upon non-technology capabilities.

PowerProtect Cyber Recovery is a component of an overall cyber resilience strategy. PowerProtect Cyber Recovery distinguishes itself from traditional backup and disaster recovery by providing additional layers of physical and logical security at both the solution, system and data/file level. This ensures critical data can be preserved with integrity, confidentiality and to ensure it is available when needed for recovery. PowerProtect Cyber Recovery is focused upon protecting critical data from cyber threats and away from the attack surface—and then recovering that data from an isolated environment when and if necessary.

PowerProtect Cyber Recovery focuses on protecting your critical data and recovering your businesses following a successful cyber attack or ransomware incident, while leveraging a combination of professional services and technology that provide the following three key elements of a Cyber Recovery solution:

1. **ISOLATION**—Gartner recently recommended that organizations who are looking to protect themselves from ransomware need to create an isolated recovery environment[1]. PowerProtect Cyber Recovery provides a physically and logically isolated data center environment that is disconnected from corporate and backup networks and restricted from users who don't have the proper clearance. Automated workflows securely move business critical data to an isolated environment via an operational air gap. You can also create protection policies in less than 5 steps and monitor potential threats in real time with an intuitive dashboard. The vault is ideally operated in a physically restricted area, such as a cage or locked room, that helps to guard against an insider threat. When the air gap is an a "locked" state—no data can flow—there is no access to any part of the solution. When unlocked, which is done to update or "sync" data, the operation is controlled from the secure, vaulted side, not from production. And during this phase the vault maintains a very secure profile. Only network traffic representing replication data is allowed and there is never access to other vault components or to the management plane of the storage or solution. So bad actors can't wait for the vault to unlock and then just drive in.

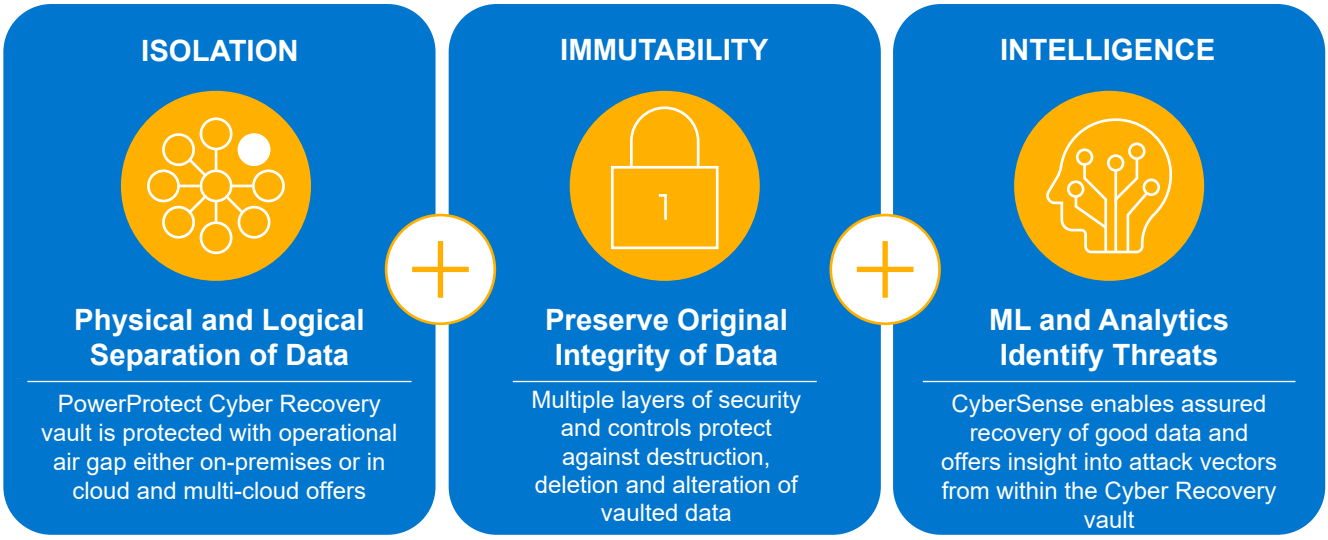
2. **IMMUTABILITY—**PowerProtect Cyber Recovery offers an automated data copy and air gap, which creates unchangeable data copies in a secure digital vault and processes that create an operational air gap between the production /backup environment and the vault. Using the Compliance Mode Retention Lock capability from Dell PowerProtect DD, data is prevented from deletion or change for a set time period. The lock cannot be overridden, even by an administrator with full privileges. PowerProtect DD offers unique enhancements that further secure the lock from an attack on the clock (or NTP server), which might otherwise allow a bad actor to create an early expiration of the lock. Those who do not want or require such a strong control, or want operational flexibility, can configure governance retention lock (which is also the available mode on our PowerProtect DD Virtual Edition (DDVE)).

3. **INTELLIGENCE**—CyberSense allows you to stay ahead of the rapidly changing threat landscape and sophisticated cyber criminals with CyberSense adaptive analytics, machine learning (ML) and forensic tools to detect, diagnose and accelerate data recovery within the security of the Cyber Recovery vault. CyberSense is fully integrated with PowerProtect Cyber Recovery and monitors files and databases to determine if an attack has occurred by analyzing the data's integrity. Once data is replicated to the Cyber Recovery vault and retention lock is applied, CyberSense automatically scans the backup data, creating point-in-time observations of files, databases, and core infrastructure. These observations enable CyberSense to track how files change over time and uncover even the most advanced type of attack. Automated integrity checks to determine whether data has been impacted by malware and tools to support remediation if needed.

[1]Gartner: "Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware": https://www.gartner.com/doc/reprints?id=1-25T81BQP&ct=210416&st=sb"

PowerProtect Cyber Recovery Advantages

Modern protection for critical data and an enabler of Security Transformation



PowerProtect Cyber Recovery provides an effective strategy against destructive cyberattacks, but it is not designed to be equally effective across all of them.

Often, the above mentioned attack vectors occur in combination. In the following sections, some of the more prominent attacks are described across three use cases.

USE CASE 1: **Large Financial Institution**

Challenges: Founders Federal Credit Union is a regional financial institution operating in North Carolina and South Carolina, with roughly $3.5 billion in assets and over 250,000 members. In an industry targeted by ever more sophisticated ransomware attacks, Founders Federal Credit Union needed an air-gapped cyber security resiliency with AI, machine learning and automation that would integrate seamlessly with their IT environment and allow them to expand business in a highly competitive regional banking market. Data protection and data integrity are a cornerstone of Founders' customer promise, so they needed a solution that provides fast, reliable and secure services on any device.

OUTCOMES: PowerProtect Cyber Recovery provides Founders Federal Credit Union with a true air-gapped solution, securing more than 10 PB of data in an isolated cyber vault. PowerProtect Cyber Recovery automates the backup, recovery and analytics workflows in addition to all cyber security reporting. In the event of a cyberattack, CyberSense analytics within the Cyber Recovery vault identifies known good copies of data, giving Founders Federal confidence knowing they can recover and resume business operations. Cyber Recovery gives Founders Federal peace of mind, according to Bob Bender Chief Technology Officer, Founders Federal Credit Union: "I sleep better at night, with over three years of experience with the PowerProtect Cyber Recovery solution". Read customer case study

USE CASE 2: **School District**

Challenges: When neighboring school districts were hit with cyberattacks, the technology leaders at Moreno Valley Unified School District knew they needed to upgrade their data protection and cyber resiliency. Moreno Valley needed to secure their student, employee and financial data, while still enabling teachers and administrators to be adaptable, collaborative and creative. Their prior data protection solution lacked analytic capabilities that would allow them to monitor the integrity of the data that they were protecting. They also needed a solution that would allow them to recover business operations quickly to maintain the critical educational services to their community.

OUTCOMES: Moreno Valley always believed in making sure that they were protected through different layers such as a firewall and a backup, but they didn't have a solution that put it all together like PowerProtect Cyber Recovery. The isolated air-gapped Cyber Recovery vault provides additional layers of security and protection for their critical data and gives Moreno Valley peace of mind that their PII data is safe and recoverable in event of a cyberattack. A 100x average daily compression rate allowed more data to be stored and protected and CyberSense provides active cyber threat analysis and alerts allowing them to easily monitor the Cyber Recovery vault to ensure data integrity. "With CyberSense, we're no longer the low-hanging fruit that can be easily picked off by bad actors", according to Glenn Alegre Executive Director of Technology, Innovation and Assessment, Moreno Valley Unified School District. Read the customer case study to learn how PowerProtect Cyber Recovery gave them peace of mind that student, employee and financial data are safe and recoverable.

USE CASE 3: **Large State Government**

Challenges: The unique circumstances of 2020 made IT transformation a must for the State of Oklahoma, with over 2.6 PB of critical data from state services and databases such as public safety information, DHS information, ODOT, and more needing modern cyber protection. These critical services can't afford to be down, or they could be facing a state government shutdown. As a result, they needed a reliable solution that ensured data availability and safeguards their data from threats such as cyberattacks. Their previous solution for restoring data was very manually intensive and didn't provide the confidence they needed.

OUTCOMES: The State of Oklahoma has embarked on a digital transformation journey that provides some immediate answers. Under the direction of their governor, the state modernized their IT processes and infrastructure, choosing PowerProtect Cyber Recovery to protect their critical data. PowerProtect Cyber Recovery provides them peace of mind that the state is able to recover from and withstand global cyberattacks such as ransomware, DDoS and defacement, among others. In fact, PowerProtect Cyber Recovery allowed the State of Oklahoma to withstand 3.8 trillion cyberattacks since January 2021. According to Steven Harpe, Chief Operating Officer, State of Oklahoma: "Cyber Recovery gives us peace of mind that we're able to recover from attacks. It's a layered approach that has absolutely been key." Read the case study

Dell PowerProtect Cyber Recovery Details

Dell PowerProtect Cyber Recovery provides management tools and the technology that performs the actual data recovery. It automates the creation of the restore points that are leveraged for recovery or security analytics. Dell Implementation Services are required for Cyber Recovery Vault design and implementation. Dell Advisory Services are recommended for designing an effective recovery strategy.

Technology Components

Organizations can dramatically reduce their surface of attack from inside and outside threats by removing the cyber-attack recovery environment from the production network. The only required connection is a data path for periodically synchronizing the data. To further reduce the surface of attack, this data link is only brought online for data synchronization. This logical air gap provides another layer of defense by reducing the surface of attack. PowerProtect Cyber Recovery protects the most critical data in a vault environment. The vault is ideally physically isolated — in a locked cage or room — and is always logically isolated via an operational air gap. The vault components are never accessible from production, and access to the vault target — when the air gap is unlocked — is extremely limited. Compute is needed inside the Cyber Recovery Vault to perform system management, infrastructure services, backup application, on-demand security analytics, and recovery testing. The required level of compute depends on the level of recovery testing an organization wants to achieve inside the Cyber Recovery Vault.

A hyper-converged appliance or a small ESX cluster with virtual SAN can be an effective and economical strategy for maintaining an environment within the Cyber Recovery Vault. The management host is required because it runs the tools to orchestrate the workflow as described in the next section. Additional compute for periodic analytics and data validation is recommended. Sizing is driven by the data to be analyzed, the analytics tools used, and frequency of validation and test.

Automated Workflow

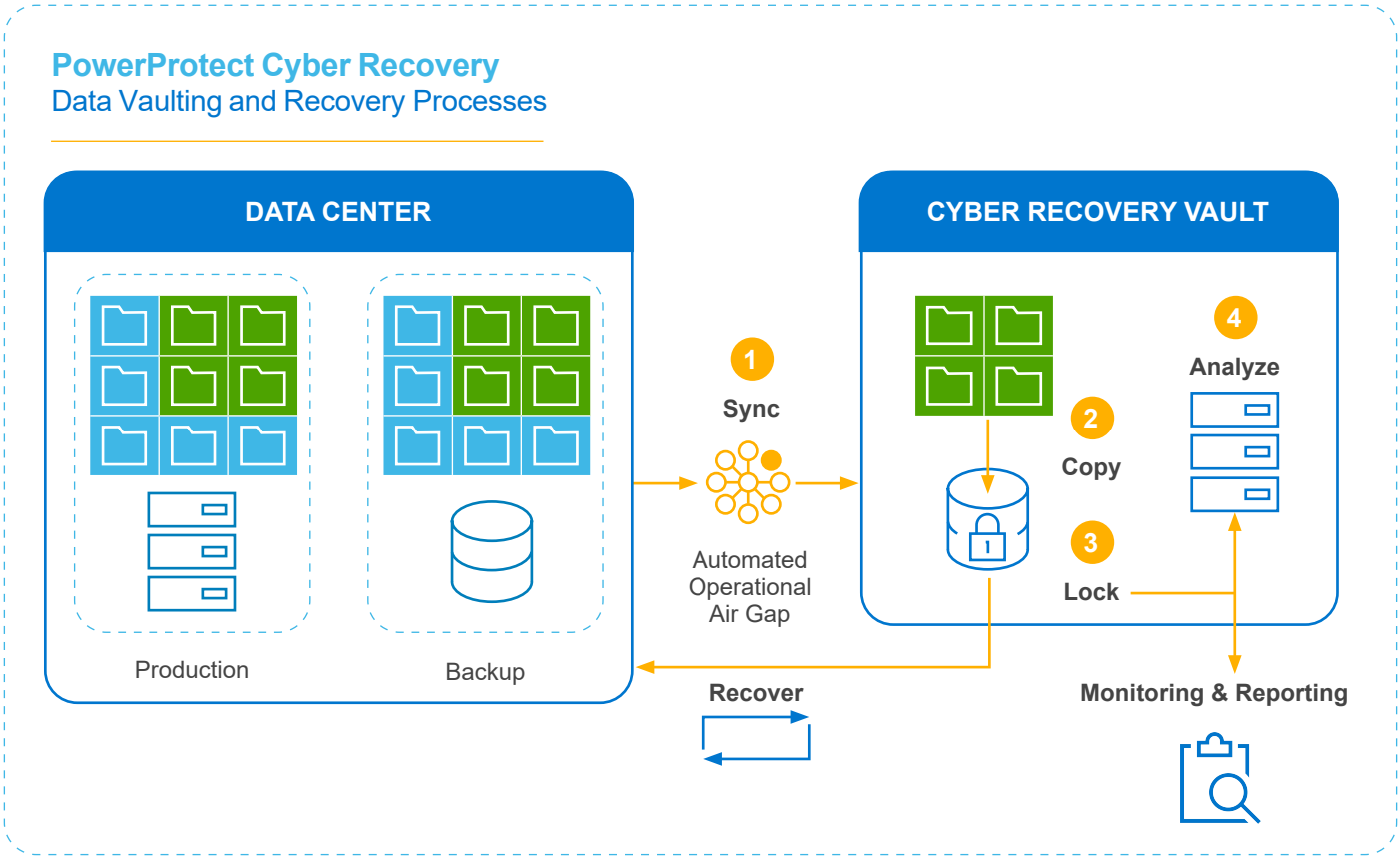
Moving infrastructure into the Cyber Recovery Vault removes it from potential access by bad actors. Isolation also introduces additional management challenges to approved administrators which is why automation is critical. PowerProtect Cyber Recovery automates the workflow associated with creating restore points needed for recovery or analytics. Three core benefits are:

Ease of Use — The time it takes to create a restore point is much faster than a manual management process. This also reduces the window of potential (but limited) exposure.

Automation — Instead of relying on manual creation of each restore point, administrators can schedule policies to create restore points at specific times and recurrence frequency — and then automatically delete the data when the retention period expires.

Reliability — Manual operations are often prone to error. An automated and policy-based approach simplifies the underlying mechanics and reduces the risk of failed recoveries.

The illustration on the next page outlines the steps of creating a restore point from which to recover business critical systems.



PowerProtect Cyber Recovery handles the following discrete operations:

1. **Data Synchronization**—Data representing critical applications is synced through the air gap, which is unlocked by the management server into the vault, and replicated into the vault target storage. The air gap is then re-locked This activity is triggered from within the Cyber Recovery Vault.. The link is enabled prior to data synchronization and then disabled once the synchronization is complete. A single transport mechanism minimizes the attack surface and brings all critical data into the Cyber Recovery Vault in a single transfer. This can include the backup catalog and metadata for backup-based deployments. Data synchronization is transparent to applications on the production side, hence the activity is not 'advertised' in the public domain. The actual data transfer is very efficient, because only changed blocks are copied over the wire. Production-side and target-side systems establish a trusted connection to prevent a rouge system from connecting to the Cyber Recovery Vault Protection Storage.

2. **Creation of Cyber-Attack Testing and Recovery Copies**—Once the data is synchronized and the data path is disabled, the target system conducts an operation that creates a space-efficient copy of the data. The management software provides the ability to create writable sandbox copies for recovery drills and tests, data validation, and analytics. Regular recovery drills are advised to ensure the data has not been compromised and that staff is prepared to perform a recovery in the event of an actual attack.

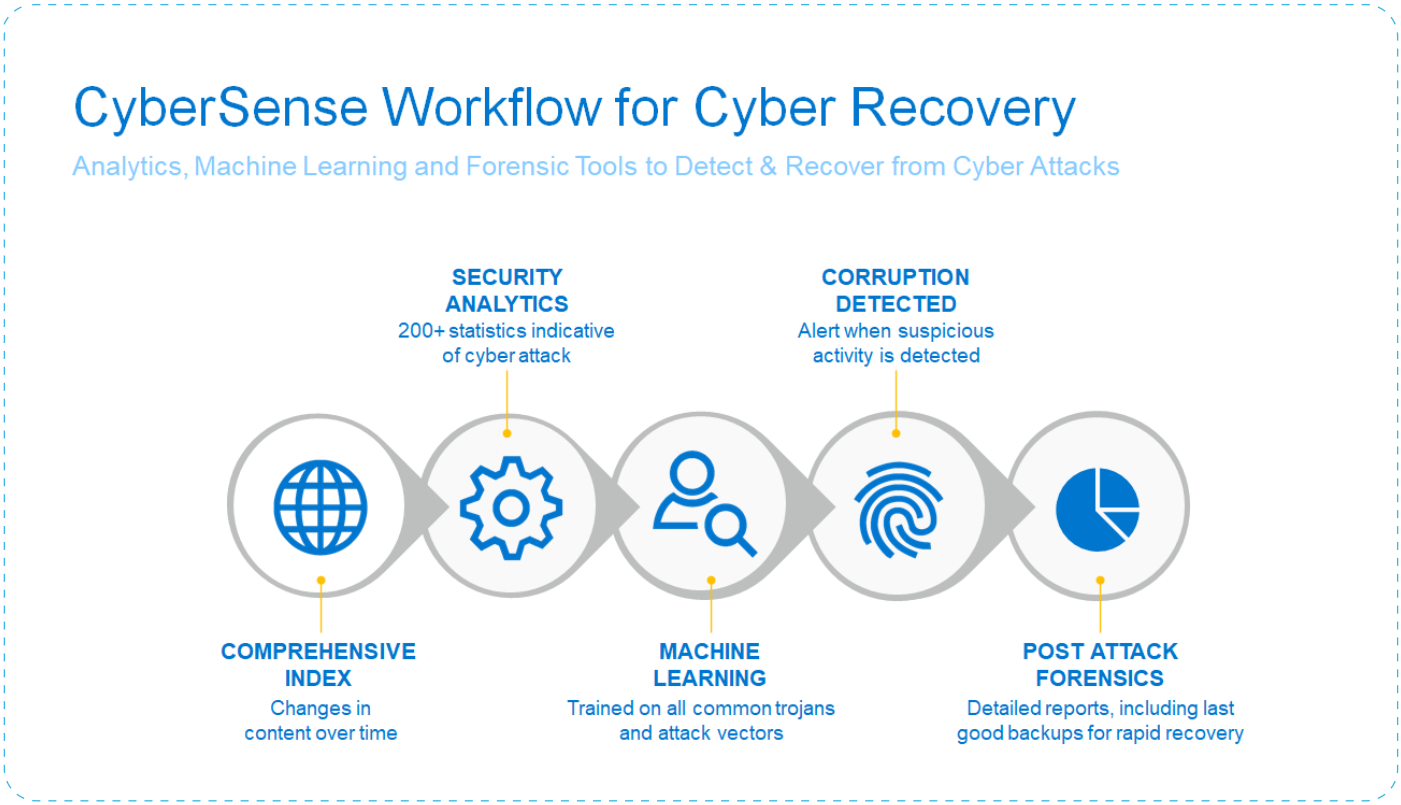
3. **Retention Lock/Creation of Immutable Restore Points**—To prevent deletion, this copy is made immutable by retention locking each file, to further protect it from accidental or intentional deletion. Policies can set retention periods based on space requirements. It is important to note that the Cyber Recovery Vault is not meant to be an archive. Retention periods typically range from 7-45 days. Exceptions can be made, for example to enable recovery of executables, organization should maintain a year's worth of copies of distribution packages containing binaries and OS images.

4. **Analyze** —The data is optionally analyzed by our analytics engine, CyberSense, which we will cover in the next section.

Analytics In the Vault

PowerProtect Cyber Recovery does not replace good security prevention and detection—it is meant to complement these security measures. At the same time, the Cyber Recovery Vault provides some unique advantages over the production environment:

- A protected environment increases the effectiveness of security analytics. Because the Cyber Recovery Vault is isolated from the network, malware scans can be run forensically and unimpeded as they are not susceptible to malware masking routines. Diagnosis of certain attack vectors are better analyzed in an isolated workbench.
- Even if caution needs to be applied, application restart activities can detect attacks that only occur when application is initially started. Application tools like DBVERIFY, that would otherwise require downtime, can also be used in the offline environment.



CyberSense

Running analytics on the data in the vault is a vital component to enable a speedy recovery after an attack. Analytics help to determine whether a data set is valid and useable for recovery; or has somehow been improperly altered or corrupted so that it's "Suspicious" and potentially unusable. PowerProtect Cyber Recovery is the first solution to fully integrate CyberSense which adds an intelligent layer of protection to help find data corruption when an attack penetrates the data center. This innovative approach provides full content indexing and uses machine learning (ML) to analyze over 100 content-based statistics and detect signs of corruption due to ransomware. CyberSense finds corruption with up to 99.5% confidence, helping you identify threats and diagnose attack vectors while protecting your business-critical content—all within the security of the vault.

CyberSense monitors files and databases and analyzes the data's integrity to determine if an attack has occurred. Once data is replicated to the Cyber Recovery vault and retention lock is applied, CyberSense automatically scans the backup data, creating point-in-time observations of files, databases, and core infrastructure. These observations enable CyberSense to track how files change over time and uncover even the most advanced type of attack. This scan occurs directly on the data within the backup image without the need for the original backup software. Analytics are generated that detect encryption/corruption of files or database pages, known malware extensions, mass deletions/creations of files, and more. Machine learning algorithms then use analytics to make a deterministic decision on data corruption that is indicative of a cyberattack. The machine learning algorithms have been trained with the latest trojans and ransomware to detect suspicious behavior. If an attack occurs, a critical alert is displayed in the Cyber Recovery dashboard. CyberSense post-attack forensic reports are available to diagnose and recover from the ransomware attack quickly.

Full Content Analytics

CyberSense delivers full-content-based analytics on all the protected data in the vault. This capability sets CyberSense apart from other solutions that take a high-level view of the data, and use analytics that look for obvious signs of corruption based on metadata. Metadata-level corruption is not difficult to detect; for instance, changing a file extension to .encrypted or radically changing the file size. These types of attacks do not represent the sophisticated attacks that cybercriminals are using today. Cybersense goes beyond metadata-only solutions because it is based on full-content analytics that provides up to 99.5% confidence in detecting data corruption. It audits files and databases for attacks that include content-only based corruption of the file structure or partial encryption inside a document or a page of a database. These attacks cannot be found using analytics that does not scan inside the file to compare how it changes over time. Without full-content-based analytics, the number of false negatives will be significant, providing a false sense of confidence in your data integrity and security.

Recovery Procedures

After CyberSense provides post-attack forensic reports to understand the depth and breadth of the attack and provides a listing of the last good backup sets before corruption, you can facilitate the recovery process. The ultimate goal of Dell Cyber Recovery is to provide an organization with the quickest and most reliable path to recovery of business critical systems. It is therefore critical to establish a cyber-attack recovery plan as part of a formal cyber incident response plan. This typically consists of the following elements:

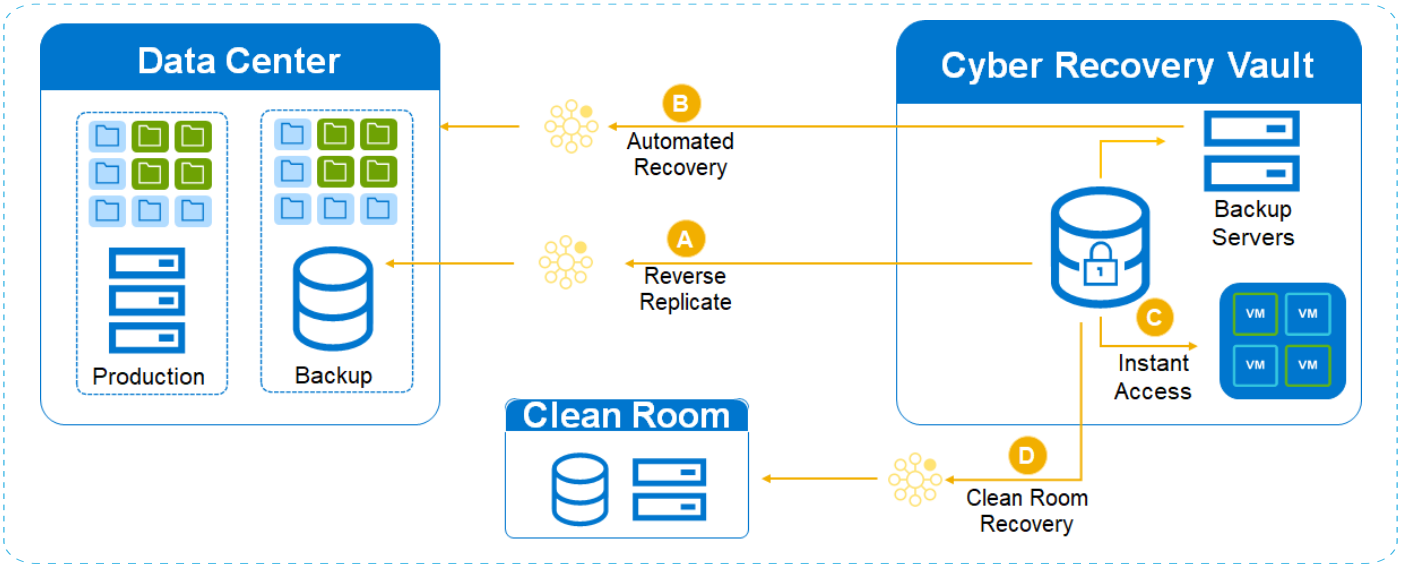
1. **Invoke Cyber Recovery Plan**—Involves securing the breach, invoking the air gap to shut down connection to the CR Vault, and marshalling the resources in the Cyber Recovery Plan to start the response process.

2. **Perform Forensics and Damage Assessment**—Forensics analyze and identify the type and scope of the attack and determine if a fix or patch available can be deployed to avoid reinfection. The Damage Assessment evaluates the affected data and systems to determine what can be repaired and what needs to be recovered, including any dependent systems. It also identifies any unaffected DB logs that can be applied to minimize data loss and determines the best restore point.

3. **Preparation for Recovery**—Determines the most appropriate recovery technique and then prioritizing and sequencing the recovery of specific systems. This evaluation factors in the affected parts of the production environment, time of day, and other circumstantial details. The end goal is to choose a recovery path that prevents or minimizes the damage to business critical systems.

4. **Recovery of Data, Applications and Services**—This step is usually the execution of the system and data recovery based on steps 1-3. An organization might choose to perform a reverse synchronization of data back to a cleansed or rebuilt production system and then apply patches to prevent reinfection. Or it might elect to perform recovery within the CR Vault and then connect the recovered infrastructure back to the production network.

Several recovery techniques can prove viable depending on the cyberattack and the damage created. A few scenarios are outlined below.



Dell Technologies offers flexible recovery options to meet your cyber resiliency requirements. There are several different factors that come into play for the recovery process from customer maturity to specific applications. Additionally, the recovery process isn't happening in a vacuum, it is going to be integrated with your incident response process. After an event occurs, the incident response team analyzes the production environment to determine the root cause of the event. Then, when the production is ready for recovery, there are four ways to perform a recovery with PowerProtect Cyber Recovery:

SCENARIO A
Reverse Replicate

Reverse Replicate or "Simplified backup restore" is the simplest, most straightforward process. This option is suggested for users who want to restore a complete known good backup and then restore the application data from it. You can Reverse Replicate from the PowerProtect DD (or multiple PowerProtect DDs) in the vault back to where that data originated. Once the data lands on the PowerProtect DD back in the production environment, then it becomes a normal recovery process using your backup software.

SCENARIO B
Automated Recovery

Automated Recovery or "Automated selective restore" allows you to recover directly from the vault rather than moving everything to the backup within the production environment. This option is suggested for users who want to restore complete or selective application data into production by maintaining and using the backup app in the vault. This process requires that you have a separate backup server in the Cyber Recovery vault. This server would access data on the PowerProtect DD from within the vault, and then you would use the server to recover datasets into the datacenter within the production environment. Automated recovery requires additional steps such as creating network connections, DNS, etc. but we can help customers work through these issues using a runbook.

SCENARIO C
Instant Access

Instant Access or “VM Instant Access” is for users who want instantaneous access to their VMs. This option takes advantage of PowerProtect DD’s instant access capability and allows you to run the VMs on that PowerProtect DD in the vault. You can instantly bring those VMs up, to use for testing or you can use that environment for production. Instant access can be used as the sole recovery process or as part of the whole process.

SCENARIO D
Clean Room

Clean Room or “Comprehensive Test and Restore” is for users who want to test their data before recovering to ensure data integrity. A clean room is a physically or logically separate area of infrastructure that isn’t connected to anything. This clean room can either be very small (i.e. a couple of VMs), or it could be quite a bit of infrastructure – it depends on what you are going to recover to the clean room. There are two recovery options for the clean room.

Option 1 – The purpose of the clean room in this option is to recover one application at a time and test it to make sure there is no malware in it. Once the integrity of the data is assured, you can recover it from the clean room back into the production environment and move on to the next application. This is how many incident response teams ensure that everything is clean before it goes back into production. In this scenario, the clean room would be sized to the largest application.

Option 2 – This option is for customers who don’t want to wait for their data center to be recovered before recovering their applications – they want to recover their applications and make them accessible right away. In this instance, there is probably more infrastructure in the clean room than in option 1. You will recover your applications from the vault into the clean room and then run that application as though it was in the production environment. In this scenario, you’re not using the clean room to test, you’re recovering the application to the clean room and running it as your production.

Conclusions

Cyberattacks have had devastating consequences on businesses worldwide and caused reduced revenue, loss of reputation, and millions of dollars in recovery costs. In the rapidly evolving threat landscape organizations are looking for effective recovery strategies with the knowledge that prevention and detection alone are not sufficient. Dell PowerProtect Cyber Recovery provides an effective recovery solution against common attack vectors, including dormant malware, data wiping and locking, data corruption, insider attacks, and destruction of backup and storage assets. It gives organizations the assurance that you can quickly and confidently recover your most critical data and systems after a cyber or other disruptive event and resume normal business operations.

Learn more about Dell PowerProtect Cyber Recovery

Contact a Dell Technologies Expert

View more Security resources

Join the conversation with #PowerProtect

DELL Technologies