Abstract
This solution guide describes the components, features, and design of the Dell EMC PowerProtect Cyber Recovery solution. It includes information about the sizing and integration of solution components and planning the solution implementation.
Contents

Chapter 1  Executive Summary  4
Business case.............................................................................................................5
Document purpose..................................................................................................5
Terminology.............................................................................................................6
We value your feedback..........................................................................................6

Chapter 2  Solution Overview  7
Introduction............................................................................................................8
Dell Technologies Consulting Services ....................................................................9
Solution architecture ............................................................................................9
Key components ..................................................................................................11
Key features of the Cyber Recovery software ....................................................12

Chapter 3  Solution Design  13
Design overview..................................................................................................14
Server design considerations .............................................................................15
Network design considerations ...........................................................................16
Storage design considerations .............................................................................18
Physical environment design considerations ....................................................19
Cyber Recovery software limitations and considerations ....................................19
Mechanisms for data protection ........................................................................19

Chapter 4  Solution Implementation  21
Planning and sizing the environment .................................................................22
Setting up the core components .........................................................................29
Hardening the solution .......................................................................................29
Sheltered Harbor certification ............................................................................29
This chapter presents the following topics:

- Business case .......................................................... 5
- Document purpose ................................................. 5
- Terminology .......................................................... 6
- We value your feedback .......................................... 6
Business case

Across industries and among organizations of every size, cyberattacks are on the rise. As reported in *State of Cybersecurity 2018*, an ISACA global survey of cybersecurity professionals in late 2017 revealed that 50 percent of respondents were seeing a higher volume of attacks than in the previous year. Further, 80 percent of survey respondents anticipated that their organizations would experience a cyberattack in 2018.

As organizations become increasingly aware of the cybersecurity risks that threaten their mission-critical operations as well as their reputation, IT security has become an essential part of enterprise digital strategy. According to Gartner, by 2020, all large enterprises will be asked to report on cybersecurity at least annually to their board of directors, up from 40 percent in 2017.

Until recently, organizations have focused on trying to prevent cyberattacks, which come primarily from hacking and malware. However, the likelihood that all malware will be discovered before harm is done is slim, particularly for slow-moving and sophisticated attacks. This difficulty of detecting malware early gives hackers time to orchestrate attacks ranging from extortion to outright destruction of mission-critical systems. Such cyberattacks can cripple an organization, leading to revenue loss, negative publicity, and lasting customer distrust. As quickly as organizations build defenses against different attack vectors, hackers devise new ways to circumvent them.

Organizations require a comprehensive approach to cyber-risk mitigation. In addition to focusing on threat detection and remediation, they need to further develop and coordinate their incident response and associated data recovery strategies. The Dell EMC PowerProtect Cyber Recovery solution is designed to meet that need.

Document purpose

This solution guide provides a holistic view of the Dell EMC PowerProtect Cyber Recovery solution. It includes an overview of the solution’s features, key components, design, and implementation.

Scope

This guide includes an overview of the solution’s features, key components, and design, as well as the solution implementation process. For more information about the solution, see the following documentation on DellTechnologies.com:

- [Dell EMC PowerProtect Cyber Recovery Installation Guide](#)
- [Dell EMC PowerProtect Cyber Recovery Product Guide](#)
- [Dell EMC PowerProtect Cyber Recovery Security Configuration Guide](#)
- [Dell EMC PowerProtect Cyber Recovery Release Notes](#)

Audience

The audience for this guide is presales engineers, solution architects, and Customer Service engineers.
## Terminology

The following table provides definitions for some of the terms used in this solution guide.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Air-gapped</td>
<td>Physically isolated from an unsecure system or network.</td>
</tr>
<tr>
<td>Cyber Recovery policy</td>
<td>Combination of objects (such as Dell EMC Data Domain systems and applications) and jobs (such as synchronization, copy, and lock). A policy, which can be scheduled, orchestrates the workflow between the production environment and the Cyber Recovery Vault (CR Vault).</td>
</tr>
<tr>
<td>Cyber Recovery Vault (CR Vault)</td>
<td>Secure location at the customer's site, which is the target for Data Domain MTree replication. The CR Vault requires at least one Data Domain and a dedicated network.</td>
</tr>
<tr>
<td>Logical air gap</td>
<td>Physical connection but logical isolation from the network.</td>
</tr>
<tr>
<td>Sandbox</td>
<td>Read/write fast copy (clone) of files and directories that are in the CR Vault.</td>
</tr>
<tr>
<td>Synchronization</td>
<td>Data Domain MTree replication between at least one Data Domain system on the production network and one Data Domain system in the CR Vault.</td>
</tr>
</tbody>
</table>

**Note:** Any references to Data Domain systems in the documentation covers existing Data Domain systems as well as newer PowerProtect DD systems moving forward.

## We value your feedback

Dell technologies and the authors of this document welcome your feedback on the solution and the solution documentation. Contact the Dell Technologies Solutions team with your comments.

**Authors:** Raghav Sachdeva

**Contributor:** Penelope Howe-Mailly
Chapter 2 Solution Overview

This chapter presents the following topics:

- Introduction ......................................................................................................... 8
- Dell EMC Consulting Services ........................................................................... 9
- Solution architecture .......................................................................................... 9
- Key components ............................................................................................... 11
- Key features of the Cyber Recovery software ................................................ 12
Introduction

Dell EMC PowerProtect Cyber Recovery focuses on the protection and recovery pillars that are referenced in many well-known cybersecurity frameworks. This solution is a combination of professional services and technology that provides the following key elements:

- **Planning and design**—The solution planning and design phase includes an assessment of mission-critical systems and applications, current infrastructure, cyberattack recovery time, and recovery objectives. Optional Dell Advisory Services can help organizations determine their business-critical systems and create dependency mappings with associated foundation services, metadata, and other components that are needed to bring critical business systems back online. Dell Consulting Services experts work with organizations to determine recovery objectives and design solutions that economically meet organizational requirements. These services are optional and can be carried out by the organization that is implementing the Cyber Recovery solution.

- **Isolation and replication**—Based on the outcome of the planning and design phase, a tailored Cyber Recovery solution with Dell EMC Data Domain MTree replication technology is implemented. MTree replication synchronizes data between the production environment and the air-gapped CR Vault. Immutable restore points that are automatically created within the CR Vault can be used for recovery and analytics after being copied to a read/write Dell EMC Data Domain MTree.

- **Vault analytics**—The CR Vault offers distinct advantages for analytics in an offline and controlled environment; however, the CR Vault is not a substitute for good endpoint and cybersecurity tools. Organizations can use various existing Dell Technologies and the CyberSense feature, for analytics in the CR Vault. Cyber Recovery provides a workflow to trigger the CyberSense indexing and analytics process. Because real-time protection solutions are not 100 percent effective, data that is protected in the CR Vault might have already been attacked. Adding CyberSense analytics to the CR Vault enables discovery of corrupt files so that they can be replaced with the last known good version. CyberSense is fully integrated with the Cyber Recovery solution for ransomware protection. Dell Technologies uses the backup workflow to copy and secure critical business records in an isolated vault using backup software such as the NetWorker, Avamar, and PowerProtect Data Manager applications. When data is replicated to the CR Vault, CyberSense scans the backup image and generates analytics, without the need for the original backup software in the CR Vault. Analytics examines the files and databases to uncover unusual behavior that is indicative of a cyber-attack. This behavior includes file corruption, encryption of files or pages in a database, or deletions and creations.

- **Recovery**—Recovery procedures mostly follow standard processes, but special considerations apply across a variety of scenarios. The steps usually include invoking a cyber-incident response plan, performing forensics and damage assessment, preparing the recovery, cleaning out the malware or rebuilding systems from gold-copy images of application and operating system binaries, and then recovering the data back into the production environment.
The Cyber Recovery solution provides management tools and the technology that performs the actual data recovery. It automates the creation of the restore points that are used for recovery or security analytics. Dell Implementation Services provide CR Vault design and implementation. Dell Advisory Services can design an effective recovery strategy.

Organizations can dramatically reduce their surface of attack from inside and outside threats by removing the cyberattack recovery environment from the production network. The only required connection is a data path for periodically synchronizing the data, which is brought online only for data synchronization. This logical air gap provides another layer of defense by reducing the surface of attack.

The Cyber Recovery software automates the recovery procedure for the NetWorker and PowerProtect Data Manager applications.

Dell Technologies Consulting Services

Dell Technologies offers the following Consulting Services for customers who want to deploy this solution:

- **Cyber Recovery Workshop**—A 1-day business workshop that assists customers in understanding cyber recovery best practices and providing recommendations for designing a customized Dell EMC PowerProtect Cyber Recovery solution. Deliverables include:
  - Cyber threat vectors, real-world examples of emerging cyberattacks, and strategies for recovery
  - Summary of priorities and cyber-recovery recommendation

- **Cyber Recovery Advisory**—A 1-week detailed exploration of the customer’s most critical data assets. Deliverables include:
  - Cyber threat vectors, real-world examples of emerging cyberattacks, and strategies for recovery
  - Recovery strategic considerations, best practices, and potential solutions
  - Prioritized recommendations for cyber-recovery preparedness

- **Cyber Recovery Advisory and Roadmap**—A 4-week engagement to design a customer-tailored strategy and solution. Deliverables include:
  - Cyber threat vectors, real-world examples of emerging cyberattacks, and strategies for recovery
  - Maturity rating
  - Tailored strategy and solution
  - Actionable roadmap for cyber-recovery preparedness

Solution architecture

The following figure shows a high-level view of the Cyber Recovery solution architecture. Production data that is destined for the CR Vault environment is stored in a production-based
Data Domain MTree and periodically synchronized to the Data Domain system in the CR Vault. Synchronization creates multiple immutable copies for subsequent security analysis.

Figure 1. High-level solution architecture

As shown in the following figure, the base-level Cyber Recovery solution architecture consists of a pair of Data Domain 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 on the Data Domain system in the CR Vault to control the flow of data from the production environment to the vault environment.

Figure 2. Base-level solution architecture
You can customize the base-level solution by:

- Using a data diode from OWL Cyber Defense Solutions for secure one-way communication from within the vault environment to the production environment for UDP Protocols such as SMTP and SNMP alerts. For more information, see [OWL Data Diodes](#).
- Setting up a ZeroTrust Network within the Vault Environment using Unisys Stealth.
- Installing a firewall on the replication data path to ensure that only expected data traffic can traverse the secure link into the vault. The link must connect directly to the CR Vault Data Domain system and not go through the CR Vault switch.

### Key components

The key components of the Cyber Recovery solution are:

- **Source (production) Data Domain system**—The source Data Domain system contains the production data to be protected by the Cyber Recovery solution.

- **Destination (vault) Data Domain system**—The Data Domain system in the CR Vault is the replication target for the source Data Domain system.

- **Cyber Recovery software**—The Cyber Recovery software orchestrates synchronization, manages and locks the multiple data copies that are stored on the Data Domain system in the CR Vault, and orchestrates recovery. The software also governs the optional process of performing analytics on the data that is stored on the Data Domain system in the CR Vault using the CyberSense feature.

- **MTree replication**—MTree replication is a Data Domain feature that copies unique data from the source Data Domain MTree to the Data Domain MTree in the CR Vault.

- **Retention Lock (governance or compliance) software**—Data Domain Retention Lock software provides data immutability for a specified time. Retention Lock functionality is enabled on a per-MTree basis, and the retention time is set on a per-file basis. Retention Lock is not mandatory for Cyber Recovery but is strongly recommended as an additional cyber-resiliency measure.

- **Cyber Recovery management host**—The management host is where the Cyber Recovery software is installed. This server is installed in the vault environment.

- **Recovery host**—The recovery host is a vault-environment component to which the backup application and data are recovered. Typically, the vault environment includes multiple recovery hosts.

- **Analytics/indexing host**—The analytics/indexing host is an optional but strongly recommended component in the vault environment. An analytics/indexing host with the data-analysis software that is installed provides direct integration between the Cyber Recovery software and the CyberSense software. Additional analytics/indexing hosts with different tools can also be used as needed.
Key features of the Cyber Recovery software

The Cyber Recovery software, which runs in the vault environment, controls the replication interface on the Data Domain system in the CR Vault as well as the Data Domain data copies in the CR Vault. The software is built on a secure microservices architecture and provides the following key features:

- HTML5-based UI built on the Dell Clarity standard
- REST API implementation
- Command-line interface
- Informative dashboards showing system alerts, CR Vault state, and other critical details
- Ability to transmit alerts through the SMTP to an environment outside the CR Vault
- Cyber Recovery policy creation and management, including scheduling
- Recovery assistance and the ability to easily export data to a recovery host
- Automated Recovery options for the NetWorker and PowerProtect Data Manager applications
- Integration with the CyberSense software for detection of backup data that has been tampered with, including scheduling
Chapter 3: Solution Design

This chapter presents the following topics:

Design overview........................................................................................................14
Server design considerations ..................................................................................15
Network design considerations ...............................................................................16
Storage design considerations ...............................................................................18
Physical environment design considerations.......................................................19
Cyber Recovery software limitations and considerations ..................................19
Cyber Recovery supports several design variants based on the level of required cyber-resiliency. The design that you ultimately implement depends greatly on your environment and requirements. This chapter highlights a base design and describes options that you can add to the base design. While not required, Dell Cyber Recovery Advisory Services can increase confidence that the Cyber Recovery solution meets your business objectives.

As part of a base-level design, the following environments are configured:

- **Production environment**—Production data to be protected by the Cyber Recovery solution must be stored on a Data Domain MTree in the production environment.

- **CR Vault environment**—The CR Vault environment contains a Data Domain system and the Cyber Recovery management host that runs the Cyber Recovery software. Data from the production environment enters the CR Vault environment through Data Domain MTree replication. This environment can also contain various recovery and analytics/indexing physical or virtual hosts that integrate with the solution.

The production and vault environment networks are not directly connected to each other, except for a replication data link between the Data Domain systems in the two environments. The solution also provides for an optional dedicated link from the Cyber Recovery management host in the vault environment to the production network operations center or security operations center for events reporting.

The Cyber Recovery solution frequently includes the following additional CR Vault components:

- Analytics/indexing hosts (physical or virtual) that the Cyber Recovery software can use to perform data analysis. One example is an analytics host that is installed with the CyberSense software and integrated with the Cyber Recovery software. For details, see the *Dell EMC PowerProtect Cyber Recovery Product Guide*.

- Recovery hosts (physical or virtual) that the Cyber Recovery software can use to perform a recovery. The Cyber Recovery software can expose sandbox data copies to any host to perform in-vault recoveries of data such as data that is protected by Dell EMC NetWorker, Dell EMC Avamar, Dell EMC DP4400 Integrated Data Protection Appliance, or Dell EMC PowerProtect Data Manager software, third-party backup data, and file system data. After recovering a backup application within the vault, you can recover application data that is stored by the backup application to additional recovery hosts in the vault.

In addition to these CR Vault components, consider including an SMTP server in the production environment for receiving Cyber Recovery alerts. Cyber Recovery can transmit alert details through the SMTP to a mailbox. This functionality requires one-way SMTP connectivity from the Cyber Recovery management server to the SMTP server. Alerts can be received by using one-way Data Diode device.
Server design considerations

Server infrastructure is installed in the vault environment and is not shared with or connected to the production environment. Keeping vault server equipment separate from the production environment helps ensure that any ongoing issues (cyberattacks, operational issues, and so on) do not propagate into the vault environment.

The following server types are part of the Cyber Recovery solution:

- Cyber Recovery management server
- Application analytics server
- Backup application recovery server
- Application recovery server

You can also implement additional server types, depending on your solution requirements.

The server infrastructure in the CR Vault can be deployed in multiple ways:

- Discrete physical servers
- VMware ESXi with or without VSAN
- Dell EMC VxRail appliance

The solution requirements help determine the infrastructure type to be deployed. For example, a VMware-based hyperconverged appliance such as VxRail simplifies server infrastructure management in the CR Vault. It also makes the solution more scalable should you need to add storage or compute for larger restores or additional analytics.

The Cyber Recovery management server is where the Cyber Recovery software is installed and from where the Cyber Recovery solution is managed.

For installation requirements and instructions, see the Dell EMC PowerProtect Cyber Recovery Installation Guide.

The analytics server is a designated server that you can use to check that the data being protected by the Cyber Recovery solution on the Data Domain system in the CR Vault is recoverable and intact. The type of analytics tools that are used depends on your solution’s analysis requirements. Cyber Recovery and the CyberSense feature provide direct, end-to-end analytics of certain datasets using the data stored on the Data Domain system in the CR Vault. Other analytics techniques might require that you rehydrate the data off the Data Domain system and restore it to an application recovery server before performing analytics operations against the data. For more information, see CyberSense for Dell EMC Cyber Recovery.

The backup application recovery server is a designated server to which the backup application (NetWorker, Avamar, DP4400 Integrated Data Protection Appliance or PowerProtect Data Manager, or other applications or combination of applications) and backup application catalog are recovered. Multiple servers can be deployed, depending on the recovery requirements of the solution. The backup application recovery server is sized so that you can recover all backup applications that are being protected by the...
Cyber Recovery solution. If the Cyber Recovery solution is protecting a physical, single-node Avamar system in a production environment, a single-node Avamar system also resides in the vault for recovery purposes.

**Note:** Cyber Recovery does not support Avamar grids and IDPA grid models (DP8000 series appliances). For more information, see Chapter 4: Solution Implementation.

**Application recovery server**

The application recovery server is a designated server to which applications are recovered. Some applications might require that you first recover other dependent applications. The infrastructure within the CR Vault is sized to support the recovery of the largest production application that is being protected by the Cyber Recovery solution. If an incident occurs, more than one application might have to be recovered, and choosing a balance between available capacity (compute, memory, storage) and cost would then be required.

**Network design considerations**

The air-gapped CR Vault environment has both a physical and logical separation from the production environment. The separation further reduces the attack surface of the CR Vault. The base-level design for the vault network starts with the vault having its own network switching infrastructure. No intervault communication is routable to any other environment. The only connectivity between the vault and another environment is as follows:

- Replication data link between the vault-environment and production-environment Data Domain systems
- Optional dedicated link from the Cyber Recovery management host in the CR Vault to the production network operations center or security operations center for events reporting

The Cyber Recovery software manages the replication link, and the connection is enabled only when new data must be ingested by the Data Domain system in the CR Vault. The Cyber Recovery software manages the link by enabling and disabling the replication port and replication context on the Data Domain system in the CR Vault. Therefore, the replication link on the Data Domain system in the CR Vault uses its own unique Ethernet interface. For the replication link that connects the production Data Domain system to the Data Domain system in the CR Vault, we recommend using the fastest link speed possible, preferably 10 Gb/s Ethernet (GbE). The amount of data to be stored in the CR Vault and the change rate of the data determine how long the replication connection stays live.

To secure the network links that connect the vault environment to the production environment, or any other network, we recommend that you install a firewall or other packet inspection tool on both the Data Domain replication link and the SMTP link. If a hyper-converged VMware appliance is installed in the CR Vault, the VMware NSX Distributed Firewall is a good firewall option for reducing complexity in the vault environment and protecting VMware-based infrastructure. Additionally, the VMware NSX Edge firewall is a potential software-defined option for protecting the Data Domain replication link between production and vault Data Domain systems at near wire speed.
The replication link between the production Data Domain system and the Data Domain system in the CR Vault should transfer only Data Domain replication traffic. For protocol and port details, see the Dell EMC Data Domain Security Configuration Guide. For the events reporting link from the Cyber Recovery management server to the production network operations center or security operations center, only the trusted outbound traffic should be permitted. For protocol and port details, see the Dell EMC PowerProtect Cyber Recovery Security Configuration Guide.

As an additional layer of security, a one-way VPN tunnel can be enabled for the events reporting connection. This tunnel allows only secure communications to be transmitted from the vault environment to the production environment. The VPN can be set up to allow access by specific users only. VMware NSX Edge VPN is a good option and supports IPsec and SSL. Dell Technologies’ ProDeploy Plus services can install and implement these tools.

In lieu of using a VPN tunnel for transmitting event details to the production network or security operations center, you can use a data diode to provide secure one-way communications from the vault. A data diode ensures that only one-way communication is possible, reducing the possibility of the vault environment becoming compromise. For more information, see OWL Data Diodes.

If other network links are required between the production and vault environments, secure those network links to the greatest extent possible by using a firewall, VPN, or data diode.

Set up a Zero Trust Network in the CR Vault using Unisys Stealth. Stealth is a “defense-grade” solution that uses identity-based segmentation. Network segments can be defined and managed by using an identity management system that has high business alignment, such as Active Directory or LDAP.

The Stealth principle is to trust no user or device (inside or outside the private network) and grant as little access as possible (always based on reliable identification).

When designing the network, also consider how to keep the vault environment time synchronized. If a reliable NTP time source is not available for the Data Domain system in the CR Vault, the Data Domain Retention Lock functionality might not function correctly. Time-of-day clocks on Intel- and AMD-based systems are not reliable; we have observed time skews of 24 hours or more. Either an NTP source should exist within the CR Vault or, with the appropriate security and access controls in place, an NTP source that is external to the vault should be allowed access to vault components. Your solution design requirements determine the better option. Additional options such as GPS-based systems might be available, depending on your environment.

DNS and Active Directory are commonly used critical components in any data center. In this solution, we do not recommend that production DNS or Active Directory instances extend into the vault environment. Such extension would require connectivity between vault and production components, which is not recommended. Instead, within the vault, separate DNS and Active Directory instances can be instantiated for only the vault components.

Note: Optionally, you can periodically copy production Active Directory and other foundation services into the CR Vault along with the business-critical data to enable recovery of those components.
For DNS, using host files is another, more secure option. Regardless of whether an Active Directory instance is implemented in the vault environment or local logins are used for vault components, passwords must be unique.

In addition, consider the bandwidth that will be required to support data recovery after a cyber-attack. Ensure that the bandwidth between the CR Vault and the recovery environment is sufficient to meet your solution’s recovery time objectives. If feasible, 10 GbE links, one for replication and two for recovery, should be available.

The following figure shows how network segmentation can be configured within the vault. The production side of the diagram is for illustrative purposes only.

![Figure 3. Example of Cyber Recovery network segmentation](image)

As shown in the figure, the only links that connect the CR Vault to the production environment are the replication network link and, optionally, the events-reporting network link. All connections that span both the production and vault environment should be secured by using a firewall, VPN, or data diode. Inter-vault communication is segmented based on the needs specified in the Cyber Recovery solution design. Unisys Stealth can provide network segmentation in the CR Vault.

### Storage design considerations

Each Cyber Recovery solution implementation requires its own storage design review. The review determines the amount of data that is to be protected in the CR Vault and the growth rate of the data. We recommend following the standard Data Domain sizing process to determine the optimal Data Domain model and capacity point. If you use Data Domain Retention Lock for storage of vault-environment data copies, you must account for the duration of data-copy retention when determining the size of the Data Domain system in the CR Vault. The longer that unique data must be retained on the vault Data Domain system, the more capacity the system requires.
Physical environment design considerations

A Cyber Recovery solution design must provide for sufficient physical security. The solution's vault environment is a secure enclave, and physical security is just as important as logical segmentation. An internal bad actor can take advantage of weak physical security.

We recommend installing the CR 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. If this is not feasible, monitoring the Cyber Recovery console through the cage (if the monitor is up and showing messages) is another possibility. Additionally, in conjunction with implementing a VPN, firewall, or other security tools, you can configure a jump server within the vault environment that allows a client in the production environment to securely access the Cyber Recovery management server.

Cyber Recovery software limitations and considerations

The Cyber Recovery software has its own design considerations that must be understood before a Cyber Recovery solution is implemented. Considerations include:

- Cyber Recovery supports up to five Data Domain systems in the CR Vault and a maximum of ten systems in all.
- Each production Data Domain MTree that is protected by using a Cyber Recovery policy requires three or more MTrees on the CR Vault Data Domain for the following purposes:
  - One as the replication destination
  - One or more for Retention Locked copies
  - One or more for read/write sandboxes

  **Note:** The CyberSense feature requires its own sandbox MTree in addition to any other sandbox MTrees.

- The solution supports MTree replication only, and the replication contexts must be set up before you create Cyber Recovery policies.

For details about the software design considerations, see the *Dell EMC PowerProtect Cyber Recovery Product Guide*.

Mechanisms for data protection

The Cyber Recovery software controls data synchronization from the production environment to the vault environment by using Data Domain MTree replication. After the datasets and their associated MTrees to be protected by the Cyber Recovery solution are determined, replication contexts are set up between the production and vault Data
Domain systems. MTree replication is designed so that all data within an MTree is replicated securely between two Data Domain systems. After the initial synchronization is completed and all data is copied to the vault Data Domain system, each subsequent synchronization operation copies only new and changed data segments. There is no limit to the number of MTree replication contexts that the solution supports; however, there are limits to the number of MTrees that each Data Domain model supports.

The Cyber Recovery software manages the synchronization of MTree replication contexts as well as the number of data copies it creates for each replication context on the Data Domain system in the CR Vault. The data copies that the Cyber Recovery software creates are possible recovery points if an incident occurs. If the Data Domain system in the CR Vault is licensed with either Retention Lock governance or compliance, the Cyber Recovery software can apply a Retention Lock for all files in the MTree based on the Cyber Recovery policy specifications. Retention Lock provides data immutability and is key to the Cyber Recovery software operations on the Data Domain system in the CR Vault. Enabling Retention Lock on data copies within the vault ensures that data copies can be trusted for recovery. The duration of the Retention Lock and the amount of data to which the Retention Lock is applied must be carefully understood. The Data Domain system in the CR Vault might reach capacity more quickly than planned if you disregard the values that are used during sizing. The two types of Retention Locks, governance and compliance, should be weighed against each other’s requirements. The most secure version should be implemented.

The Cyber Recovery solution uses the following additional mechanisms to further protect the data being stored in the CR Vault:

- Replication traffic in and out of the vault is encrypted using Data Domain encryption. For information about the replication technologies that are employed, see [Dell EMC Data Domain Replicator White Paper](#).
- Other data being sent to the production environment, such as Cyber Recovery alerts, can be encrypted using other tools.
- The Data Domain system in the CR Vault is disconnected (air-gapped) from the production network most of the time. The Data Domain system in the CR Vault is connected to the production Data Domain system only during the data synchronization operation.
- The CR Vault is set up as a separate security zone by using a VPN tunnel and a DMZ.
- Access to the CR Vault is limited using least-access-privilege concepts.
- Temporary access for recovery testing is set up just before testing and brought down immediately after testing.
- The CR Vault functions as an enclave and can operate without production IT services. Power and HVAC can be common to the rest of the environment.
- The data and binaries that are stored in the CR Vault can be analyzed forensically and in a nonexecutable format.
- Two-factor authentication can be implemented for access to critical vault components.
This chapter presents the following topics:

- **Planning and sizing the environment** .............................................................. 22
- **Setting up the core components** ................................................................... 29
- **Hardening the solution** .................................................................................. 29
- **Sheltered Harbor certification** ....................................................................... 29
Planning and sizing the environment

Proper sizing of a Cyber Recovery solution requires gathering many details about the current environment and determining the business-level solution requirements. Although not all-inclusive, this section addresses some of these considerations. Dell Consulting Services can assist you in sizing and implementing the Cyber Recovery solution.

Each organization implementing Cyber Recovery needs to determine the Cyber Recovery metrics and goals to regulate recovery; different metrics are used for Cyber Recovery than are used for traditional business continuity and disaster recovery. Organizations need to set time and recovery objectives to ensure a predictable recovery from an event.

The following data protection metrics are key in ensuring that the Cyber Recovery solution is properly sized and that the solution meets your design objectives:

- **Destruction detection objective (DDO)**—The amount of time between the point of incursion and when the incursion is detected. Cyber Recovery mechanisms (including analytics) must operate within the DDO rolling window.

- **Destruction assessment objective (DAO)**—The amount of time that is allotted to the cybersecurity team to assess damage after an incursion is discovered. The purpose of the assessment is to determine the amount of destruction and if the data can be cleansed or if a fallback to a previous data copy is required.

- **Data recovery point (DRP)**—The point in time to which you can return after a destructive cyberattack. This metric is analogous to a recovery point objective in a disaster recovery scenario. The DRP most commonly spans from days to months, depending on the dataset that is being protected by Cyber Recovery.

- **Data recovery time (DRT)**—The amount of time it takes to recover from an incident.

- **Cyber Recovery synchronization interval**—The frequency at which data is copied from the production environment to the CR Vault. This interval is based on the established recovery point objective (RPO) for the Cyber Recovery solution. For example, for an RPO of 24 hours, each day Cyber Recovery would synchronize data from the production Data Domain system to the Data Domain system in the CR Vault. In doing so, Cyber Recovery creates a point-in-time copy on the Data Domain system in the CR Vault for potential recovery. How long the copy is retained depends on the specific requirements of the solution but typically ranges from 1 week to 1 month.

- **Cyber Recovery data copy count**—The number of data copies held in the CR Vault. The data copy count, coupled with the Cyber Recovery synchronization interval, roughly translates to how far back in time data can be recovered. For example, with a 24-hour synchronization interval and seven data copies retained, data from the past 7 days can possibly be used for recovery.
In addition to determining the objectives for the Cyber Recovery solution, you must characterize the data to be protected. The Cyber Recovery solution can protect any data that can be stored on a Data Domain MTree. If Cyber Recovery is to protect an entire backup application and its backup data, the backup software must be able to store both its backup catalog (metadata) and backup data on one or more Data Domain MTrees.

**Note:** For Cyber Recovery to support Avamar data protection, the Avamar system must store its checkpoint on a Data Domain MTree, which is an option for all Avamar Virtual Edition and Avamar single-node implementations. If the Avamar system is not configured in such a way, you cannot reconstitute and restore Avamar protected data within the vault. Because Avamar grids store their checkpoints locally on the grid and not on a Data Domain MTree, Cyber Recovery cannot replicate Avamar grid metadata into the CR Vault using MTree replication. As a result, immutable copies of Avamar grid checkpoints cannot be created in the CR Vault system using the standard Cyber Recovery workflow. To enable Cyber Recovery to protect a subset of Avamar grid data, you can migrate specific datasets from a grid to an Avamar single-node or Avamar Virtual Edition instance and configure the instance to store its checkpoint on a Data Domain MTree.

To identify and characterize the data to be protected and to ensure that a thorough analysis is performed, you can use optional Dell Consulting Services. Details to be determined include:

- Mission-critical and business-critical applications that must be protected
- Characteristics and dependencies of each application, including host platform, location and amount of data, and Cyber Recovery objectives and metrics; in addition, any dependencies on core infrastructure services (such as DNS, LDAP, and Active Directory) that must be protected to ensure a successful recovery
- Data, such as application binaries, boot images, and backup catalog, that must be protected

These details, along with the previously defined objectives, help determine the ideal size of the Data Domain system in the CR Vault and an estimate of the time that will be required for data replication on an operational basis. The information also helps determine networking and compute requirements for the vault.

Recovery requirements and the type of data to be protected help determine the data synchronization frequency and data retention time. For example, for the greatest recovery flexibility, you might categorize data to be protected in one of the following backup streams:

- Full-application and file-system backups, including image-level (if possible) and application-specific data
- Binary and executable backups, including base-level operating system distributions and application builds

The following figure illustrates these two backup streams.
In the production environment, backups of applications and their data, including image-level backups, are typically performed daily. Backups are made to one or more Data Domain MTrees on the production Data Domain system. During solution sizing, the production MTrees to be protected are identified based on which applications and critical data must be protected in the CR Vault. If an MTree contains a large amount of data and the Cyber Recovery solution must protect only a subset of the data, we recommend copying the desired subset to a separate MTree. Dell EMC backup software can perform this operation with limited overhead. The Cyber Recovery software enables you to specify on an MTree basis the data synchronization frequency and retention time.

In addition to protecting application data, we recommend that you also protect binaries and executables to enable full reconstruction of an application if needed. If the production environment is subject to a destructive cyberattack that infects base-level operating system and application components, a complete re-creation of application hosts, beginning at the operating system level, might be necessary. Because cyberattackers can remain dormant within operating system binaries for a long time, the retention period for such data is typically measured in years.

Data analytics techniques

After the Cyber Recovery objectives and metrics are determined and the data to be protected is defined, a plan to confirm the validity of the vault data should be crafted. The list of techniques in this section is not all-inclusive, but it provides an overview of the types of analytics options that are available. Some of the analytics techniques require third-party software and associated infrastructure to run the software. The Cyber Recovery software and the CyberSense feature provide automated analysis of backup data in native format directly off the vault Data Domain system.
System-level analytics

System-level analytics focuses on analyzing that data copies are successfully created on the Data Domain system in the CR Vault. The goal is to ensure that the steps involved in synchronizing the data and creating immutable (Retention Locked) copies were completed successfully. System-level analytics provide assurance that the restore point is recoverable. This type of analytics also identifies health issues that are related to the overall CR Vault infrastructure and the Cyber Recovery software. System-level tools perform the required level of analysis and issue alerts when needed.

Anomaly detection

You can use anomaly detection tools to detect unusual patterns and then trigger alarms for further analysis. Anomaly detection is typically achieved through a combination of system-level, Dell EMC, and third-party analytics tools. System-level tools can examine two or more data copies that are stored on the Data Domain system in the CR Vault and, based on user-defined thresholds, identify unusual rates of change. For information about other types of entropy checking for ransomware, see the SANS Internet Storm Center InfoSec forums. Failed entropy thresholds could indicate encryption or wiping of data that is being synchronized to the CR Vault, or it could signal a benign change in the data.

You can establish processes to look for unexpected changes or new files in sensitive execution paths. Specialized tools can find anomalies in file systems, such as a change in a file without a change in the modification time, a change in sentinel records, or a failed entropy check. An anomaly can indicate that a file was manipulated, but anomaly detection tools might not identify the specific malware. When anomalies are detected, you should conduct further security analytics using malware scanning tools.

Application-level analysis

You can use application-level analysis tools to verify the integrity of the entire application or database stack, or both. This level of analysis requires a complete restore of the environment, and you must take caution to prevent rehydrating malware. Segregation of resources in the CR Vault can mitigate this risk. Tools and techniques are typically application-specific. For example, Oracle DBVERIFY and Exchange Eseutil can validate the overall integrity of an Oracle or Exchange instance. Because this activity requires downtime, running the utility inside the static CR Vault is preferred. You can use other tools, such as those that inspect sentinel records or run a read-only month-end report, to validate the integrity of the application itself.

Malware detection

You can use malware detection tools and methods to identify the malware that has been persisted to specific files and binaries. Many of the recent malware attacks have used a combination of traditional malware coupled with newer tools. To increase the efficacy of malware detection, you should use several detection methods. Signature-based and artificial-intelligence-based engines typically require a connection to a network and sometimes a cloud provider. To protect sensitive air-gapped systems, consider special designs such as secure VPNs. Common classes of malware-detection heuristics are:

- **Signature-based technologies**—Signature-based technologies that track known threats are less effective for zero-day malware, but they are still useful for identifying known malware distributions. When an anti-malware solution provider identifies an object as malicious, the object’s signature is added to a database of known malware. These repositories might contain millions of signatures that identify
malicious objects. Malware products use the repositories as the primary technique in identifying malicious objects.

- **Behavioral analysis**—Behavior-based malware detection evaluates an object based on its intended actions before an incident occurs. Statistical analysis and machine learning tools can determine if an object’s actual or potential behavior is suspicious. Attempts to perform actions that are clearly abnormal or unauthorized indicate that the object is malicious or, at least, suspicious. Evaluating for malicious behavior as it occurs is called dynamic analysis. Threat potential or malicious intent can also be assessed by static analysis, which looks for dangerous capabilities within the object’s code and structure.

### Other optional analysis techniques

Other techniques for analyzing data in the Cyber Recovery solution environment include:

- Monitoring the daily number of database logs or log file sizes for abnormalities
- Monitoring the vault Data Domain deduplication rate for abnormalities
- Monitoring manifest files and checksums (applicable to executables and historic data)
  - In the production environment:
    1. Create a manifest of all files in a file system.
    2. Create a checksum hash value for each file.
  - In the vault environment:
    - Compare the checksum to the original.
    - Investigate any file that cannot be read or that is not on the manifest. Either issue indicates a problem with the file.
- Validating NAS server file integrity with sentinel files:
  1. In the production environment, seed the file system with sentinel files (known filenames and values).
  2. In the vault environment, check for the expected values.
- Validating database recovery with sentinel records:
  To validate database recovery with sentinel records, use the same procedure as with NAS server files.

---

**Note**: Database software and reports might have to be modified to tolerate sentinel records.

---

**Recovery techniques**

If a destructive cyberattack requires a recovery, a plan must be formulated that specifies how data will be recovered and what infrastructure must exist in the vault to support the recovery operation. This section presents two of several potential scenarios.
Restoring data and application binaries in the CR Vault

You can restore data and application binaries in the CR Vault as follows:

1. Identify the restore points that were created before the attack occurred.

2. Using the forensic findings, identify the malware and where it has been persisted. If binaries or operating system images have been compromised, decide whether to cleanse the malware from the backup image and then restore the binaries from the vault Data Domain system. If you are not confident that cleansing will be successful, select a backup that was taken before the infection. If no clean copies of binaries exist in the generational backup images, you can rebuild using the CR Vault copies.

3. Apply security patches if possible.

4. Restore the data to a recovery host that is located within the CR Vault using the disaster recovery runbook for the associated application. Segment the application from the rest of the CR Vault infrastructure and then launch the application. Determine if the recovery process has eliminated the effects of the offending malware. This step is important when there is concern that the cyber-attack was based on multiple malware strains.

5. Test-run production applications using the CR Vault compute.

6. Cleanse or re-image the production environment and connect the recovery host to production (either logically or through physical shipment). Then copy the application and data back to the original production servers.

The following figure illustrates the restore process.

Figure 5. Process for restoring data and application binaries
Chapter 4: Solution Implementation

**Completely rebuilding from the CR Vault**

Completely rebuilding from the CR Vault is more comprehensive and conservative, but it is a slower recovery method. This method also minimizes concerns around dormant malware. The high-level steps for a complete rebuild are as follows:

1. Reformat the production systems based on the damage and forensics assessment that was done as part of the incident response.

2. Rebuild the binaries by restoring the appropriate CR Vault data copies. This recovery process is consistent with the previous scenario. Apply security patches if possible and distribute them to freshly formatted hosts.

3. Recover the application and data to the original production environment by locating and restoring the appropriate copy, restoring configuration files, restoring data, and performing application recovery using the disaster recovery runbook for the application.

The following figure illustrates the rebuild process:

![Diagram of the rebuild process](image)

**Figure 6. Process for rebuilding from the CR Vault**

Depending on the applications that are being protected by Cyber Recovery and on the extent of damage from the attack, the recovery process might vary. This guide does not address all nuances of the analytics and recovery plans, which are highly dependent on the environment and the solution requirements. Dell Consulting Services can provide customization details.

**Testing the recovery**

In addition to performing the recovery, you need a plan to enable authorized individuals to test the application recovery. How those individuals carry out the test can vary. If a jump box is configured within the vault environment, a user can log in to that server and then access the vault infrastructure to recover data. If a jump box is not configured, the user...
must be physically present within the vault environment to have access to the necessary equipment.

**Setting up the core components**

Setting up the core solution components involves:

1. Setting up the production and vault environments as described in this guide. Solution components—Data Domain systems and Networker, Avamar, or PowerProtect Data Manager software, or both—must be at the minimum or greater supported code level. For details, see the *Dell EMC PowerProtect Cyber Recovery Installation Guide*.

2. Identifying the MTrees on the Data Domain system in the production environment and then setting up the replication context between the Data Domain systems in the production and vault environments. If Cyber Recovery is to protect a backup application, the backup catalog (metadata), in addition to the backup data, must be replicated to the Data Domain system in the CR Vault.

3. Ensuring that the Data Domain system in the CR Vault has at least two interfaces enabled and in use—one for replication traffic and the other for management by the Cyber Recovery software in the vault.

4. Installing and configuring the Cyber Recovery software on the Cyber Recovery management server in accordance with the guidelines in the *Dell EMC PowerProtect Cyber Recovery Installation Guide*.

5. Ensuring that all data is secured both physically and logically, as described in Chapter 3: Solution Design, after it has been copied to the vault.

**Hardening the solution**

During solution implementation, ensure that all components in the vault are secured as best as they can be. Dedicated security guidelines might be available for some products that are installed in the vault environment; if so, follow the guidelines and lock down the products as best as possible. For example, disable unused ports and nonessential protocols, and use unique and limited-access credentials. Dell Services provides an offering that ensures that the Data Domain system is secured in accordance with best practices.

**Sheltered Harbor certification**

Sheltered Harbor was created to protect customers, financial institutions, and public confidence in financial systems if a catastrophic event like a cyberattack causes critical systems—including backups—to fail. Implementing the Sheltered Harbor standard prepares institutions to provide customers with timely access to balances and funds in this worst-case scenario.

Dell EMC PowerProtect Cyber Recovery for Sheltered Harbor is a Sheltered Harbor-endorsed solution for achieving compliance with data vaulting standards and certification, planning for operational resilience and recovery, and protecting critical data.
The following figure shows how the Sheltered Harbor solution protects against a cyberattack:

**Figure 7. Sheltered Harbor solution overview**

Dell Technologies is an early and committed member of the Sheltered Harbor initiative. The Dell EMC PowerProtect Cyber Recovery for Sheltered Harbor solution meets all technical product requirements for participants implementing the Sheltered Harbor standard.

For more information, go to [Sheltered Harbor](#) and contact your Dell Technologies sales representative.