DELL Technologies

TECHNICAL WHITE PAPER

# How Dell Technologies supports recoverability of the Epic EHR System


**Abstract**

This paper describes using a comprehensive cyber recovery approach leveraging Dell Technologies PowerProtect Cyber Recovery to safeguard medical records and Epic applications against today's sophisticated cyberattacks.



July 2023

# Table of Contents

# Executive summary

Healthcare often tops the list of cybersecurity attack targets. According to the FBI, the healthcare and public health sector was the most targeted critical infrastructure sector for ransomware attacks in 2022.[1] A successful attack results in both a financial problem and a clinical problem impacting patient care.

The always-on connectivity in today's modern healthcare introduces a host of challenges, requiring IT to rethink technologies to secure electronic patient health information (ePHI). Rather than emphasizing ransomware or cyberattack prevention, organizations should focus on protecting patients' medical records with solutions that enable you to recover your critical assets with integrity so you can resume normal clinical operations with confidence. Remaining HIPAA-compliant starts with protecting your data and applications—against ransomware and other sophisticated cyber threats.

With cybersecurity, it's not a matter of "if" but "when" you will be faced with such an attack. How do you recover quickly, at size and scale, and continue to operate your organization with minimal impact on patients?

Dell PowerProtect Cyber Recovery provides the highest levels of protection, integrity and confidentiality for your most valuable data and critical business systems and is a vital component of a comprehensive cyber resiliency strategy. This assurance that you can quickly recover after a cyber or other disruptive event is a necessary step in resuming normal business operations. A modern and powerful cyber resiliency strategy and Dell PowerProtect Cyber Recovery are key to enabling our customers to increase business agility, achieve business continuity and reduce business risk.

[1] FBI Internet Crime Report 2022, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

# The critical nature of the Epic EHR system requires enterprise backup and data protection

For many healthcare organizations, Epic is the electronic health records (EHR) system of choice. Combining clinical workflow management, patient health information, operations and integrations, Epic increases efficiency, enables secure access to medical records and improves patient care.

Epic is not a monolithic application with a single database, but a complex combination of different data types requiring a robust IT infrastructure as a foundation. For example, Epic deployments often use Microsoft Active Directory to synchronize user credentials, which would also handle federation services and certificate services, among others. There are also a host of configuration files that need to be managed, as well as APIs to integrate with business applications. All of these services require a comprehensive enterprise solution for backup and data protection.

Healthcare organizations today work with highly sensitive patient information where maintaining the security and integrity of their data is of the utmost importance. Furthermore, many care providers may need to work in remote locations, like ambulances and mobile clinics, where secure network connections are essential.

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 should not be limited to the Epic platform in isolation but should rather be part of a larger strategy that incorporates people, process and technology into a holistic framework that protects an entire organization or entity.

# The benefits of a vault for protecting data and apps

The Department of Health and Human Services (HHS) recognizes the threat of the cybercriminal ecosystem on the healthcare sector and public health critical infrastructure. As a result, HHS recommends that organizations not only implement vetted cybersecurity practices against malware and other threats but also incorporate tactics to protect new technologies targeted by attacks.

This level of 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.

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

- **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.
- **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 a minimum these requirements should block administrative overrides or virtually based / software-defined components that can be destroyed using an administrator's credentials.
- **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.

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 cyberattack defense continuum. In short, a cyber resiliency strategy allows you to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions.

## Dell PowerProtect Cyber Recovery is a component of an overall cyber-resiliency strategy

PowerProtect Cyber Recovery distinguishes itself from traditional backup and disaster recovery by providing additional layers of physical and logical security at the solution, system and data/file level. This ensures critical data can be preserved with integrity, confidentiality and availability 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 three key elements of a Cyber Recovery solution (Figure 1).

**Figure 1.** 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.[2] Likewise, CISA and MS-ISAC recommend that organizations who are looking to protect themselves from ransomware need to maintain offline, encrypted backups of data.[3] 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 five 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 locked cage or 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. 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. Bad actors can't wait for the vault to unlock and then just drive in.

[2] "Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware," Gartner, https://www.gartner.com/en/documents/3995229

[3] "#StopRansomware Guide," Cybersecurity and Infrastructure Security Agency (CISA) and Multi-State Information Sharing and Analysis Center (MS-ISAC), https://www.cisa.gov/stopransomware/ransomware-guide

### IMMUTABILITY

PowerProtect Cyber Recovery offers an automated data copy and air gap, which creates unchangeable data copies in a secure digital vault and an operational air gap between the production/backup environment and the vault. Originally developed to meet the write-once-read-many requirements of a U.S. Securities and Exchange Commission (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 the Dell PowerProtect DD storage appliance, data is protected 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.

### INTELLIGENCE

CyberSense, our analytics engine, 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 the 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 determine whether data has been impacted by malware, and tools are provided 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 without 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.

# How PowerProtect vaulting and recovery work

Dell PowerProtect Cyber Recovery provides management tools and the technology that perform vaulting and the recovery of data. It automates the creation of the restore points that are leveraged for recovery or security analytics. To ensure PowerProtect Cyber Recovery is set up and optimized for your environment, Dell Implementation Services are required for Cyber Recovery Vault design and implementation. These services include expert guidance to select critical data sets, applications and other vital assets determined by Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) to streamline recovery. In addition, Dell Advisory Services are recommended for designing an effective recovery strategy.

## WHAT YOU SHOULD VAULT

Organizations with an Epic implementation should copy all aspects of Epic and any ancillary applications that support it. This includes all patient data in both the Operational Database (ODB) and Web BLOB share, as well as Epic applications such as Cogito Clarity and Caboodle.

There are four main data sets used by the Epic application:

1. The Operational Database (ODB), which contains the structured information of a patient's record
2. The Web BLOB share, which contains the unstructured information of a patient's record
3. The Cogito Clarity database
4. The Cogito Caboodle database

The first two datasets are required for patient care and must be available. The Cogito Clarity database includes some audit-trail information that may be unique and could be deemed critical by the organization's compliance team. The Cogito Caboodle database can contain unique financial information from external sources and could be deemed critical by the organization's finance team.

## 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.

## VAULTING DATA AND APPS

PowerProtect Cyber Recovery can reside at the production data center, in a disaster recovery (DR) environment, in a public cloud or in a shared managed environment delivered by a partner. Basic operations are followed in any deployment, which are described as follows and illustrated in Figure 2:

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.

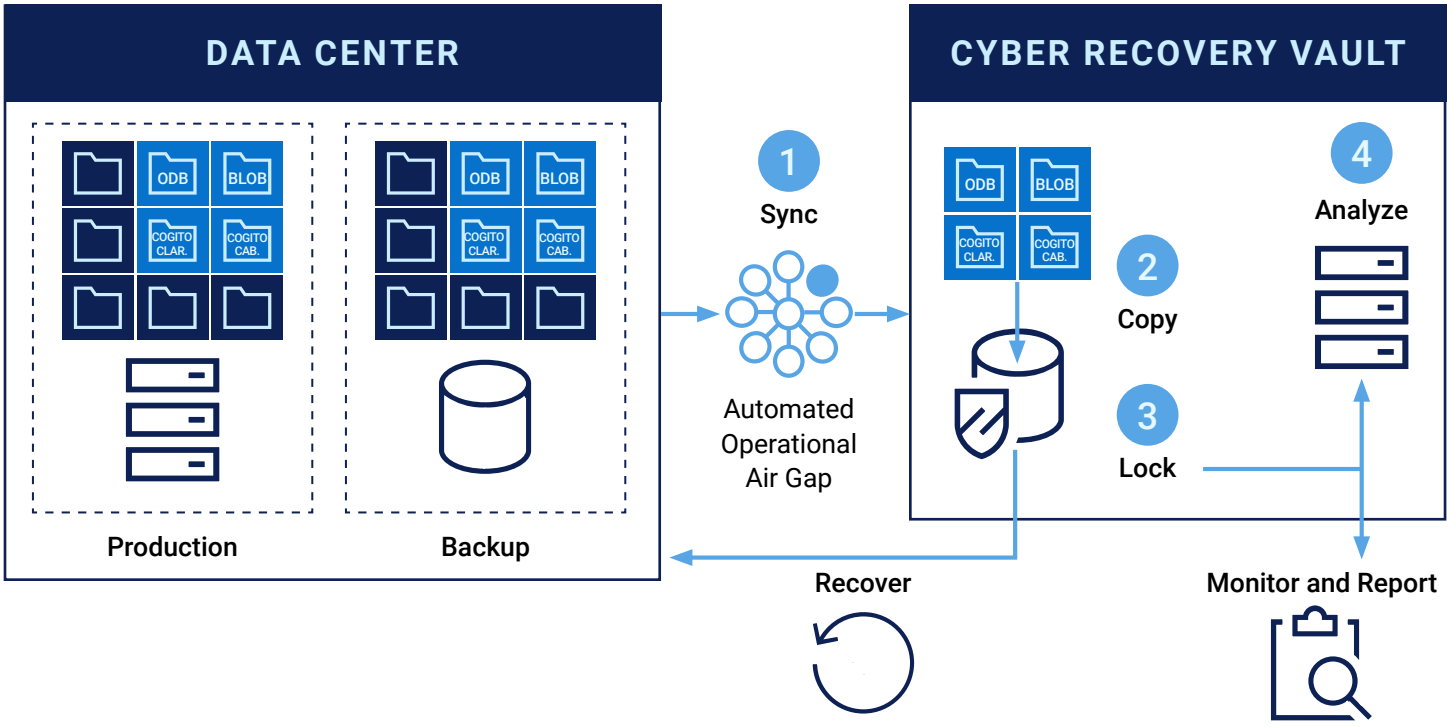
Data synchronization is transparent to applications on the production side; hence, the activity is not "advertised" in the public domain. The actual data transfer is very efficient because only changed blocks are copied over the wire. Production-side and target-side systems establish a trusted connection to prevent a rogue system from connecting to the Cyber Recovery Vault Protection Storage.

2. **Creation of Cyberattack 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 the 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, the recovery 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 to 45 days although exceptions can be made. For example, to enable recovery of executables, organizations should maintain a year's worth of copies of distribution packages containing binaries and OS images.

4. **Analyze:** The data is optionally analyzed by the CyberSense analytics engine. Analyzing the data within the vault increases the accuracy of the integrity of the data.

**Figure 2.** PowerProtect Cyber Recovery data-vaulting process to secure critical data for recovery.



# Analytics in the vault

PowerProtect Cyber Recovery does not replace a comprehensive prevention strategy. It is meant to complement as a last line of defense should other protection methods fail. At the same time, the Cyber Recovery Vault provides 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 is better analyzed in an isolated workbench.
- Even if caution needs to be applied, application restart activities can detect attacks that occur only when an application is initially started. Application tools, such as an integrity check, 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 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% confidence, helping you identify threats and diagnose attack vectors while protecting your business-critical content—all within the security of the vault.

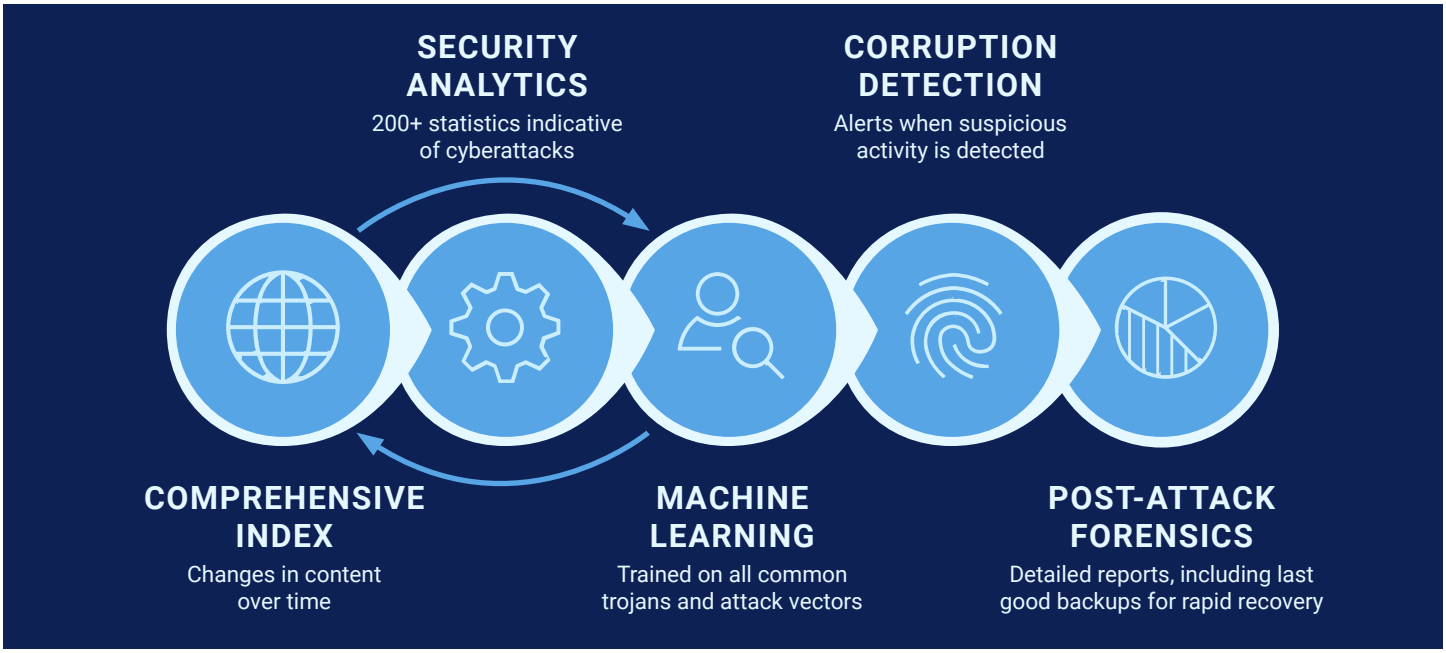
CyberSense monitors files and databases and analyzes the data's integrity to determine if an attack has occurred. Once data is replicated to the Cyber Recovery vault and retention lock is applied, CyberSense automatically scans the backup data, creating point-in-time observations of files, databases, 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%[4] 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 do 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.

**Figure 3.** CyberSense workflow including analytics, machine learning and forensic tools to detect and recover from cyberattacks.



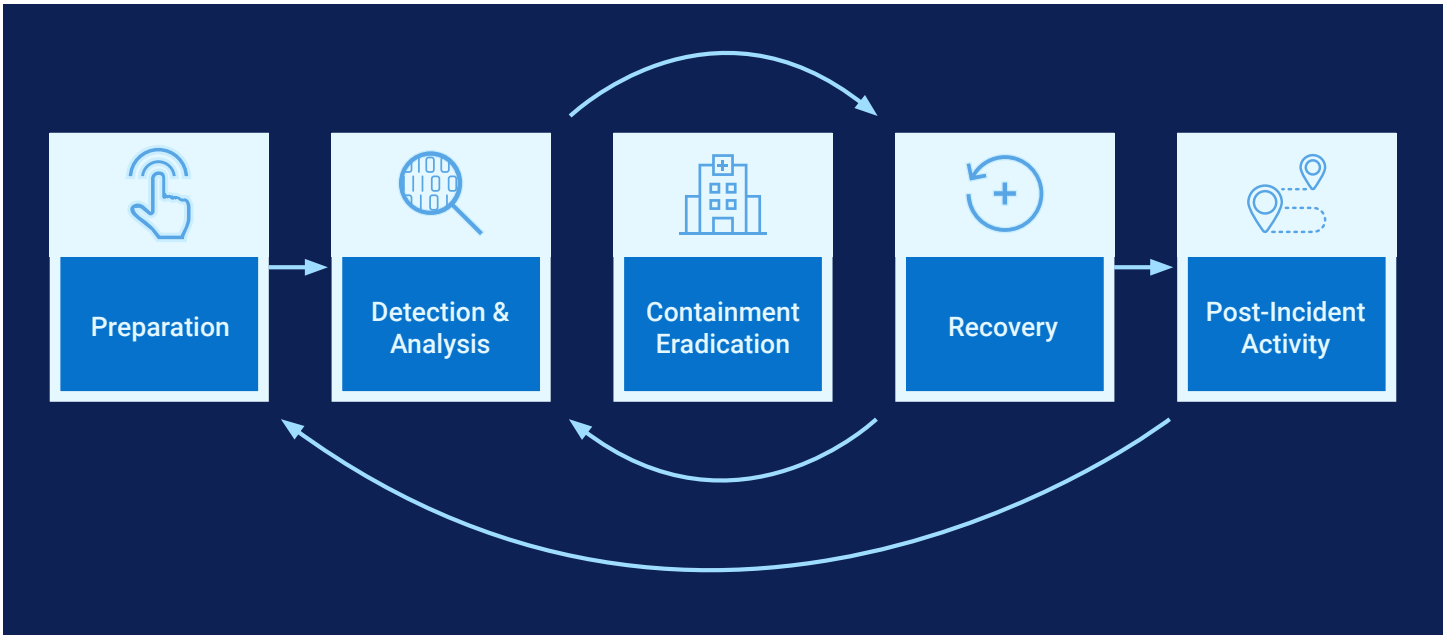

# Incident response and recovery options

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 highly important to remember that active cyber-resiliency 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 cyberattack recovery plan as part of a formal cyber-incident response plan.

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

**Figure 4.** Incident-response workflow detailing critical strategy to identify, eradicate and recover from cyber threats.




## INCIDENT-RESPONSE WORKFLOW

As a best practice, organizations should have an up-to-date cyber-recovery runbook to use as guidance once an incident occurs. The runbook, which is unique to every organization, outlines the steps an incident team takes to recover from an event. An example of a high-level runbook is as follows:

1. Respond to the cyberattack.
2. Isolate the attack.
3. Initiate cyber-recovery incident communication plan.
4. Initiate and perform forensics.
5. Perform damage assessment.
    a. Identify affected systems.
    b. Determine impact.
6. Cleanse the impacted environment.
7. Invoke the cyber-recovery plan.
8. Cyber Recovery vault response:
    a. Follow the CR/DR plan for affected systems.
    b. Handle other dependencies.
9. Prepare for recovery/restore.
10. Recover.

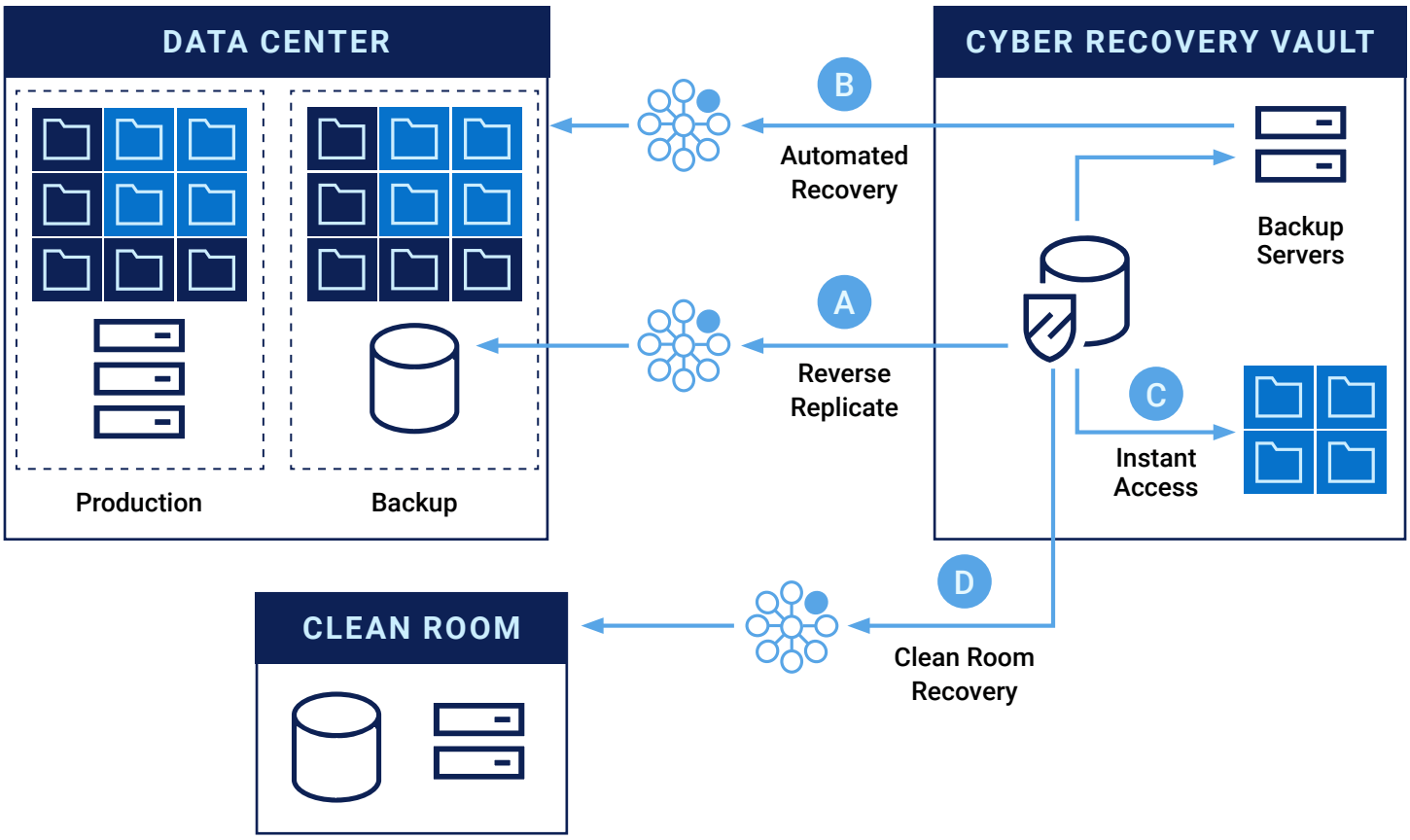
The incident-response workflow, designed to identify, eradicate and recover from cyber threats, is a multi-step process, as follows:

1. **Preparation**: This stage involves understanding the business impact of the critical data to be protected, the personnel that need to be involved, the communication methods and the details of the runbook.
2. **Detection and Analysis**: This stage involves the forensics analysis to detect and identify the type, scope and resources affected by the attack. It involves securing the breach, invoking the air gap to shut down the connection to the Cyber Recovery vault, and marshalling the resources to start the mitigation process.
3. **Containment Eradication:** This stage involves a 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, followed by prioritizing and sequencing the recovery of specific systems. This evaluation factors in the affected parts of the production environment, the 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 damage is being done. This also involves providing documentation and alerts to the necessary team members regarding the type of cyberattack, resources affected and estimated RTO and RPO.
4. **Recovery:** This stage is usually the execution of the system and data recovery based on the steps of 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.
5. **Post-Incident Activity:** This involves the lessons learned from the attack. After the attack, it is important to review the steps and missteps that were taken to mitigate the attack and resume business as quickly as possible. Knowledge gained from this stage will be used to revise the incident response plan in the preparation for the next attack.

## RECOVERY FROM THE VAULT

An important part of incident recovery is understanding what tasks must be performed sequentially and those that can be run in parallel. For example, before any part of Epic is restored, you must first ensure that the production environment has been cleaned and is ready for restore. The critical rebuild items—such as Active Directory, Lightweight Directory Access Protocol (LDAP), Domain Name System (DNS), network settings, operating systems, and so on—have been redeployed. From there, you can restore the ODB, Web BLOB share, Cogito Clarity, and Cogito Caboodle and then bring the other Epic modules online.

**Figure 5.** PowerProtect Cyber Recovery: Flexible recovery options to restore critical data




Cyber Recovery offers flexible recovery options to meet your cyber-resiliency requirements. Several different factors come into play for the recovery process, from customer maturity to specific applications. Additionally, the recovery process doesn't occur in a vacuum; it is 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 several ways to perform a recovery with PowerProtect Cyber Recovery. The most common options are:

- Recovery from the vault to production
- Reversing the replication connect back to the production backup environment
- Recovering virtual machines (VMs) directly in the vault environment and VMware vMotion back to the production environment
- Recovery to a clean room environment and then move to production

Different restore methods may be used for different applications and data depending on business need and confidence in the fidelity of the production environment. PowerProtect Cyber Recovery provides the accessibility of the recovery environment and the availability of the data necessary for recovery.

# Conclusions

**Secure Care: comprehensive security for clinical and business staff, network, endpoints, data and recovery**

At Dell Technologies, we believe security should be holistic, intelligent and scalable, spanning the entire healthcare organization with consistent objectives and policy application. Dell Technologies Secure Care is a portfolio of solutions that enable healthcare organizations to secure data and assets. Using a multi-layered approach, these solutions encompass physical security, network and endpoint security, data protection and recovery, and training.

The Epic EHR system is a core business application in the healthcare industry. A majority of health-related organizations rely on Epic to store and exchange patient information. When access to Epic is interrupted, many clinical processes are impacted.

Cyberattacks have had devastating consequences on the healthcare sector, resulting in lost revenue, loss of reputation and millions of dollars in recovery costs. More critically, patient welfare has been at risk in the form of delayed tests and procedures, longer hospital stays and even death. In the rapidly evolving threat landscape, healthcare 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.

## ONE SOURCE TO DEPLOY AND MANAGE YOUR EPIC ENVIRONMENT

Dell Technologies delivers solutions to meet the most rigorous application, user and business demands. Solutions are built to speed performance, simplify management, enhance data protection and deliver always-on availability for patient care delivery. Our strategically aligned business solutions are designed to meet all of your EHR needs, including end-to-end protection from pre-attack to cyber recovery.

**LEARN MORE**
**about Dell PowerProtect →**

**CONTACT**
**a Dell Technologies Expert →**

**VIEW MORE**
**Healthcare Security resources →**

**JOIN THE CONVERSATION**
**with #PowerProtect →**

DELL Technologies

**Connect** on social

Copyright © 2023 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.