DELL Technologies

Technical Whitepaper

Fortify Your Organization Against Destructive Cyberattacks

PowerProtect Cyber Recovery

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

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 cybercrime in 2021[1]. Ransomware attacks not only cost organizations millions of dollars in lost revenue per day, but 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.

June 2022

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

Table of Contents

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 cybercrime.[2] As organizations become increasingly aware of the cybersecurity risks that threaten their mission-critical operations and 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. 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 cyberattacks, 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 cyberattack.[3]

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.

Cyber resilience cannot be achieved without a major component. The Vault!

[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

Major Elements of a Vault

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.

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 data updates is permitted on a regular basis, typically daily.
2. **Immutability:** All data written to the data vault must be "locked" in a manner that electronically prohibits deletion or changes until the expiration of the locking period, which is typically a few weeks to a month. At minimum these requirements should block administrative overrides or virtually based / software defined components that can be destroyed using an administrator's credentials. While there is not yet a relevant cybersecurity standard for this capability, the requirements of 17 CFR 240.17a-4(f)(ii) and related guidance from the US Securities and Exchange Commission can be a useful starting point.
3. **Intelligence:** Data in the vault should be analyzed or interrogated in a manner that ensures it has not been manipulated or corrupted. Where the focus of both isolation and immutability is to protect anything copied into the vault, intelligence validates that the data was not corrupted before reaching the vault.

Public and private sector organizations have increasingly implemented data vaults, which securely store updated copies of their most critical data and applications. If a ransomware or data destruction attack impacts data and applications in the main production environments, the threat actors still cannot access the contents of the data vault. Post-attack, as part of the incident response and recovery process, the clean copies of data and applications stored in the data vault are used to restore the production environment.

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.

Dell PowerProtect Cyber Recovery Overview

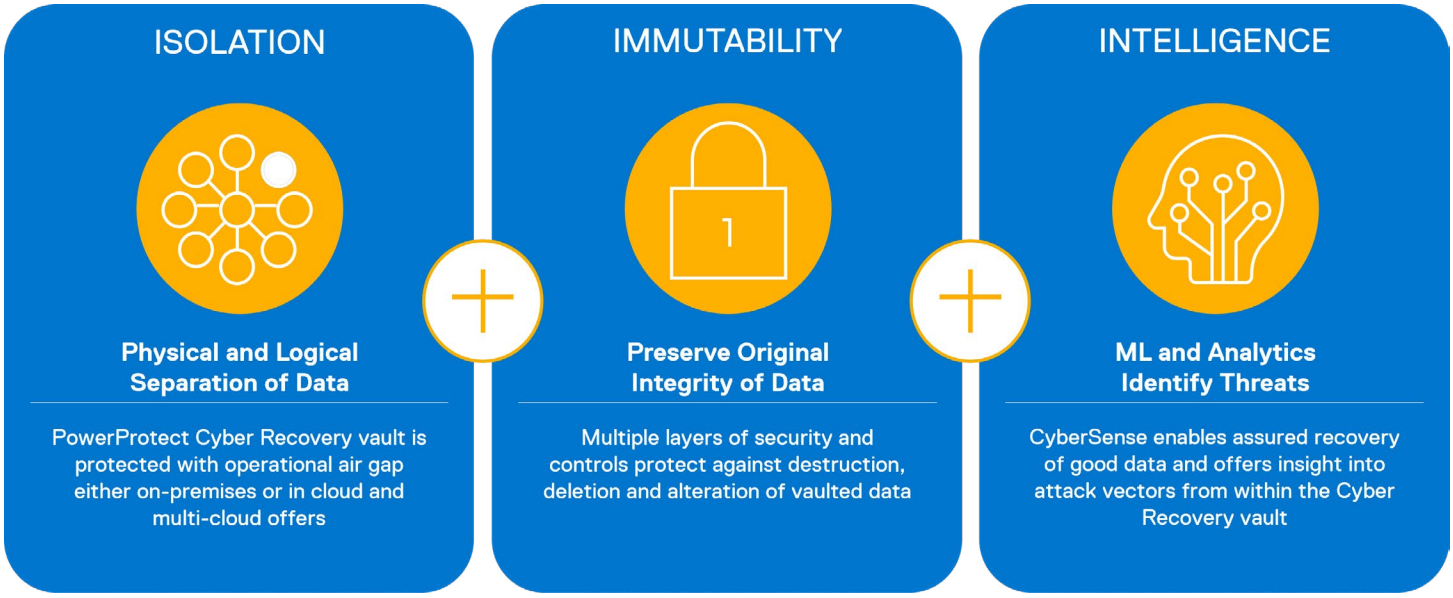
A robust and comprehensive cyber resiliency strategy should leverage frameworks like the National Institute of Standards and Technology (NIST Cybersecurity Framework (CSF)), which can help outline an end-to-end cyber- attack defense continuum. In short, Cyber Resiliency is a strategy that incorporates 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 on-premises or in the cloud and recovering your businesses following a successful cyberattack or ransomware incident, while leveraging a combination of professional services and technology that provide the following three key elements of a Cyber Recovery solution:

PowerProtect Cyber Recovery Advantages

Modern protection for critical data and an enabler of Security Transformation



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 in a "locked" state — no data can flow — there is no access to any part of the solution. No SSH, HTTPS or non-data traffic is permitted. All other components in the vault utilize private address space (RFC 1918) and are never accessible from outside the secure vault area. 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.

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. Originally developed to meet the write-once-read-many requirements of an SEC archiving standard, 34 CFR 17a-4(f)(2), this capability protects data from being deleted or modified during a specified retention period. 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)).

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. Signatures are not used so regular updates are not necessary and new techniques used by threat actors can be discovered with knowing about them beforehand. Post attack forensic reporting will quickly and safely identify a 'last known good' copy of data that can be used to recover data to resume business.

[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"

Vault Components, Connectivity and Communications

Vault Components

Dell PowerProtect Cyber Recovery vault provides the functionality of synchronizing data from critical applications and ingesting that data into the vault. This allows organizations to dramatically reduce their surface of attack from inside and outside threats by removing the cyber-attack recovery environment from the production network. Connectivity to and from the vault must be carefully designed such that the integrity of the data inside vault is not compromised. It can also be desirable to consider additional connectivity to the vault for the purposes of messaging, alerting, and management of vault components.

When considering cyber recovery, having a basic understanding of the of the vault components, connections and communication are imperative.

Data Repository – PowerProtect DD is the repository for backup data stored in the Cyber Recovery vault. PowerProtect DD is deployed as either a physical appliance, or as a virtual appliance from the cloud provider's marketplace.

Management Workstation – A physical vault includes a physical workstation allowing complete management of the vault environment without requiring any connectivity external to the vault. Any remote management functionality would typically leverage this workstation as the jump box.

Cyber Recovery Instance – Cyber Recovery software runs inside the vault to manage locking/unlocking the air gap, making a fastcopy (snapshot) of the backup data on the PowerProtect DD, and applying retention lock to the data on the PowerProtect DD as well as orchestrating other functions of the vault. Cyber Recovery can be deployed on VMware, or from the public cloud provider's marketplace.

CyberSense Instance – CyberSense software runs inside the vault providing intelligent scanning of backup data for anomalies. CyberSense is deployed on either physical or virtual servers.

Domain Name Service – Domain Name Service (DNS) is deployed as a service inside the vault providing host name service to the internal components of the vault. The DNS instance in the vault is completely isolated from DNS running external to the vault. It is straightforward and recommended to provide redundant DNS servers running on different hardware to protect against loss of one of the DNS servers.

Firewalls – A firewall provides the ability to monitor network traffic and is configured, via software, to permit or block that traffic from being passed through. A firewall is inherently multi-directional, meaning that the network traffic can originate from either side of the firewall. Because the network traffic permissions and rules are software defined, the integrity of the protection it provides is only as good as the rules which are defined, the integrity of the underlying software, and security of administrative credentials.

Data Diodes – A data diode provides the ability to allow only certain pre-defined protocols to pass through in a single direction. A data diode is, by design, uni-directional appliance, with physical isolation from one side to the other. Because the hardware is physically unable to send data back to the source network, it is inherently more secure than a firewall. Stolen credentials, misconfiguration, or compromise of the insecure side cannot change the uni-directional nature of the hardware.

Zero Trust – A zero trust architecture begins with the premise of trusting no-one. The framework focuses on authentication, authorization, and ensuring there is no implicit trust as much as possible, providing granular levels of authority, enforcing least privilege policies, while maintaining the goal of IT, which is the availability of services, and minimizing delays in authentications. Authentication is required for any communication session to occur.

Vault Connectivity and Communications

The only connectivity which is required for a cyber recovery vault is the lockable air-gap which is used for the ingest of data. The characteristics and security of this connection are described in the PowerProtect Cyber Recovery Advantages section under Isolation. As additional connectivity is considered for a cyber recovery vault, it is imperative to design the methods of communication so that any risk introduced is minimized, or ideally, eliminated. A uni-directional communication stream originating from the vault is inherently easier to implement securely than a communication stream coming into the vault. Care must be taken when considering if a desired connection is absolutely necessary. From an architecture standpoint, additional communication is done via a separate network than the data synchronization air gap due to the fact that the air gap is unlocked for only the time needed for data ingest.

Outbound Messaging and Alerts – Monitoring the status of the vault and being able to see notifications and alerts coming from the vault in a timely manner is essential. Screen mirroring and/or email notifications can both be set up securely as it is uni-directional communications coming from the vault.

Inbound Software Patches and Updates – The ability to ingest periodic software updates and patches in the various internal components of the vault are necessary for ongoing operations of the vault. Two common methods of ingesting software are 1) leveraging PowerProtect DD Mtree replication and 2) leveraging a data diode. Each method has its own advantages and drawbacks to be considered.

- PowerProtect DD Mtree Replication leverages the existing PowerProtect DDs in the environment by simply configuring an additional Mtree for the express purpose of copying in software updates. Inside the vault, it can be automatically scanned by CyberSense to assess risk of compromise of the update files. The timeliness of bringing in software updates is dependent on the schedule of unlocking the air gap allowing inbound replication, which may be inconvenient for quick updates.

- Data Diode transfer allows the ingest of software updates using a uni-directional hardware devices which can provide near real-time transfer of the software updates into the vault, as it does not rely on the PowerProtect DD air gap schedule but lacks the automated CyberSense scanning.

Inbound Time Synchronization – While sub-millisecond time synchronization of various components of the vault with each other and the outside world is not explicitly necessary, it is straightforward to provide accurate time synchronization into the vault using a uni-directional data diode. The data diode, due to its physical separation between secure and public facing sides and its unidirectional nature, plus its ability to inspect an incoming NTP packet and ensure it is only relaying the actual time.

Remote Management – Depending on the needs of the environment, remote management may be necessary for tasks such as deeper investigation of alerts or messages, software updates, product support sessions, or other things. As much as possible, any type of remote management should be done physically at the vault, but it is recognized that there are times that a means of having remote management may be necessary. Zero Trust architecture should be of primary consideration for any remote management requirements. A separate whitepaper describes zero trust architecture in more detail. If considering a bi-directional data diode (which is, basically, two data diodes in a single package) for remote management, the security of the source workstation is critical, as is protecting against any device assuming the IP address and/or credentials necessary to connect to the vault. It is not recommended to leave a remote management data diode physically connected to the vault when not in operation.

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.

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:

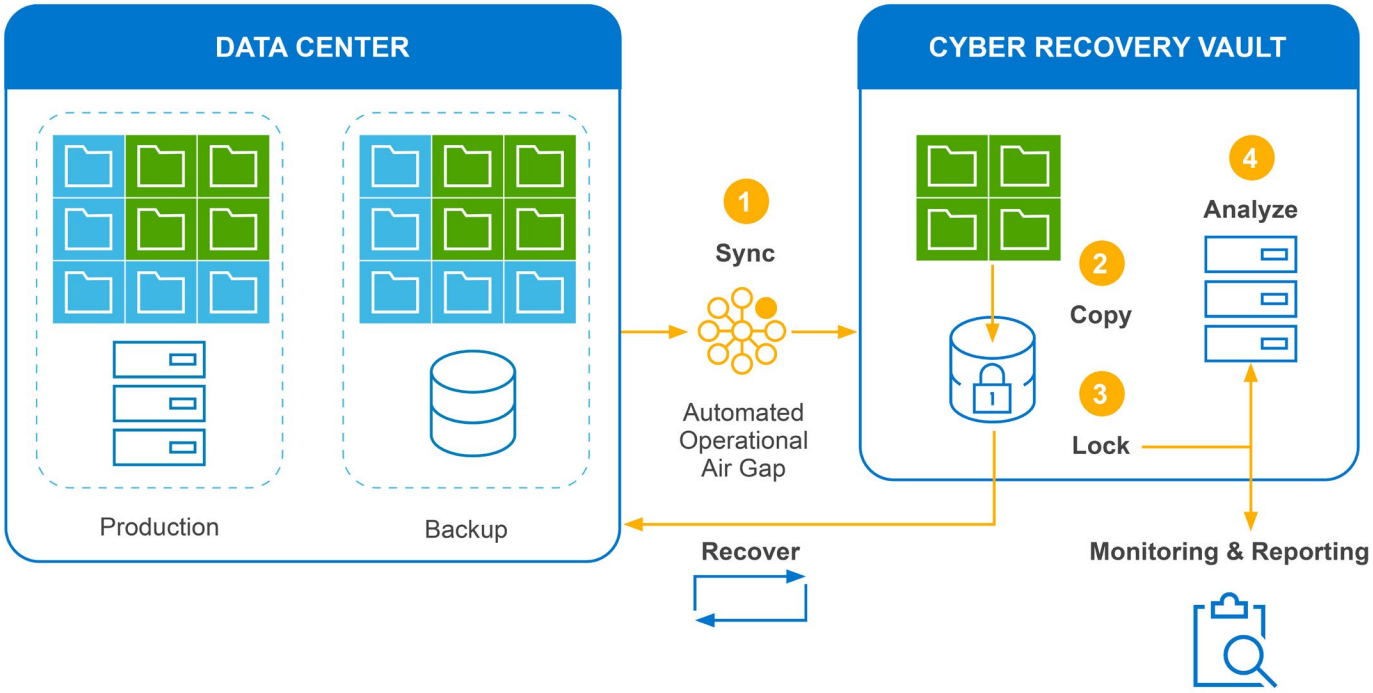
Ease of Use — The time it takes to create a restore point is much faster than a manual management process. This also reduces the window of potential (but limited) exposure.

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
Data vaulting process to secure critical data for recovery



PowerProtect Cyber Recovery can reside at the production data center, a DR environment, in a public cloud or in a shared managed environment delivered by a partner. In any deployment the basic operations below are followed:

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. Analyzing the data within the vault increases the accuracy of the integrity of the data. We'll cover CyberSense more in detail later.

Analytics In the Vault

PowerProtect Cyber Recovery does not replace a comprehensive prevention strategy – it is meant to compliment as a last line of defense should they fail. 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, scans for data corruption due to malware 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

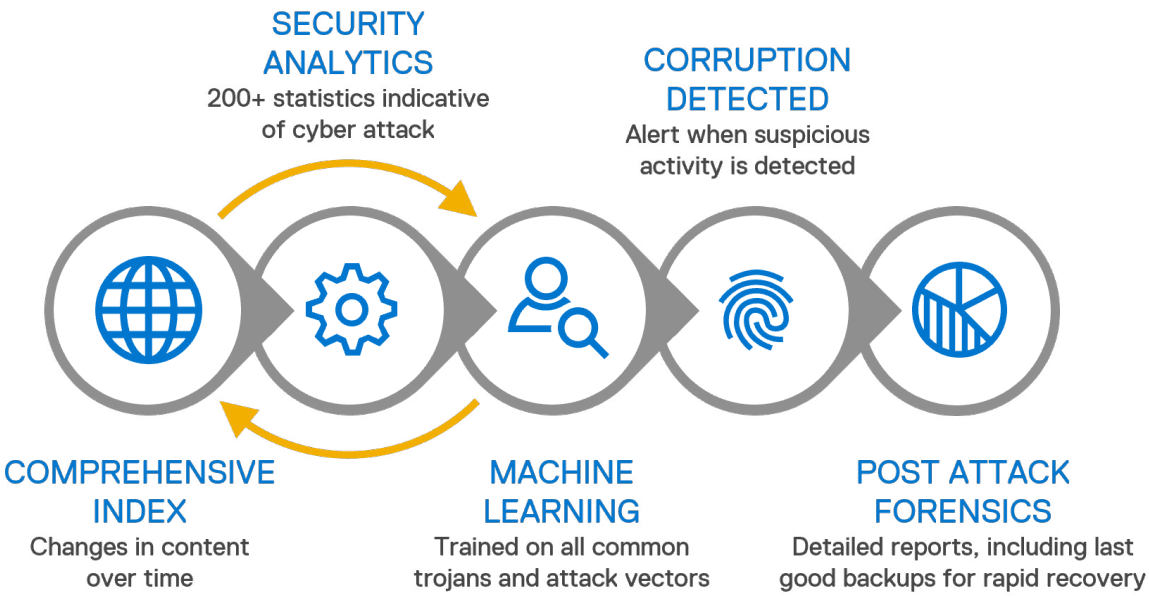
Running analytics on the data in the vault is a vital component to enable a speedy recovery after an attack. Analytics help to determine whether a data set is valid and useable for recovery; or has somehow been improperly altered or corrupted so that it's "Suspicious" and potentially unusable. PowerProtect 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 200 content-based statistics and detect signs of corruption due to ransomware. CyberSense finds corruption with up to 99.5%[1] 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.

[1] Based on Dell analysis of publicly available data, June 2022. Actual results may vary.

CyberSense Workflow

Analytics, Machine Learning and Forensic Tools to Detect and Recovery from Cyberattacks



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%[1] 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.

[1] Based on Dell analysis of publicly available data, June 2022. Actual results may vary.

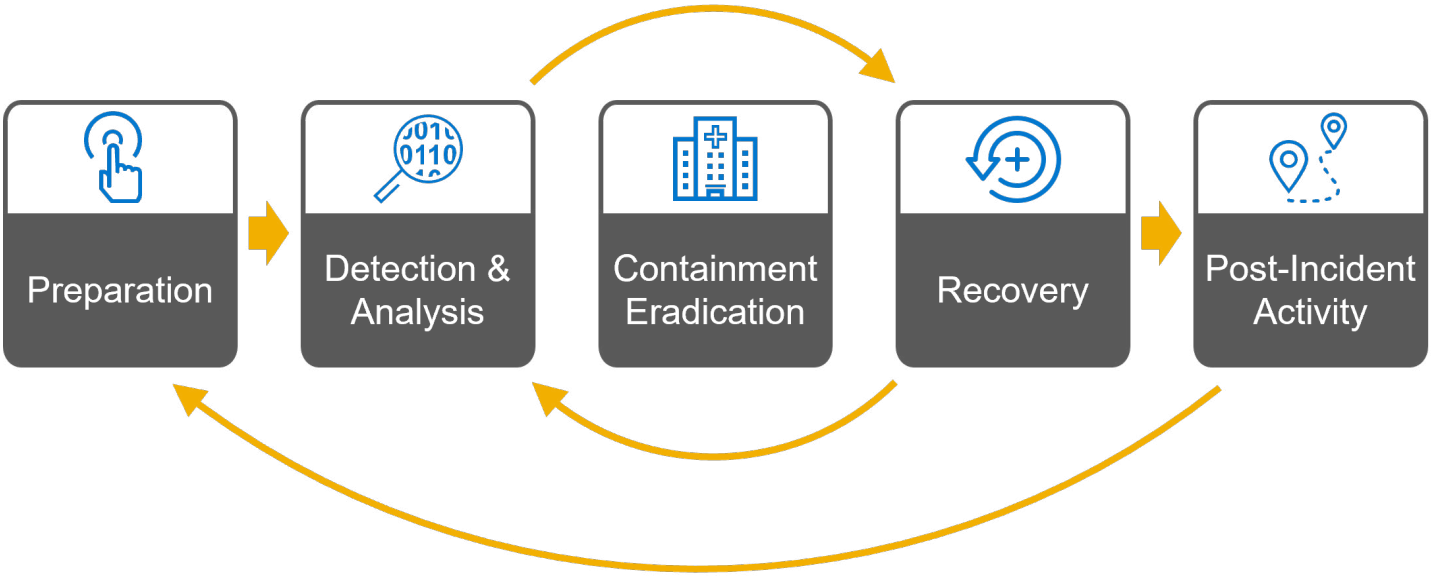
Incident Response and Recovery Options

When faced with an attack, recovery option flexibility is paramount. There are many factors that come into play to determine the best recovery option for a particular event. 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 to select the most appropriate recovery plan.

The ultimate goal of Dell PowerProtect 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:

Incident Response Workflow

Critical strategy to identify, eradicate and recover from cyber threats



1. Preparation – involves understanding the business impact of the critical data to be protected, the personnel that needs to be involved, the communication methods and the details of the run book.

2. Detection and Analysis – involves the forensics analysis to detect and identify the type, scope and resources affected by the attack. Involves securing the breach, invoking the air gap to shut down connection to the cyber recover vault, and marshalling the resources to start the mitigation process.

3. Containment Eradication – This stage involves damage assessment of 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. At this stage the most appropriate recovery technique is determined 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. In this stage, the attack has been halted and no more damaged is being done. This also involves providing documentation and alerts to the necessary team members of the type of cyberattack, resources affected, and estimated RTO and RPO.

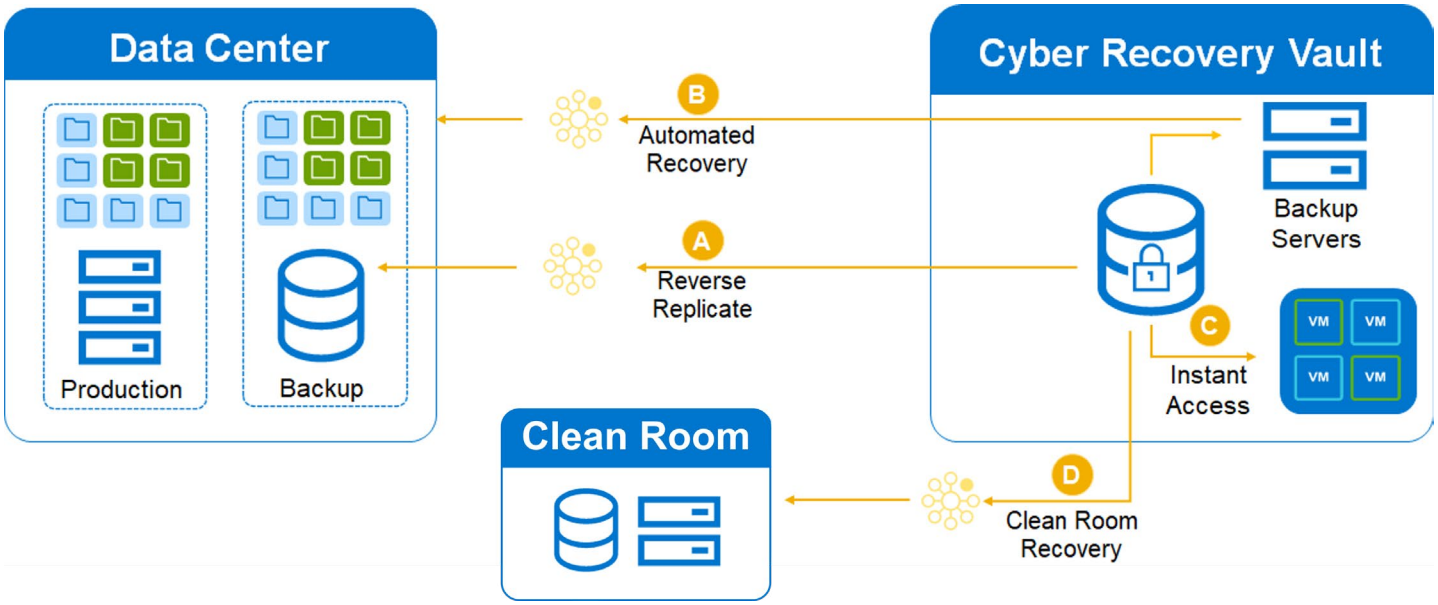
4. Recovery – This step is usually the execution of the system and data recovery based on steps the migration results. An organization might choose to perform a reverse synchronization of data back to a cleansed or rebuilt production system and then apply patches to prevent reinfection. Or it might elect to perform recovery within the cyber recovery vault and then connect the recovered infrastructure back to the production network. Recovery options will be discussed in the next section.

5. Post Incident Activity – This involves the lessons learn from the attack. After the attack it is important to understand that the appropriate steps were taking to mitigate the attack and resume business as quickly as possible. The results from this stage will be implemented in the preparation for the next attack.

Recovery Options

Cyber Recovery 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:

PowerProtect Cyber Recovery
Flexible recovery options to restore critical data



SCENARIO A
Reverse Replicate

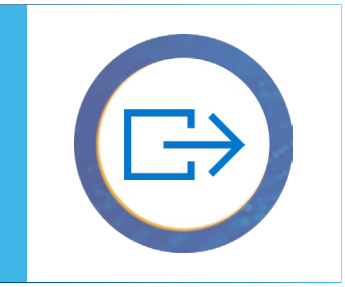
Reverse Replicate or "Simplified backup restore" is the simplest, most straightforward process. This option is suggested for users who want to restore a complete known good backup and then restore the application data from it. You can Reverse Replicate from the PowerProtect DD (or multiple PowerProtect 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

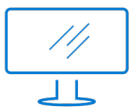
Clean Room or "Comprehensive Test and Restore" is for users who want to test their data before recovering to ensure data integrity. A clean room is a physically or logically separate area of infrastructure that isn't connected to anything. This clean room can either be very small (i.e., a couple of VMs), 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