Improve cyber resiliency and protect data from cyber ransomware threats by using an isolated vault, AI-based ML analytics software, and more

With Dell Technologies PowerProtect Cyber Recovery with CyberSense

As the frequency of cyber threats continuously grows and attack methods evolve, data protection plans must take an approach that secures and analyzes all IT components, from the most superficial to the deepest reaches. Dell PowerProtect Cyber Recovery can help protect the most critical and sensitive data while also helping ensure proper recovery in the face of a cyberattack or another disruptive event.

Dell PowerProtect Cyber Recovery is a data management, protection, and recovery solution that helps organizations protect their data and applications against ransomware, destructive cyberattacks, and unexpected events. The solution uses a multi-copy approach, meaning that after creating backups, it copies those backups to isolated storage for safeguarding and analysis. PowerProtect Cyber Recovery comprises many components, including one or more storage vaults, located either potentially on-premises in a PowerProtect DD (formerly known as Data Domain) appliance or in the cloud via software-defined Dell APEX Protection Storage for Public Cloud (formerly known as DD Virtual Edition). In both cases, the vault is operationally air-gapped, i.e., isolated from the production environment--potentially physically air-gapped in the case of the on-premises environment, and logically air-gapped in the case of the APEX environment. This makes it extremely difficult for bad actors or unauthorized users to log in and compromise backup copies.

PowerProtect Cyber Recovery also includes CyberSense, a fully automated and integrated intelligent security analytics engine that automatically scans data, files, databases, and images in the vault for signs of corruption from a ransomware attack. CyberSense provides full content analysis; takes observations from files to use as inputs for its artificial intelligence (AI)-based machine learning (ML) model; and detects malicious activity that includes mass deletions, encryption, and other suspicious changes in core infrastructure (including Active Directory and DNS), user files, and critical production databases that might indicate ransomware or a destructive attack. When CyberSense detects patterns of corruption, it generates an alert in the PowerProtect Cyber Recovery dashboard that gives additional information on the scale and impact of the attack.[1]

PowerProtect Cyber Recovery helps organizations mitigate cyberattacks, enhance data resilience with multiple copies of data backups from separate locations, reduce downtime, and maintain business continuity. This report uses publicly available data to highlight key data protection features and functionality and presents our findings from a competitive analysis of CyberSense.

Protect sensitive data

Encrypt immutable data in flight during backup replication to physically and logically isolated vaults

Detect SQL Server page corruption

CyberSense found an infection where a competing solution could not

Identify uncorrupted backup copies

CyberSense identified the most recent uninfected backup copy for recovery

Security

Dell PowerProtect Cyber Recovery offers several security features to help protect critical data from ransomware and other sophisticated threats, prevent unauthorized users from gaining access to sensitive information, and make recovery swift so organizations can resume normal operations.

The features and functionality of PowerProtect DD appliances are critical to the security, integrity, and recovery that PowerProtect Cyber Recovery solutions deliver. These features include:

1. **Immutability**
   Immutable data cannot be modified or deleted, only written. DD systems can write immutable backups on both production systems and in the Cyber Vault, which means if a bad actor should somehow gain access to the backup system, they cannot modify, delete, or compromise the existing protected copies.[2] Any backup that the DD system creates in the production environment is immediately immutable and available for IT to copy into the vault for added security. The next section in this report looks more at immutability.

2. **Retention Lock**
   The DD Retention Lock feature makes data immutable for a predetermined period. Once the solution places data under a retention lock, no user or system can alter, delete, or modify the data until the lock period expires.[3]

   Retention Lock has governance and compliance modes. Its compliance mode can enable customers to meet many regulatory standards. An independent third party attested that DD Retention Lock meets storage requirements specified in SEC Rules 17a-4(f)(2) and 240.18a-6(e)(2) and FINRA Rule 4511(c).[4] This capability can also help to support an organization's efforts to comply with FDA 21 CFR Part11, Sarbanes-Oxley Act, IRS 98025 and 97-22, ISO Standard 15489-1, and MoREQ2010.[5]

   Because attackers could attempt to circumvent Retention Lock by changing a system's clock, which would cause the solution to delete files earlier than expected, DD has an internal security clock. The system regularly compares the times of the security and system clocks. If there is an accumulated two-week skew between the two in a single calendar year, the system automatically disables the DD File System (DDFS) to prevent access to data.[6]

3. **Encryption of data in flight with DDBoost**
   Data in flight can pose a significant security risk. DDBoost limits the amount of data in flight by enabling the backup server or application client to send only unique data segments, rather than all data, across the network to the DD appliance. In addition, organizations can use the DDBoost protocol with or without certificates for authentication and encryption of data. Certificates offer a more secure data-transport capability. In-flight encryption enables applications to encrypt in-flight backup or restore data over LAN from the system. The client can use Transport Layer Services (TLS) to encrypt the session between the client and the system.[7]

4. **DD Operating System (DD OS) security**
   DD security features extend to the operating system as well. DD OS implements custom access controls and restrictions on the Bash shell for security purposes. The restricted Bash shell mode allows users to perform only a set of predefined commands necessary for their roles and tasks. DD OS enhances data integrity by blocking undefined commands that make unauthorized or unintended modifications to the system.[8]

5. **Role-based access control (RBAC) and DD Filesystem (DDFS) security**

   DD systems use several measures to protect files and data within the filesystem. First, DD systems provide RBAC, which enables administrators to define roles with specific privileges and assign users to those roles. Only authorized users with appropriate privileges can access the appliance and its data. This ensures that users have access to only the functions and data they need to perform their tasks, reducing the risk of unauthorized access or accidental data exposure.

   DDFS also uses hashing for data integrity verification. Hashing transforms a given key or string of characters into another value. The appliance stores unique data chunks in logical storage containers, and the filesystem hashes both the data chunks and the containers. When the system retrieves data, it recalculates the data's hash value to match the stored hash value in DDFS, which helps ensure that nothing has tampered with or corrupted the data.[9]

6. **Dual-role authorization**

   When an organization enables DD Retention Lock compliance mode, the DD system provides additional administrative security in the form of dual sign-on. This means that both the system administrator and a second authorized user (e.g., the Security Officer) must sign on together. The dual sign-on mechanism of DD Retention Lock compliance mode functions as a safeguard against any actions that could potentially compromise the integrity of locked files before the expiration of the retention period.[10]

7. **Data Invulnerability Architecture**

   The DD OS provides end-to-end verification, fault avoidance and containment, continuous fault detection and healing, and file system recoverability to safeguard against problems with data integrity caused by hardware and software malfunctions. When the DD system receives write requests from backup software, it first analyzes a data segment for redundancy by calculating the fingerprint for the data segment and comparing it with existing fingerprints stored in the system. It stores only unique data segments and their fingerprints to disk. DD then continuously reads data back from disk, recalculates the fingerprint it reads back, and ensures it matches the fingerprint on the disk. The DD system conducts a self-healing process to reconstruct corrupted data and restore data to its correct state if the system detects corruption during this process (i.e., if what it reads back does not match what is written). In addition, the self-healing process helps protect the system against other changes that could impact the integrity of the platform.

Immutability*

Making backups immutable, and thus read only, ensures that an organization can trust these backups for recovery. Operationally, immutability helps maintain data authenticity and reliability.

*Dell's products are designed to support customers' efforts to secure their critical data. As with any electronic product, data protection, storage, and other infrastructure products can experience security vulnerabilities. It is important that customers install security updates as soon as they are made available by Dell.

How it works

DD systems provide immutability in how they store data using MTrees. MTrees are logical partitions of the filesystem. When an application writes data to an MTree, the DD system uses a feature called Fast Copy to create a point-in-time copy of the original MTree to a new MTree. Within the new MTree, DD applies Retention Lock to ensure that a user or process cannot delete the new MTree for the duration defined by the Retention Period. The new MTree is an immutable copy of data and is independent from the original MTree.[11]

PowerProtect Cyber Recovery solutions also use MTree replication to copy immutable data copies from a production DD to another DD in the vault via the DDBoost protocol.[12] In the initial synchronization between the two DDs, the solution copies all data to the vault DD. Each subsequent synchronization will copy only new and changed data segments. CyberSense, which we'll discuss later in this report, scans all the immutable copies in the vault for potential corruption.

Approaches to immutability

The need to delete immutable backups is rare, but the scenario does occur. Organizations could potentially run into capacity and subsequent cost issues after accumulating immutable backups that they cannot delete. Storing backups can require a hefty amount of capacity, which in turn requires ongoing operating, management, and monitoring costs in addition to the initial hardware investment. Periodically deleting immutable backups can help solve those problems.

As we've noted, Dell PowerProtect Cyber Recovery offers immutability by leveraging Retention Lock and other tools. Retention Lock offers some flexibility as the two modes, Compliance and Governance, offer slight modifications in how customers can implement immutability. Immutability means users or bad actors cannot delete backups, but in certain cases, such as storage capacity issues, PowerProtect Cyber Recovery allows customers to delete them with Retention Lock – Governance mode.

In comparison to PowerProtect Cyber Recovery, how do similar offerings from other companies stack up? We looked at publicly available information for Cohesity Cyber Recovery, Veeam, Rubrik, and Veritas NetBackup. Except for Cohesity Cyber Recovery, the solutions can reside either on-premises or off (Cohesity is a cloud-based solution backed by AWS). Documentation for the four solutions claim to offer immutability, but noticeably, Rubrik and NetBackup have some differences from PowerProtect Cyber Recovery.

For Rubrik, administrators can delete backups, but not from the client side and only with certain controls in place. In addition, all writes are "out-of-place," meaning new writes never touch previously written data.[13]

Despite offering immutability, administrators or bad actors can delete the lock on backups within a NetBackup WORM-capable storage. They could then delete the image using the bpexpdate command.[14]

Isolation

Data isolation refers to the separation of and restricted access to data created by barriers or boundaries to prevent unauthorized access. Isolation uses temporary network connections instead of persistent connections.

Data isolation helps critical data remain unconnected from an infected network where a bad actor could try to modify configurations, delete data, change policies, or sniff network traffic for user credentials. Isolation also helps reduce the attack surface, giving bad actors fewer opportunities to gain access and control. Additionally, organizations can restrict access to only authorized personnel, which helps prevent unauthorized users from overwriting data.

In addition to the features that we noted, PowerProtect Cyber Recovery can provide both physical and logical isolation, in the form of operational air gaps, to help protect data. PowerProtect Cyber Recovery can use both a physical air gap, wherein the backup data is physically disconnected from the production network and stored in an isolated location, and a logical air gap, which relies on network access controls to separate the logically disconnected backup copies from the production environment. Having both types of air gaps is valuable because a logical air gap alone cannot stop an internal user with network access to the vault from accessing and compromising the data.

A physically isolated on-premises PowerProtect DD could function as the vault, in which users or systems from the production environment cannot access the components, and the vault is physically disconnected from the production network.[15] By eliminating access to the recovery environment from the production network, an organization can reduce its surface of attack. As noted, accessing the isolated data requires separate security credentials as well as multi-factor authentication (MFA).[16]

Approaches to isolation

Gartner states that, "Isolated recovery environments (IREs) with immutable data vaults (IDVs) provide the highest level of security and recovery against insider threats, ransomware and other forms of hacking."[17] They also note that an "IRE with an IDV does not replace, but rather complements, traditional backup and disaster recovery (DR) systems by delivering a tertiary immutable backup copy in an IRE equipped with all the tools, processes and resources to recover impacted systems."[18]

While reviewing publicly available information on the Cohesity, Veeam, Rubrik, and Veritas solutions, we found that each has at least a slightly different approach to IRE from PowerProtect Cyber Recovery. With the Dell solution, customers can physically or logically isolate their DD vaults from production to keep the control and data planes of production separate from the vaults. Additionally, PowerProtect Cyber Recovery automates air gaps, something that not all the other solutions do.

According to documentation:

- Cohesity Cyber Recovery offers only a dynamic automated logical air gap for their AWS-based FortKnox vault.[19]
- Veeam supports a logical air gap for public and private cloud providers via Veeam Cloud Connect, but it's not automated. Veeam also offers Veeam Hardened Repository, which functions as the on-premises vault for the solution and which organizations could configure to have a physical air gap.[20]
- Rubrik does not offer an automated air gap for Rubrik Cloud Vault, but customers can add a logical air gap through a third-party partnership with Microsoft.[21]
- NetBackup customers must manually enable a logical air gap and could create a physical air gap with an on- of off-premises solution.[22]

How it works

Figure 1 shows the networking paths of the isolated Cyber Recovery vault. Note that the vault has no management or control path to the production environment to reduce the attack plane.

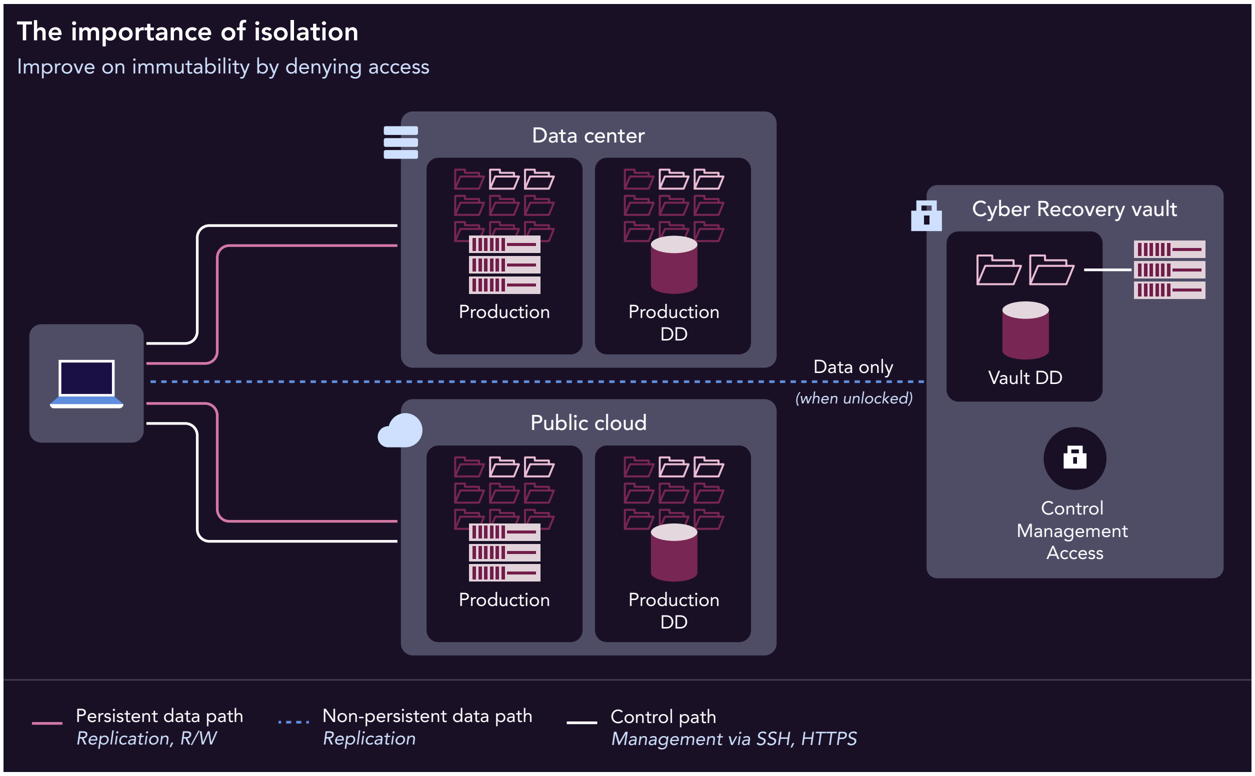


Figure 1: High-level data and control path architecture of the Cyber Recovery vault. Source: Principled Technologies.

The only required connection for the Cyber Recovery vault is a data path for periodic data synchronization. Synchronization is when the Cyber Recovery solution ingests data in short, policy-driven intervals for replication.[23] The PowerProtect Cyber Recovery Solution Guide states that "the base-level Cyber Recovery solution architecture consists of a pair of PowerProtect DD systems and the Cyber Recovery management host. In this base-level configuration, the Cyber Recovery software, which runs on the management host, enables and disables the replication Ethernet interface along with replication contexts on the PowerProtect DD system in the Cyber Recovery vault to control the flow of data from the production environment to the vault environment."[24] Dell suggests additional ways that organizations can secure and isolate data paths. We observed Cyber Recovery unlocking and locking the vault during and after replication in our testing.

For the physical implementation of the vault, Dell recommends "installing the Cyber Recovery vault equipment in a dedicated room or cage with physical access controls. This secured room should have a limited access list with key sign-out or two-person key access. Video surveillance of entry points into the cage or room and of the equipment should be in place. For the utmost security, the Cyber Recovery software must be accessible only by physical access to the Cyber Recovery management server and an associated keyboard and mouse."[25]

With the separation of the management and control paths, Cyber Recovery's physical and logical air-gapped isolation options distinguishes itself from other solutions. Some solutions allow access to their vault data from a production environment interface. This places the vault data on the same attack surface as the production data, potentially allowing bad actors to access backup copies using compromised credentials.

CyberSense

Protecting your data well requires a comprehensive strategy that provides security at every level. Despite all the self-healing, security, immutability, and isolation features of a Dell PowerProtect Cyber Recovery solution, less obvious attacks could still dive deeper into an enterprise infrastructure, such as at the data backup level, potentially going undetected until production data or an entire user group became compromised. Dell PowerProtect Cyber Recovery solutions provide a last line of defense against cyberattacks and an efficient approach to help expedite recovery via CyberSense. CyberSense is an analytics engine that uses AI-based ML analytics algorithms to scan and validate the integrity of backups in the vault and the user content of the files within the backups.

CyberSense runs inside the vault, isolated from the production environment. It monitors files, VM images, and databases inside the vault to determine if an attack has occurred by analyzing the data's integrity. Once the Cyber Recovery solution replicates backup copies to the vault and applies the Retention Lock feature, CyberSense automatically scans the copies, creating point-in-time observations of files, databases, and core infrastructure. The analytics engine scans the full content of files and each database page—not just metadata. Where other solutions look for changes in data thresholds or metadata, CyberSense looks within the contents of files to validate data integrity. These observations allow CyberSense to track how files and databases change over time and uncover many advanced types of hidden attack. CyberSense then generates analytics that detect patterns of corruption that might indicate bad actor activity, including encryption; deletion, creation, or obfuscation of files; and more.[26] Other solutions push analysis to the cloud, thus potentially widening the attack surface, whereas organizations can choose to run CyberSense on-premises or in one of the many cloud options that Cyber Recovery supports.

CyberSense combines over 200 analytics with data observations that become more useful over time as observations increase. The ML algorithm uses information about thousands of malware infections to find unusual patterns of behavior and distinguish user activity from ransomware, while minimizing false positives and negatives. The algorithm receives new education on things, such as attack variants, via ongoing research. Additionally, the ML algorithm receives updates based on real-life data from existing CyberSense customers.[27]

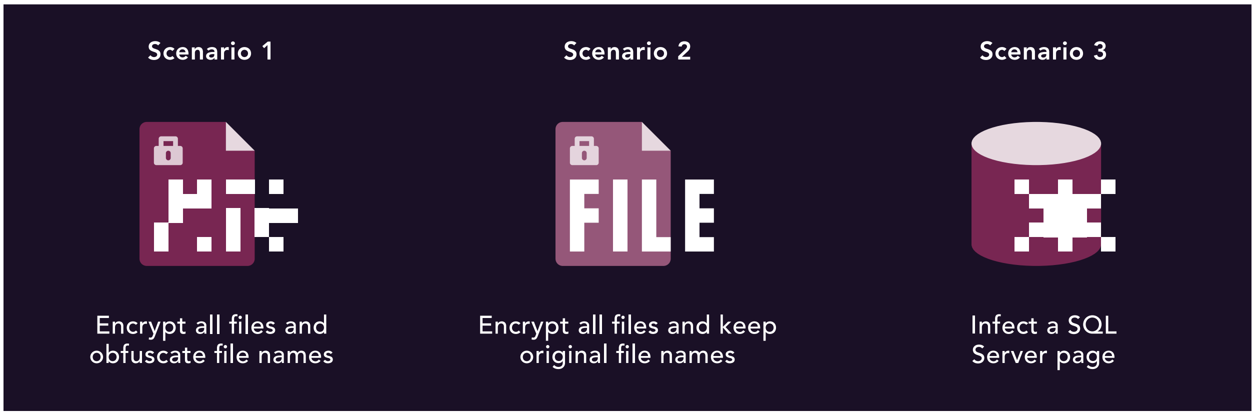
In addition, CyberSense supports indexing data in common disk backup formats from Dell, IBM, Commvault, and Veritas.[28] By supporting backup formats from other vendors, Dell demonstrates a willingness to meet customers where they are in terms of data backups.

We tested the ML-driven intelligent analytics software of two turnkey enterprise data protection and cyber recovery solutions: CyberSense for Dell PowerProtect Cyber Recovery on a Dell PowerStore™ 7000T and a similarly functioning tool from the data management platform of a competitor ("Vendor X") for a similarly sized appliance.

How we tested

We ran all tests remotely and had full control over and unfettered access to the testbeds. Both the Dell solution (including CyberSense, the PowerProtect Data Manager backup application, APEX Protection Storage (formerly known as DD Virtual Edition), and PowerProtect Cyber Recovery solution) and the Vendor X solution were located in an offsite data center lab.

On both solutions, we ran three script-based malicious event scenarios that targeted backups:



Scenario 1

Encrypt all files and obfuscate file names

Scenario 2

Encrypt all files and keep original file names

Scenario 3

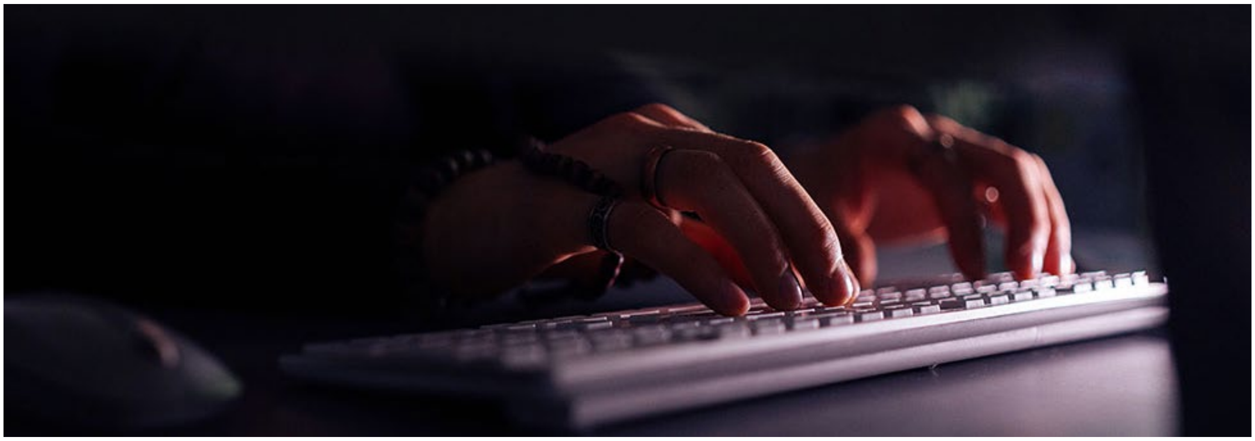
Infect a SQL Server page

Figure 2: Our testing scenarios. Source: Principled Technologies.

For both solutions, the first two scenarios followed the same general procedure. First, we created a full backup of all clean VMs on the Dell PowerProtect Data Manager and Vendor X storage appliances, created incremental backups for scanning, and verified that the target solution did not detect a threat. This gave us a baseline set of backups onto which we could execute the attack scripts.

Next, we executed the ransomware simulation script onto four VMs with different operating systems and application types, took new incremental backups on the target appliance, and checked to see whether the target analytics software detected the encryption threat.

For the third scenario (infect a SQL Server page), we followed a similar procedure as in the other two scenarios but instead focused on SQL VMs and used a page corruption script rather than an encryption script. We executed the script on a single VM.



What we found

Scenario 1: Detecting encrypted files with obfuscated file names

This scenario simulated a malicious event that encrypted files and obfuscated their names, which changed the metadata of the file in addition to its contents. This type of attack is typically known as ransomware, a security event where malicious software blocks access to a computer system until the owner or user of the system pays a predetermined amount of money. According to the US Cybersecurity and Infrastructure Security Agency (CISA), "[t]he economic and reputational impacts of ransomware and data extortion have proven challenging and costly for organizations of all sizes throughout the initial disruption and, at times, extended recovery."[29] Using intelligent analytics software to detect encryption in backups can strengthen any organization's data protection strategy, help protect valuable and sensitive information, and reduce the potential for costly downtime due to cyberattacks.

In our testing, both intelligent analytics applications discovered the encrypted files with changed file names. The Vendor X solution needed a baseline of 15 backups before it detected infections (one full backup and 14 incremental backups), whereas CyberSense detected infections after just one full backup, meaning that the Vendor X solution required 14 additional backups compared to CyberSense.

When the Vendor X solution alerted us to the suspicious activity, it indicated only that something had removed many files and added an equal number of files, which was suspicious activity based on the backup's entropy rating.[30] The Vendor X solution did not indicate that the files had been encrypted or that the file names had changed. In contrast, Cyber Recovery with CyberSense alerted us that something had encrypted and obfuscated file names.

The results for Vendor X could indicate a false positive. In other words, if we assume an organization runs daily backups with the Vendor X solution, they could have ingested 14 days of infected files before anomaly detection. In contrast, CyberSense needed only one baseline backup to alert with intelligence about the infection and its details. Recovery with Cyber Recovery at this stage in our example occurs from the isolated vault, assuring the organization that it did not expose the production network to the 14 infected backups as the Vendor X solution might have done.

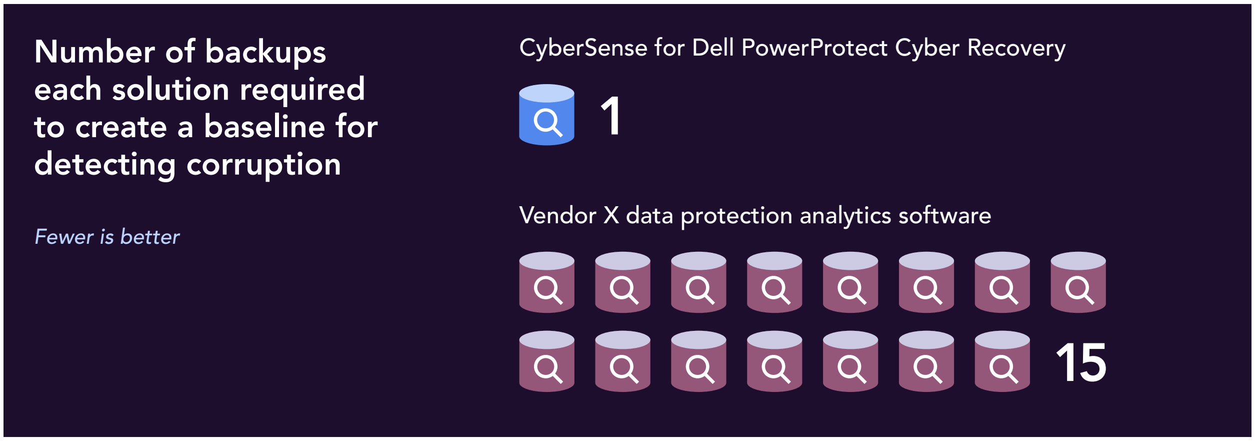


Figure 3: The number of backups each solution required to create a baseline for detecting corruption.
Source: Principled Technologies.

Scenario 2: Detecting encrypted files with original file names

This scenario was similar to the first scenario, but the script retained the original file names of the encrypted files. This change did not affect the files' metadata, only the files themselves. An act such as this could be timebomb ransomware, in which the attack remains dormant for a period before activating. Timebomb ransomware can evade detection and target backups, making the infected backups useless when the organization needs them.[31] Without changes in the metadata, the file may appear to be uninfected on the surface, helping keep the dormant attack hidden.

In our testing, both intelligent analytics applications discovered the encrypted files. Again, the Vendor X solution needed a baseline of 15 backups, including 14 incremental backups, before it could detect an anomaly. CyberSense needed a baseline of only one full backup before it detected an anomaly.

As in the first scenario, the Vendor X solution alerted us only that something had changed many files, which was suspicious based on the backup's entropy rating. It did not indicate that something had encrypted the files, while Cyber Recovery with CyberSense did tell us this. Detecting corruption in this way means CyberSense is looking at the contents of the files, not just the surface-level metadata. This type of scan adds another layer of security for your backups, and thus your digital infrastructure or estate overall. One might suggest that CyberSense is a "true" intelligent analytics application. Additionally, organizations might detect corrupt sooner with CyberSense as the solution needed significantly fewer backups to create a baseline. Depending on an organization's backup schedule, that could be many days sooner.

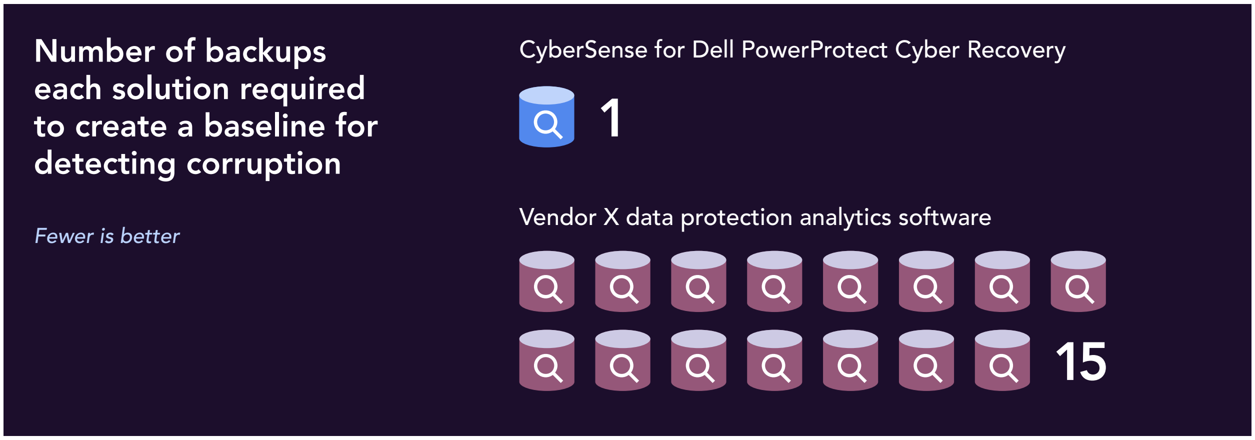


Figure 4: The number of backups each solution required to detect corruption. Source: Principled Technologies.

```
CREATE TABLE `cart` (
  `id` int(10) NOT NULL,
  `p_id` int(10) NOT NULL,
  `ip_add` varchar(250) NOT
  `user_id` int(10) NOT NUL
  `product_title` varchar(1
  `product_image` varchar(3
  `qty` int(100) NOT NULL,
  `price` int(100) NOT NU
  `total_amount` int(100
) ENGINE=InnoDB DEFAULT
```

Scenario 3: Detecting SQL Server page corruption

This scenario simulated a malicious event that corrupts a SQL Server page. In SQL Server, the fundamental unit of data storage is the page, and the database reads or writes whole data pages.[32] Again, this change did not affect metadata, just the files themselves. This type of attack is commonly known as a SQL injection, in which attackers target SQL data-based applications by injecting malicious code into SQL statements via web page input.[33] Even if infected, databases may continue to run. In addition to data theft, corrupting SQL Server pages can cause data integrity issues, data loss, and disruptions to database functionality. These outcomes can damage an organization's reputation, disrupt operational workflows, result in pecuniary loss, and even incur legal liability.

Although CyberSense and the Vendor X solution both detected the encryption in the first two scenarios, only CyberSense was able to scan deep enough to detect the corruption in the SQL Server page in this third scenario. This shows that while the two solutions offer similar detection abilities at some levels, CyberSense offers a deeper scan into backups for potentially business-critical SQL Server-based applications. In this way, CyberSense adds a layer of security resiliency with deeper scans and more comprehensive protection.

SQL Server powers many applications in financial, retail, health care, and other industries. Because SQL Server can function as the back end of development architecture, a SQL Server attack can result in downtime, interrupt operations, and potentially threaten the revenue these applications generate.

Restoring and recovering with Dell PowerProtect Cyber Recovery

The Dell cyber resilience strategy provides a broad range of recovery capabilities. These recovery options include common industry capabilities, such as instant access or traditional recovery from the immutable backups maintained in production. In addition, Dell enables unique recovery capabilities from the PowerProtect Cyber Recovery solution. Because PowerProtect Cyber Recovery maintains copies in isolation and scans them for integrity with CyberSense, organizations can access the copies immediately after an attack and use them to begin recovery steps or immediate restores to alternative recovery platforms, such as clean rooms.

Compare this immediate use case to an organization that can only access data in production or the public cloud. The organization cannot safely access data stored in the compromised area until they have determined and remediated the root cause; closed off bad actor persistence; taken forensic images for insurers and their legal department; rescanned the data; and have sufficient available infrastructure (AD, DNS) to access backup infrastructure. This process could take days or weeks based on the scope and sophistication of the attack.

How it works

During normal production, PowerProtect Cyber Recovery automatically creates restore points for recovery and security analytics. In the event of a cyberattack, Cyber Recovery uses its automated restore and recovery procedures and those restore points to bring business-critical systems back online. CyberSense and forensic reports help cybersecurity and recovery teams diagnose the impact of the attack. Once the production environment is clean and ready for recovery, Cyber Recovery provides the tools and technology that perform the actual data recovery.

Following a cyberattack, several data protection metrics come into play to determine the speed of recovery (the cyber recovery time or CRT) and the point in time to which users can return following a destructive attack (the cyber recovery point or CRP). For a Cyber Recovery solution, these metrics include the following:

- **Destruction detection objective (DDO):** This is a rolling window based on the amount of time between an attack and detection of the attack. Analytics and other Cyber Recovery mechanisms must operate within this period.
- **Destruction assessment objective (DAO):** This is the amount of time allotted to the cybersecurity team following an incursion to determine the scope of damage and potential responses.
- **Cyber Recovery synchronization interval:** This is the frequency at which the Cyber Recovery solution copies data from the production environment to the vault. The timing is based on a previously established recovery point objective (RPO) for the solution. The period of copy retention varies by solution, but typically ranges from one week to one month.
- **Cyber Recovery data copy count:** This is the number of data copies held in the Cyber Recovery vault. When paired with the synchronization interval, this metric gives a rough measure for how far back in time an organization can recover data, e.g., seven copies coupled with a 24-hour interval allow users to recover data up to one week old.

In addition to recovery requirements, the type of data that the solution protects can help determine the data synchronization interval and retention time. According to the Cyber Recovery Solution Guide, for the greatest recovery flexibility, users might categorize data that the solution protects in one of the following backup streams:[34]

- Binary and executable backups, including base-level operating system distributions and application builds
- Full-application and file-system backups, including images and application-specific data

These separate backup streams lead to two different recovery strategies:

1. **Restoring data and application binaries in the Cyber Recovery vault:** The solution identifies usable restore points, along with malware and where it has persisted, and decides whether to cleanse the malware from the backup image or rebuild using Cyber Recovery vault copies. After applying security patches, the solution restores data to a recovery host using the DR runbook for the application, then determines whether the recovery process has eliminated the effects of the malware. It then conducts a test run on the application using vault compute and cleanses or re-images the production environment. Finally, Cyber Recovery connects the recovery host to production and copies the application and data back to the production environment. Figure 5 shows this process.

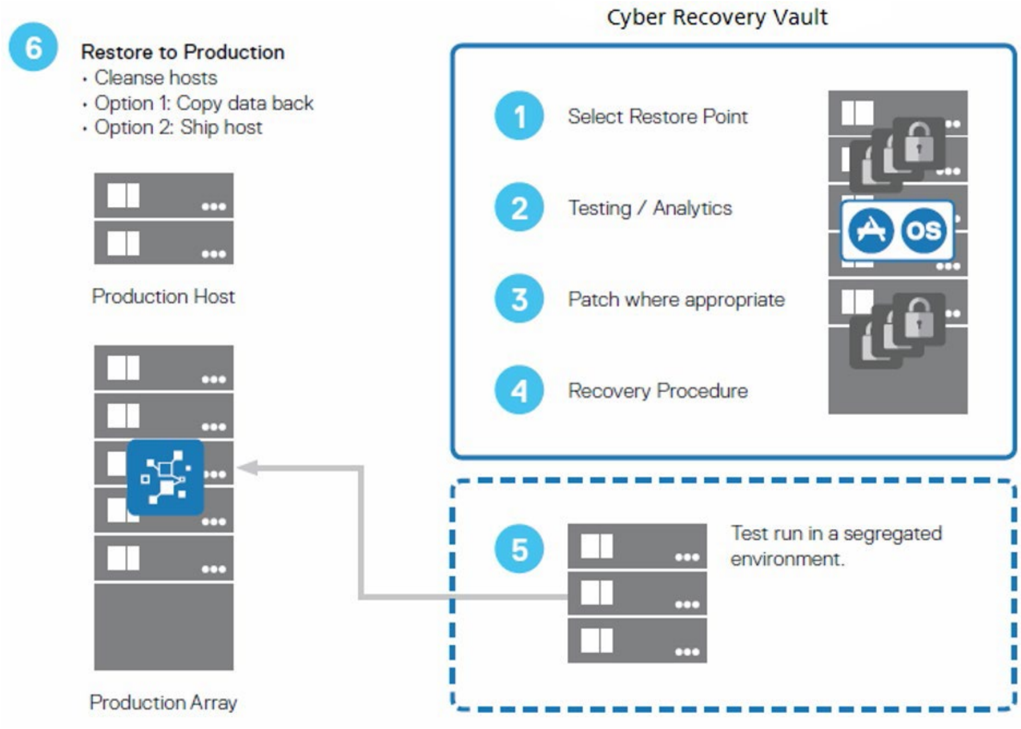


Figure 5: The process for restoring data and application binaries. Source: Dell Technologies.[35]

2. **Completely rebuilding from the Cyber Recovery vault:**
   In this approach, the Cyber Recovery solution reformats the production systems based on the level of damage determined by the forensics assessment during incident response. The solution then rebuilds binaries via copies in the Cyber Recovery vault and applies available security patches. Lastly, it restores appropriate copies of applications, data, and configuration files to the production environment using the associated DR runbooks for the application. Figure 6 shows this process.

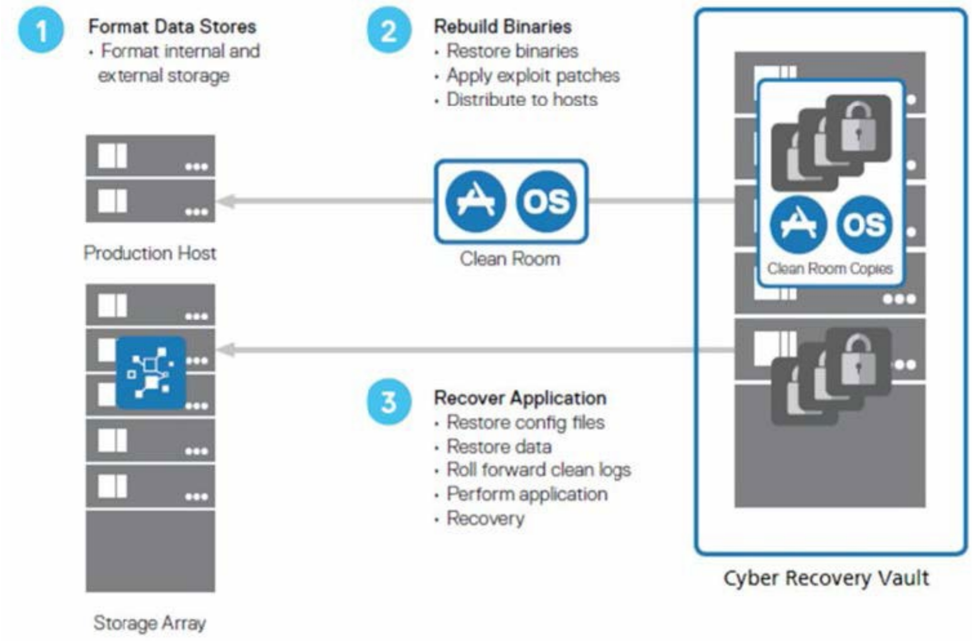


Figure 6: The process for completely rebuilding from the Cyber Recovery vault. Source: Dell Technologies.[36]

The Cyber Recovery solutions include physical or virtual recovery hosts (or both) that the Cyber Recovery software can use for recovery. These hosts include both a backup application recovery server, which is a designated server to which the backup application and backup application catalog recover, and an application recovery server. Organizations could deploy multiple servers depending on the recovery requirements of the solution. The Cyber Recovery software can expose sandbox (a testing environment for running new or untested software securely) data copies to any host to perform recoveries of data within the vault, such as file system data; IBM, Commvault, and Veritas backup data; or data protected by Dell NetWorker, Dell Avamar, a Dell PowerProtect DP Series Appliance, or Dell PowerProtect Data Manager software. After recovering a backup application within the vault, the solution can restore that data to additional recovery hosts in the vault.

Organizations size the backup application recovery server ahead of time so users can recover all backup applications that the Cyber Recovery solution protects. Similarly, the application recovery server is a designated server to which the solution recovers applications. Some applications might require customers to first recover other dependent applications. The infrastructure within the vault can support the recovery of the largest production application that the solution protects.

Conclusion

Organizations must consider many attack vectors when constructing a data protection plan. This includes protecting all data, but most importantly, the critical data imperative to operations. PowerProtect Cyber Recovery isolates the critical data and helps ensure proper recovery of data in the event of a cyberattack. Cyber Recovery uses ML-based analytics, in CyberSense, to determine the integrity of the data in the vault and identify clean backup data for recovery. In our testing, we found that PowerProtect Cyber Recovery detected infection in SQL database pages—something that a competing solution could not do. PowerProtect Cyber Recovery also required fewer backups than a competing solution to determine corruption in the data. In addition to all this and more, the Cyber Recovery solution delivers many recovery options, relying on uncompromised data from the vault for an efficient and smooth return to operations.

[1] Dell, "CyberSense® for PowerProtect Cyber Recovery," accessed September 8, 2023, https://www.delltechnologies.com/asset/en-in/products/data-protection/briefs-summaries/h18214-cybersense-for-dellemc-powerprotect-cyber-recovery-solution-brief.pdf.

[2] Dell, "Dell PowerProtect Cyber Recovery Solution Guide," accessed August 23, 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/h17670-cyber-recovery-sg.pdf.

[3] Dell, "Dell PowerProtect Cyber Recovery Solution Guide."

[4] Cohasset Associates, Inc, "Dell Technologies PowerProtect DD and DDVE – Compliance Assessment: SEC 17a-4(f), SEC 18a-6(e) and FINRA 4511(c)," accessed October 27, 2023, https://infohub.delltechnologies.com/section-assets/cohasset-dell-powerprotect-dd-compliance-assessment.

[5] Dell, "Data Domain: Retention Lock Frequently Asked Questions," accessed September 12, 2023, https://www.dell.com/support/kbdoc/en-us/000079803/data-domain-retention-lock-frequently-asked-questions-faq.

[6] Dell, "Data Domain: Retention Lock Frequently Asked Questions."

[7] Dell, "Encryption types offered by DD series encryption appliance," accessed September 8, 2023, https://infohub.delltechnologies.com/l/powerprotect-dd-series-appliances-encryption-software-1/encryption-types-offered-by-dd-series-encryption-appliance.

[8] Dell, "Dell EMC Data Domain – Security Configuration Guide," accessed September 11, 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/technical-support/docu91808.pdf.

[9] Dell, "Role based access control (RBAC) in Data Domain," accessed September 11, 2023, https://www.dell.com/community/en/conversations/data-domain/role-based-access-control-rbac-in-data-domain/647f70a9f4ccf8a8dee30f99.

[10] Dell, "Dell EMC Data Domain – Security Configuration Guide."

[11] Dell, "MTree replication," accessed September 11, 2023, https://infohub.delltechnologies.com/l/dell-powerprotect-cyber-recovery-reference-architecture/mtree-replication-3.

12. Veeam, "Dell EMC Data Domain - DataDomain MTree overview and limits," accessed September 11, 2023, https://bp.veeam.com/vbr/2_Design_Structures/D_Veeam_Components/D_backup_repositories/datadomain.html

13. Chris Wahl, "Recovering Fast from Ransomware Attacks: The Magic of an Immutable Backup Architecture," accessed December 13, 2023, https://www.rubrik.com/content/dam/rubrik/en/resources/white-paper/rwp-recovering-fast-from-ransomware-attacks.pdf.

14. Veritas, "NetBackup™ Security and Encryption Guide," accessed December 13, 2023, https://www.veritas.com/support/en_US/doc/21733320-149123528-0/v143394540-149123528.

15. Principled Technologies, "Dell EMC Cyber Recovery protected our test data from a cyber attack," accessed August 21, 2023, http://facts.pt/rkew01n.

16. Dell, "Dell PowerProtect Cyber Recovery," accessed September 12, 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/briefs-summaries/isolated-recovery-solution-overview.pdf.

17. Jerry Rozeman and Michael Hoeck, "Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware," accessed December 14, 2023, https://www.gartner.com/doc/reprints?id=1-27MOHCBD&ct=211011&st=sb.

18. Jerry Rozeman and Michael Hoeck, "Innovation Insight for Leveraging Isolated Recovery Environments and Immutable Data Vaults to Protect and Recover From Ransomware."

19. Nikitha Okmar, "Going Beyond the Air Gap - Data Isolation and Recovery for the Modern Era," accessed December 13, 2023, https://www.cohesity.com/blogs/going-beyond-the-air-gap-data-isolation-and-recovery-for-the-modern-era/.

20. Marco Horstmann, "How to protect your data from ransomware and encryption Trojans," accessed December 13, 2023, https://www.veeam.com/blog/how-to-protect-against-ransomware-data-loss-and-encryption-trojans.html.

21. Rubrik, "Rest easy with immutable, off-site data storage," accessed December 13, 2023, https://www.rubrik.com/products/rubrik-cloud-vault.

22. Veritas, "NetBackup Isolated Recovery Environment," accessed December 13, 2023, https://www.veritas.com/content/dam/www/en_us/documents/solution-overview/SO_flex_appliance_netbackup_ire_solution_V1543.pdf.

23. CSI Group, "Dell Cyber Recovery Vault (overview by CSI)," accessed August 23, 2023, https://youtu.be/ej5nZzWNRM0.

24. Dell, "Dell PowerProtect Cyber Recovery Solution Guide."

25. Dell, "Dell PowerProtect Cyber Recovery Solution Guide."

26. Dell, "CyberSense® for PowerProtect Cyber Recovery."

27. Dell, "CyberSense® for Dell PowerProtect Cyber Recovery – Powered by Index Engines," accessed September 13, 2023, https://www.delltechnologies.com/asset/en-us/products/data-protection/industry-market/cybersense-for-dell-powerprotect-cyber-recovery-whitepaper.pdf.

28. Index Engines, "CyberSense for Dell Cyber Recovery," accessed September 25, 2023, https://indexengines.com/csmatrix.

29. CISA, "#StopRansomware Guide," accessed August 1, 2023, https://www.cisa.gov/stopransomware/ransomware-guide.

30. "In security, most people use Shannon Entropy—a specific algorithm that returns a value between 0 and 8. The higher the number, the more random the data, and many times, a higher value means that the data is either packed or encrypted." Mueller, Clint, "How to Use Entropy Analysis in Penetration Testing," August 28, 2023, https://www.schellman.com/blog/cybersecurity/penetration-testing-methods-entropy.

31. Cooper, Steven, "How to Protect your Backups from Ransomware in 2023," August 1, 2023, https://www.comparitech.com/net-admin/protect-backups-from-ransomware/.

32. Microsoft, "Pages and extents architecture guide," accessed August 3, 2023, https://learn.microsoft.com/en-us/sql/relational-databases/pages-and-extents-architecture-guide?view=sql-server-ver16.

33. W3 Schools, "SQL Injection," accessed August 3, 2023, https://www.w3schools.com/sql/sql_injection.asp.

34. Dell, "Dell PowerProtect Cyber Recovery Solution Guide."

35. Dell, "Dell PowerProtect Cyber Recovery Solution Guide."

36. Dell, "Dell PowerProtect Cyber Recovery Solution Guide."

Read the science behind this report ▶

Principled Technologies®

Facts matter.®

This project was commissioned by Dell Technologies.

For additional information, review the science behind this report.