Unisys Cyber Recovery for ClearPath Forward®

Protect and isolate critical data from ransomware and other sophisticated threats within ClearPath Forward MCP operating environments

Solution overview

Cybercrime, including ransomware, is rampant and is creating a significant data protection and recovery challenge for many organizations. Traditional backup and recovery approaches have proven insufficient for fending off these evolving threats.

Ransomware attacks cost organizations millions of dollars in lost revenue per day, damage reputations, and negatively impact stock prices. Cyber threats are expected to continue rising, primarily because of remote work and distributed work environments.

Most organizations already have strong data protection and detection capabilities in place. But could your organization recover if an attacker were to break through the perimeter and encrypt or delete your data? And if you could recover your data, how confident would you be in its integrity?

Organizations need to consider recovery as part of their cyber resiliency and risk management strategies.

Table of contents

Protect data and recover quickly

Given the frequency of ransomware attacks, a well-designed data isolation architecture is mandatory for mission-critical applications. This architecture should maintain multiple recovery point-in-time copies and include integrity checking to ensure data remains uncompromised.

Unisys Cyber Recovery for MCP protects and isolates critical data from ransomware and other sophisticated threats within ClearPath Forward® MCP Operating Environments. This modern approach keeps a copy of critical data off the network and creates multiple recovery points, ensuring an uncompromised gold copy is available for recovery.

What is Unisys Cyber Recovery for ClearPath Forward?

Unisys Cyber Recovery for ClearPath Forward leverages decades of experience in traditional data center services, including backup recovery and disaster recovery. Its specialized architecture enables restoring an environment compromised by a cyberattack quickly and safely.

Unisys IT experts use best practices to decide which data is critical, design secure recovery and restoration architectures, and create runbooks. This ensures you have a valid plan that quickly restores applications and services. Gain continuity while avoiding learning curve mistakes by drawing on Unisys' hands-on experience installing, configuring and running ClearPath environments. Additionally, benefit from the following fundamental solution attributes:

- **Isolation**: physical and logical separation of cyber recovery data to avoid contamination
- **Immutability**: the capability to preserve the integrity of data
- **Intelligence**: technology that finds malware threats
- **Security**: data protected in an air-gapped, network-connected vault
- **Documentation**: trained and prepared IT staff that uses documented and tested procedures to quickly clean and reimage servers and user systems

The specifics of how the cyber recovery solution is defined depends on your existing data backup solution and ClearPath deployment architecture. Figure 1 provides an overview of the main elements of the solution and the sequential flow of data through the solution. (Defaults are elaborated on in later sections.)

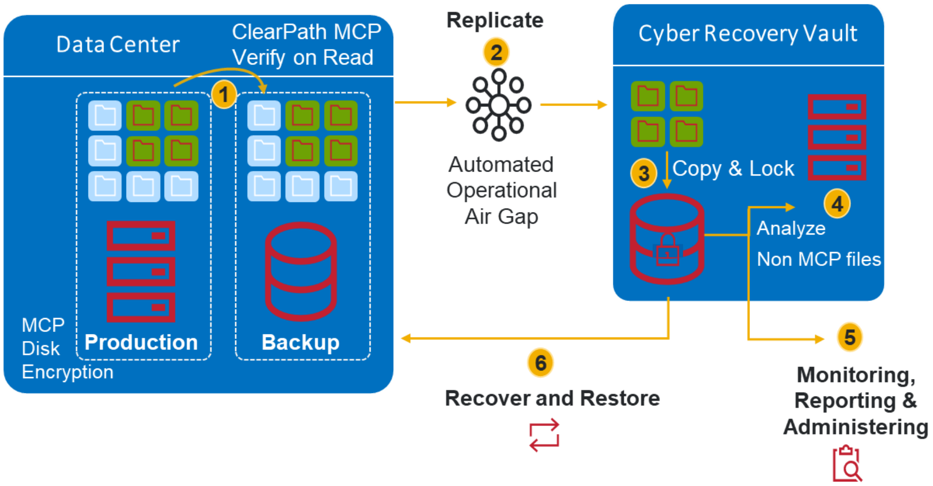


Figure 1. Solution Overview

The seven cyber recovery steps

1. Enable ClearPath MCP Disk Encryption to protect ClearPath data and detect tampering. Continue traditional backups as usual. As MCP Disk Encryption reads ClearPath data, it checks for tampering against the Cyclic Redundancy Check (CRC) stored with the data.

2. Replicate backups, typically daily, by copying data to a designated tape library in the Cyber Recovery vault. This process includes data de-duplication to minimize bandwidth and storage needs. This network connection is air-gapped to isolate the Cyber Recovery vault from outside attack.

3. Copy the data and apply retention locks to create an immutable copy.

4. Analyze any stored Windows and Linux data for tampering using software within the Cyber Recovery vault.

5. Throughout these steps, a secure outbound-only connection can report success/failure via email, and ongoing administration can be performed from a terminal on an isolated network.

6. Unisys provides a runbook documenting the steps needed to restore operations should a cyberattack occur. A malware-free gold copy is located, and recovery operations are initiated.

ClearPath MCP operating environment

Unisys provides a highly secure cyber recovery solution that meets modern cyber resilience requirements and sets the standard for fast, clean and secure recovery, minimizing downtime and associated inefficiencies. To offer the best protection against ransomware for your business-critical data, Unisys has partnered with Dell.

MCP Disk Encryption ensures data integrity by automatically validating MCP data every time it's read from the disk. This process detects data corruption, resulting in a clean gold copy securely placed into the vault. For data validation, MCP Disk Encryption is mandatory and requires that data be stored in the VSS-2/VSS-3 (Virtual Sector Size) disk formats.

Supported MCP environments

Deployment options for Unisys Cyber Recovery for ClearPath vary based on your specific ClearPath MCP system and backup method.

Unisys ClearPath MCP Cyber Recovery with Data Domain VTL

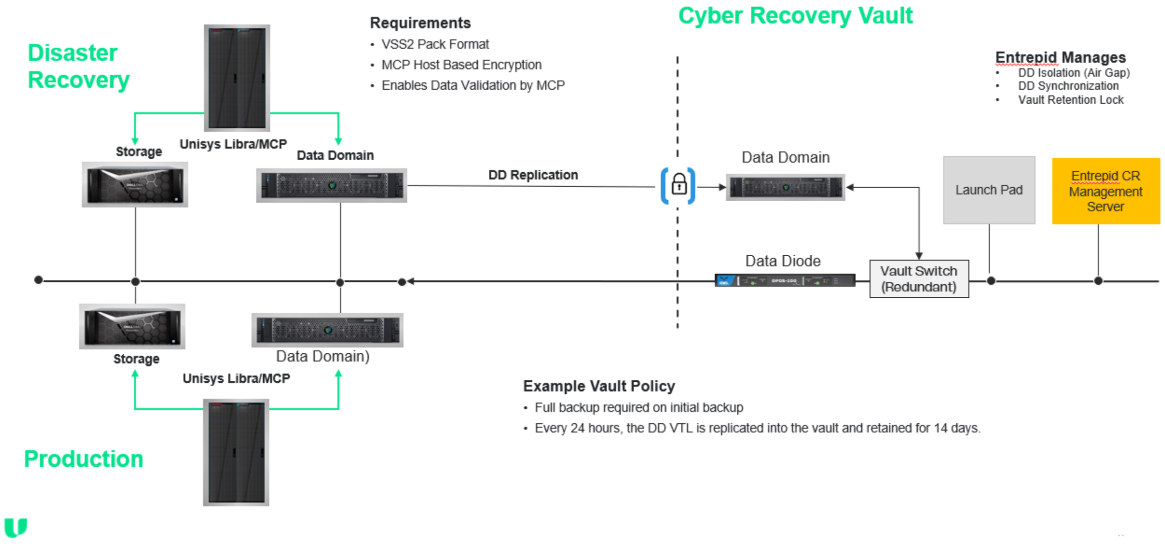


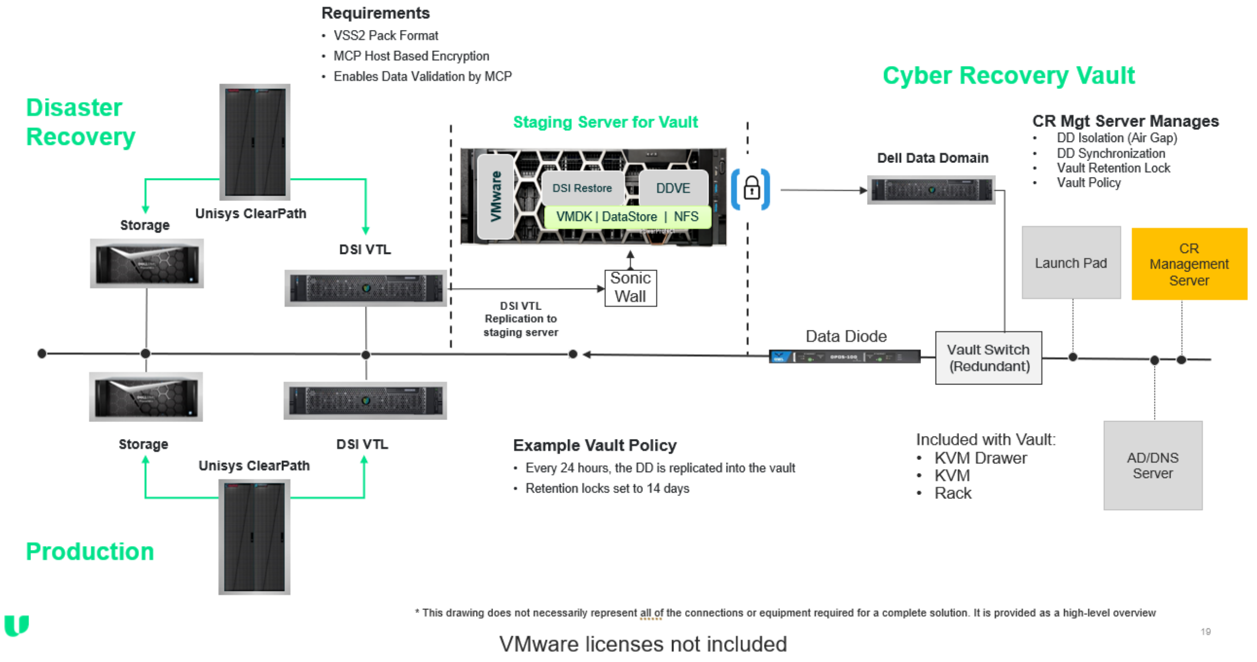
Figure 2. Cyber Recovery with Data Domain VTL

In the above Cyber Recovery architecture, MCP data is first checked for the presence of any malware/ransomware and then backed up to the Data Domain. This Data Domain is configured as a point-to-point connection to another Data Domain inside the vault and is protected by an air gap between them. The vault has no other connections except through this air gap.

The air gap allows only one-way traffic into the vault by activating the NIC during replication. Once replication is complete, the NIC is deactivated, re-establishing the air gap and preventing any inbound traffic to the vault.

For outbound transmissions, the vault uses a device called a data diode. This device supports one-way data communication exiting the vault. For instance, if the Data Domain inside the vault needs to “call home,” it would do so via the data diode.

Unisys ClearPath MCP Cyber Recovery with DSI VTL


Requirements

- VSS2 Pack Format
- MCP Host Based Encryption
- Enables Data Validation by MCP

CR Mgt Server Manages

- DD Isolation (Air Gap)
- DD Synchronization
- Vault Retention Lock
- Vault Policy

Example Vault Policy

- Every 24 hours, the DD is replicated into the vault
- Retention locks set to 14 days

Included with Vault:

- KVM Drawer
- KVM
- Rack

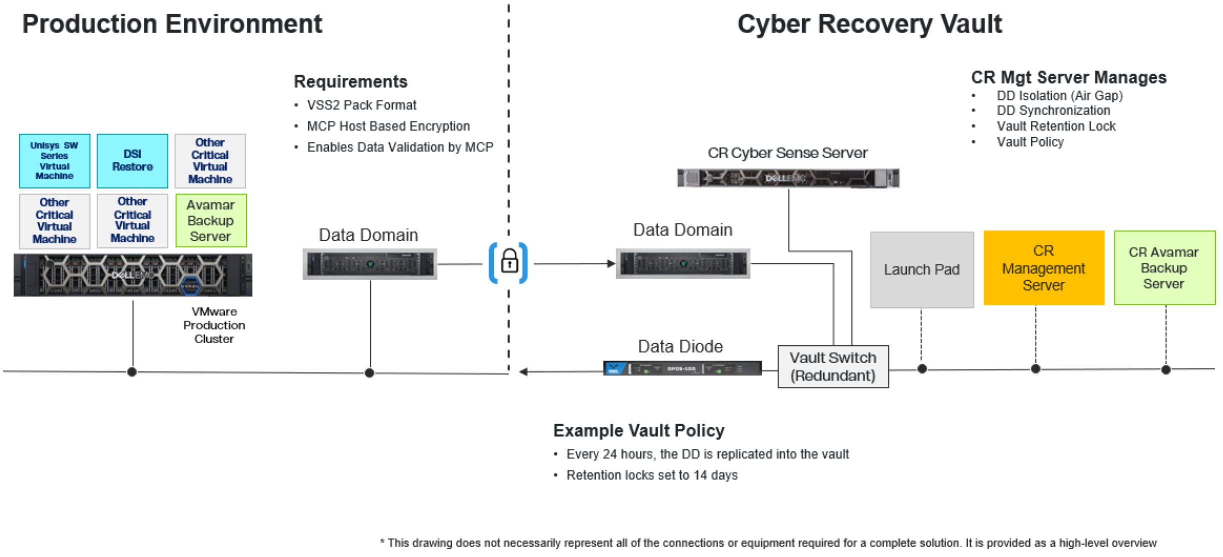
* This drawing does not necessarily represent all of the connections or equipment required for a complete solution. It is provided as a high-level overview

VMware licenses not included

Figure 3. Cyber Recovery with DSI VTL

In this solution, the MCP data is backed up into a DSI VTL after it has been checked for ransomware. To replicate the data from the DSI VTL into a vault, a staging server running a DSI Restore instance on VMware is used. Additionally, another VM running Data Domain Virtual Edition (DDVE) presents a NAS data store to DSI Restore. When the DSI VTL replicates to the DSI Restore, it writes directly into the data store presented from the DDVE. This data from the DDVE is then replicated to the Data Domain inside the vault.

Unisys ClearPath MCP Software Series Cyber Recovery with DSI Restore


Requirements

- VSS2 Pack Format
- MCP Host Based Encryption
- Enables Data Validation by MCP

CR Mgt Server Manages

- DD Isolation (Air Gap)
- DD Synchronization
- Vault Retention Lock
- Vault Policy

Example Vault Policy

- Every 24 hours, the DD is replicated into the vault
- Retention locks set to 14 days

* This drawing does not necessarily represent all of the connections or equipment required for a complete solution. It is provided as a high-level overview

Figure 4: Cyber Recovery with DSI Restore

In this hybrid model, a virtual instance of DSI Restore is used to backup MCP Software series data. Dell Avamar then performs a VM-level backup of CSS MCP and DSI Restore. This data is then replicated across the air gap to the Data Domain inside the vault. A Cyber Sense server confirms the integrity of the Open Systems data inside the vault. MCP data is confirmed as it is backed up into the DSI restore.

Unisys ClearPath MCP Cyber Recovery with BL/BackBox™

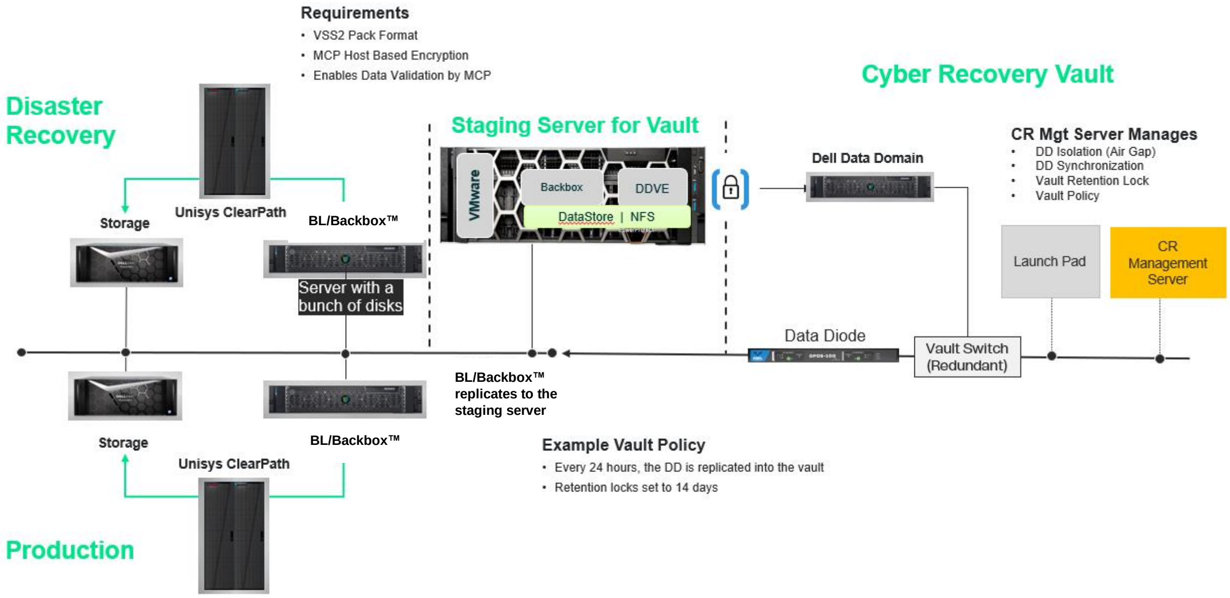


Figure 5. Cyber Recovery with BL/BackBox™

The above architecture is like the “Cyber Recovery with DSI VTL” (*Figure 3*), but instead of DSI VTLs, we use B&L Associates BL/BackBox™ to backup ClearPath MCP data. The staging server runs a virtual edition of BL/BackBox on VMware, which writes data to a DDVE-exposed NFS disk.

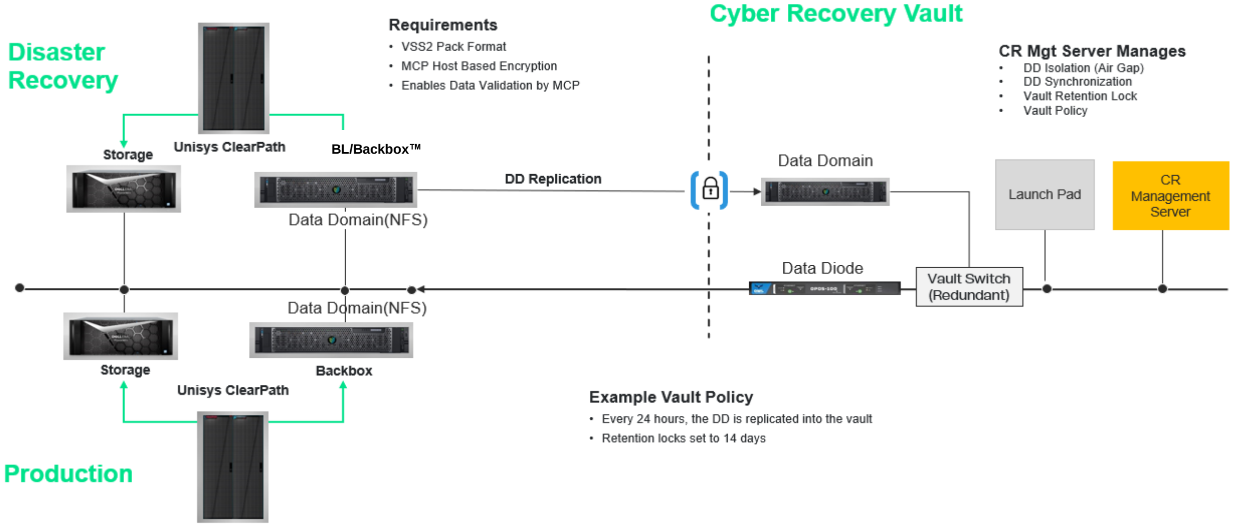
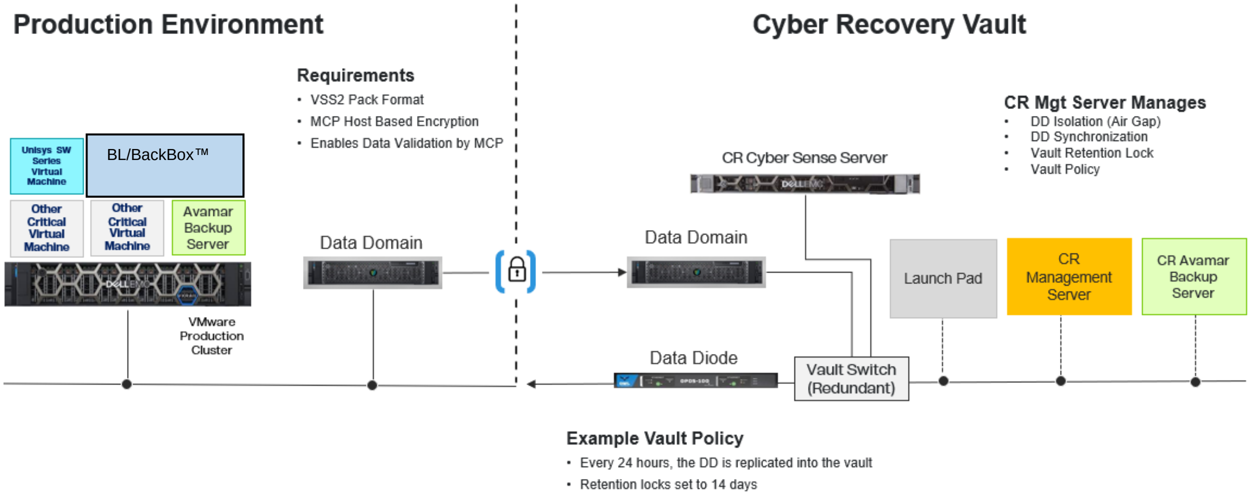


Figure 6. Cyber Recovery with B&L Backbox

In the above Cyber Recovery model, the BL/BackBox™ server writes ClearPath MCP data directly to an NFS mount from a Data Domain. MCP data integrity is confirmed during the backup process. Once backed up, the MCP data is then replicated to the Data Domain inside the vault via an air gap.

Unisys ClearPath MCP Software Series cyber recovery with BL/Backbox™



Requirements

- VSS2 Pack Format
- MCP Host Based Encryption
- Enables Data Validation by MCP

CR Mgt Server Manages

- DD Isolation (Air Gap)
- DD Synchronization
- Vault Retention Lock
- Vault Policy

Example Vault Policy

- Every 24 hours, the DD is replicated into the vault
- Retention locks set to 14 days

Figure 7. Software Series Cyber Recovery with BL/BackBox™

In this hybrid model, a virtual BL/Backbox™ instance running on VMware backs up ClearPath MCP software series data to the Data Domain. This Data Domain target is shared with an Avamar server to back up open systems data. This data is then replicated into the Data Domain inside the vault, where a Cyber Sense server checks the integrity of the open systems data.

Unisys ClearPath Libra integrated systems

Backup Technology	Supported for Cyber Recovery?
Physical Tape*	✓
Dell Data Domain Virtual Tape Library	✓
DSI Virtual Tape Library	✓
BL/BackBox™	✓

Unisys ClearPath MCP Software on bare metal servers

Backup Technology	Supported for Cyber Recovery?
Physical Tape*	✓
Dell Data Domain Virtual Tape Library	✓
DSI Virtual Tape Library with De-Duplication	✓
BL/BackBox™	✓

Unisys ClearPath MCP Software in VMware ESXi

Backup Technology	Supported for Cyber Recovery?
DSI Virtual Tape Library	✓
BL/BackBox ™	✓
VMware Backup to Dell Data Domain Disk Storage	✓
DSI Restore	✓

*Physical tape backup is not an automated solution.

Unisys Cyber Recovery for ClearPath Forward features

Vault policy

A vault policy is created to define critical data and systems that need to be protected, establish the frequency of both full and incremental backups, and provide details for retention. For example, the vault policy could specify:

- Replicate ClearPath production data into the Cyber Recovery vault every 24 hours.
- Retention lock tapes so they cannot be changed or removed for 14 days.
- Hold tapes for a specified number of days and then delete them. Set the default to 14 days.

ClearPath MCP data validation

MCP disk encryption is a prerequisite for MCP data validation, which requires the VSS2 or VSS3 disk format. The initial backup for the MCP host should be a full backup. Once the baseline is established, incremental backups with periodic full backups can be performed.

MCP data validation occurs during the creation of the full backup as data is read. This is done by reading the MCP data using the encryption key, decrypting it, and verifying its validity to ensure that the data has not been changed or corrupted externally. If the backup is created successfully, it becomes the gold copy candidate.

ClearPath MCP utilizes encryption processes enabled at the individual pack level, even when the system is running. Encryption will cause little or no performance impact on production as it occurs in the IOP, resulting in negligible processor consumption.

ClearPath MCP critical data to store in the vault

The most important aspect of any cyber resiliency solution is that the data needed for a successful recovery is stored in the vault. Without this, a successful recovery will not be possible. Unisys will collaborate with you to ensure your backup routines capture the correct data, allowing it to be copied into the vault. Below is an example of the data that needs to be stored in the vault:

- Known serial number tape.
  - MCP system configuration information
  - Tape backup catalog for data restoration
  - Copy of halt/load pack data, such as

    - user data file (e.g., user IDs and passwords)
    - Network initialization file
    - All Unisys software
- Application source code
- Application data
- WFL job files
- Third-party software
- All required firmware
- Any other file not part of the backup process needed for recovery

ClearPath MCP Recovery Run Book

“The Run Book” is a procedure guide used to recover the MCP environment in an attack. “The Run Book” documents the procedure to restore the MCP hardware and firmware environment. Once this step is complete, the guide will explain how to restore the data from the vault, restart your applications and return to normal business operations.

Where to begin

1. Start with a consulting workshop to identify the data that should be stored in the vault
2. . Next, review your backup process(es), adjusting them to ensure the required data is backed up.
3. Enable data validation to confirm your backup data is free from malware.
4. Invest in a vault to securely store a gold copy of your backup data, ensuring successful recovery when needed.
5. Train your team to ensure they know how to execute the recovery procedure.

To explore how Unisys Cyber Recovery for ClearPath can help you protect backups and quickly recover from ransomware attacks, visit us online or contact us today.

unisys

unisys.com