Unisys Cyber Recovery for ClearPath Forward®

Protect and isolate critical data from ransomware and other sophisticated threats within ClearPath Forward OS 2200 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. In fact, the estimated global impact of cybercrime is expected to grow by 15% per year over the next five years, reaching $10.5 trillion annually by 2025.[1]

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 due to the increase in 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 cyber resiliency and risk management strategies.

[1] **Unmasking the True Cost of Cyberattacks: Beyond Ransom and Recovery**

Table of contents

Protect data and recover quickly

Given the frequency of ransomware attacks, a well-designed data isolation architecture should maintain multiple recovery points (point-in-time copies) to ensure recoverability, and it should run integrity checks on incoming data. If an issue is detected, it should use alerting mechanisms to identify data corruption promptly.

Unisys Cyber Recovery for OS 2200 protects and isolates critical data from ransomware, social engineering, and other sophisticated threats to ClearPath Forward® OS 2200 Operating Environments. This modern approach allows you to keep a copy of critical data off the network and create multiple recovery points to ensure 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 expertise in traditional data center services, including backup recovery and disaster recovery. Its specialized architecture enables an environment compromised by a cyberattack to be restored quickly and safely.

Our solution safeguards a copy of your critical data, enabling rapid recovery. Unisys IT experts add additional value by applying best practices — such as determining what data is critical, designing secure recovery and restoration architectures, and creating runbooks — providing you with a validated plan that restores applications and services quickly. Drawing upon Unisys' hands-on experience installing, configuring, and running ClearPath environments means you gain the necessary continuity while avoiding learning curve mistakes. You'll also 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 identifies threats and determines the presence of malware
- **Security**: data protected in an air-gapped point-to-point connected vault
- **Documentation**: trained and prepared IT staff with tested procedures for quick server and system reimaging in the event of ransomware detection

The specifics of how the cyber recovery solution operates depend on your existing data backup solution and ClearPath deployment architecture. Additional defaults are detailed in later sections; however, Figure 1 provides an overview of the solution's main elements and the sequential flow of data through the solution.

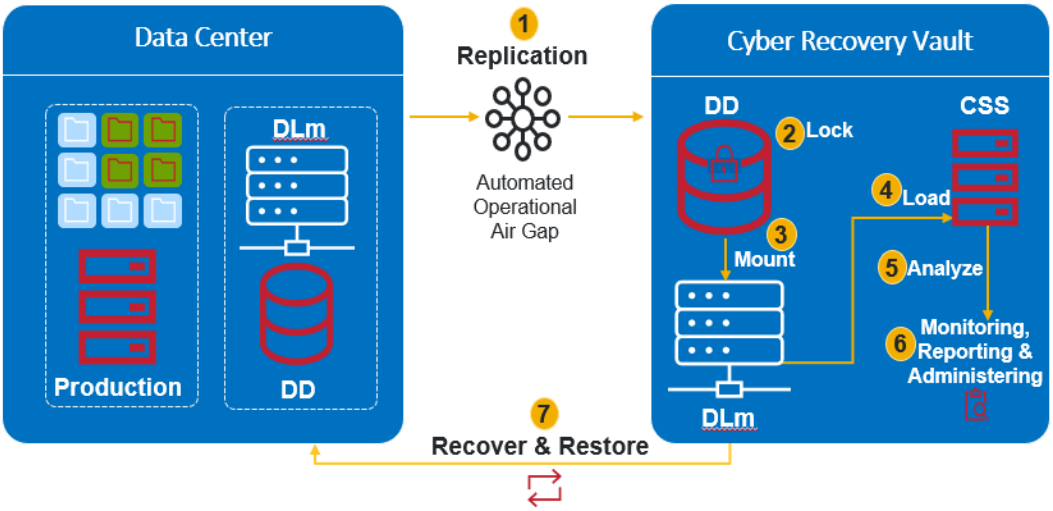


Figure 1. Solution Overview

1. The Dell DLM stores the production tape data to the Data Domain. This data is then replicated to another Data Domain inside the vault using an air-gapped point-to-point connection that isolates the Cyber Recovery vault from outside attack.

2. After replication to the vault is completed, the snapshots are taken and locked into a read-only state to make an immutable copy.

3. To initiate data validation, the snapshot is mounted to the vault's DLM.

4. Within the vault, an instance of the OS 2200 operating system loads the data from the DLM.

5. The OS 2200 Software Series is booted from the tapes and runs a series of verification utilities to validate the data structures' integrity. If all checks are passed, the snapshot is designated as a gold copy, making it eligible for recovery.

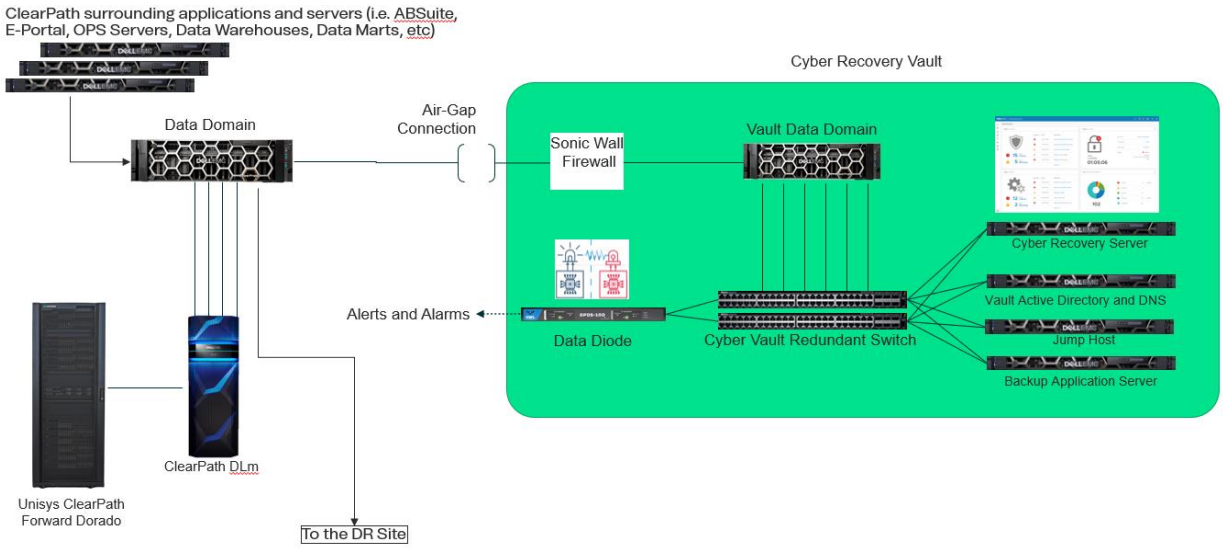
6. During this process, a secure outbound-only connection can report success or failure via email, and ongoing administration can be performed from a physical terminal on an isolated network within the vault.

7. Unisys provides a runbook detailing step-by-step procedures to restore operations. In the event of a cyberattack, a malware-free gold copy of data is identified, and recovery operations are initiated.

ClearPath OS 2200 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 and proposes the following scenarios for protecting your ClearPath data.

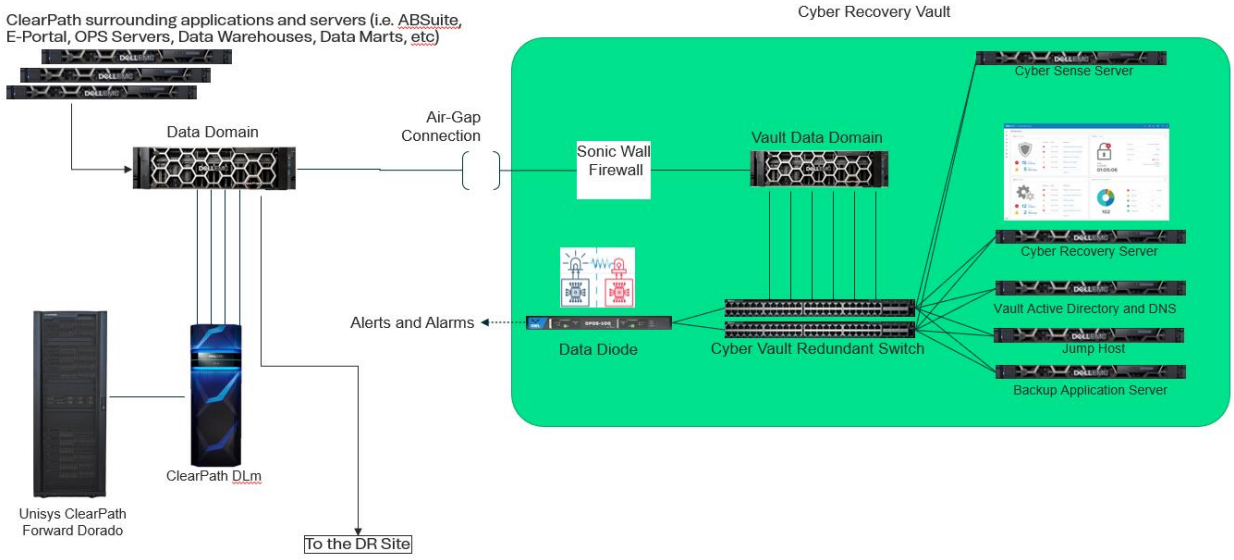
Unisys Cyber Recovery for ClearPath OS 2200 with data domain and DLM – no data validation



The above architecture illustrates how open systems data from the production environment and ClearPath data from the DLM are backed up to the production Data Domain. This backed-up data is then replicated via an airgap into the vault Data Domain. The connection between the two Data Domains is further secured with a point-to-point communication link and a SonicWall Firewall. Although snapshot capabilities are

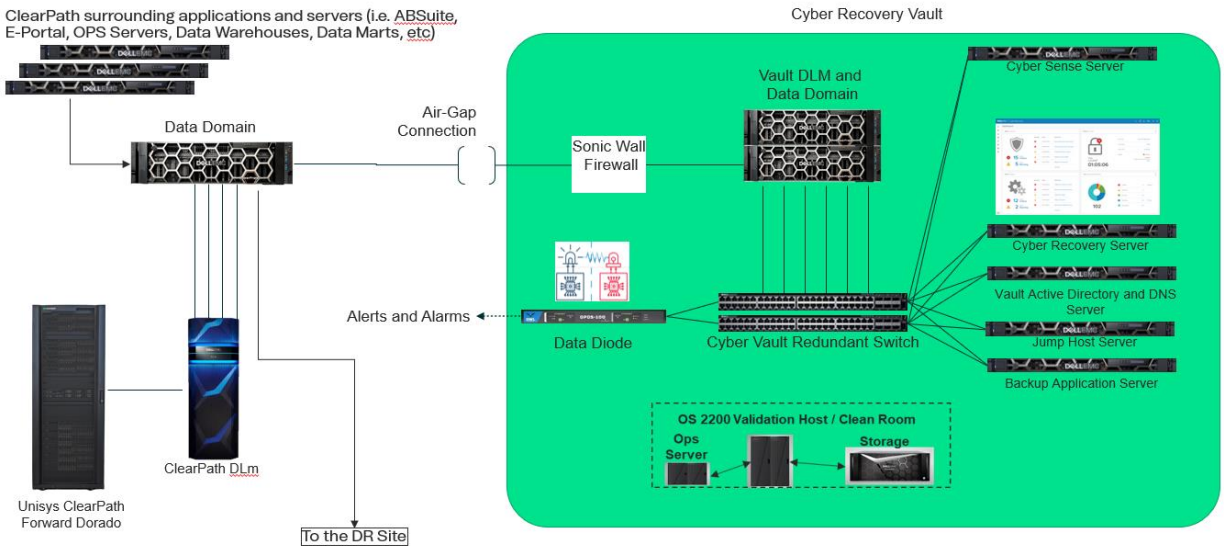
present, no validation happens post-replication. The recovery process, in this case, is a manual one where the client would have to determine which snapshot is not compromised and perform a restore from that snapshot accordingly. This involves manual checking of each snapshot for integrity.

Unisys Cyber Recovery for ClearPath OS 2200 with Data Domain and DLM – open systems data validation



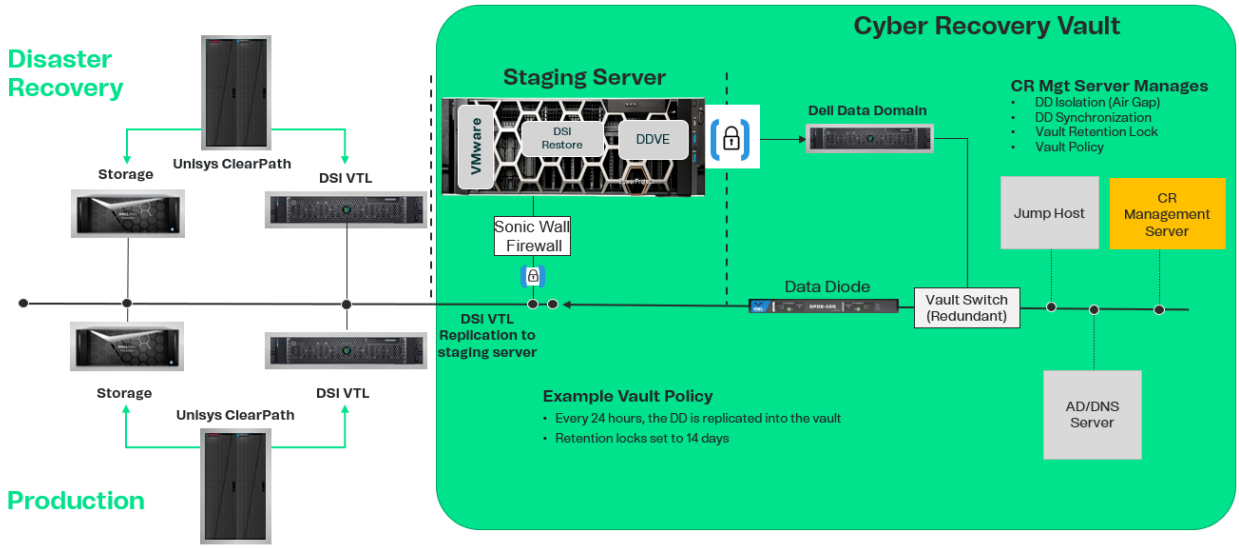
In the above architecture, a Cyber Sense server is present inside the vault to validate open systems data. The Cyber Sense server detects any malware or ransomware that may have been replicated into the vault. While ClearPath data is also backed up into the vault Data Domain, it doesn't undergo an automatic validation. For ClearPath data recovery, clients must manually determine which snapshot is uncompromised, check each snapshot for integrity, and perform a restore from the selected snapshot.

Unisys Cyber Recovery for ClearPath OS 2200 with Data Domain and DLM – open systems and ClearPath data validation



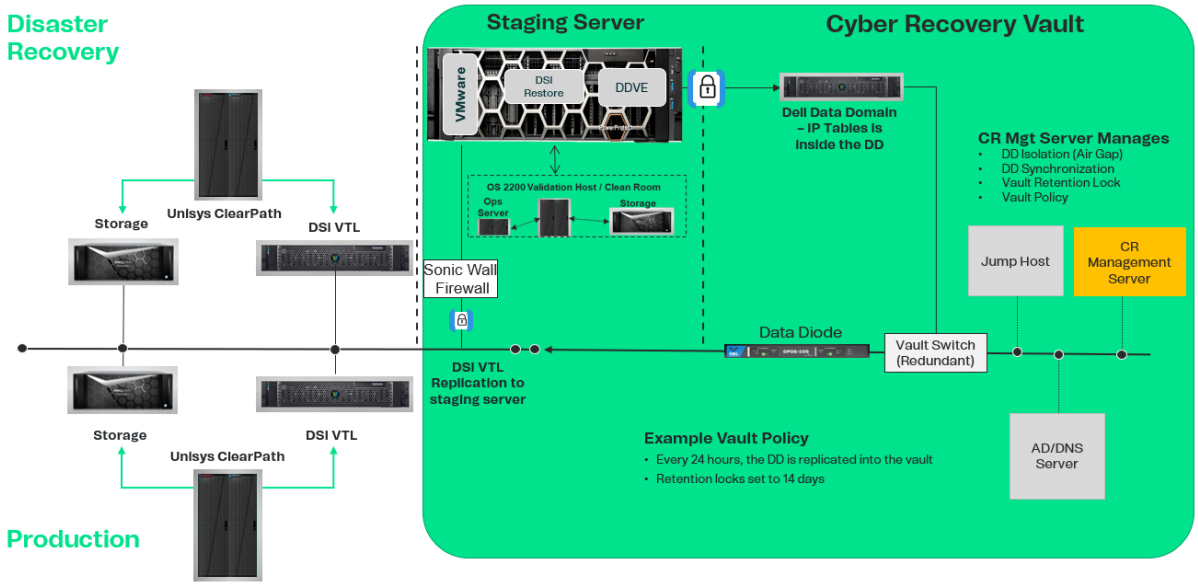
The above architecture introduces the concept of ClearPath data validation. A Cyber Sense server present inside the vault validates the open systems data. Additionally, a ClearPath OS 2200 validation host inside the vault checks the OS 2200 data integrity. The target Data Domain in the Cyber Recovery vault is connected to a Dell DLM, which mounts the snapshots as tape data. These tapes are then loaded onto the vault's ClearPath OS 2200 host, which reads the tapes' data and boots the system. Once the system boots, remaining data is loaded and validation routines check for ransomware and malware. This process repeats automatically for every snapshot.

Unisys Cyber Recovery for ClearPath OS 2200 with DSI VTL



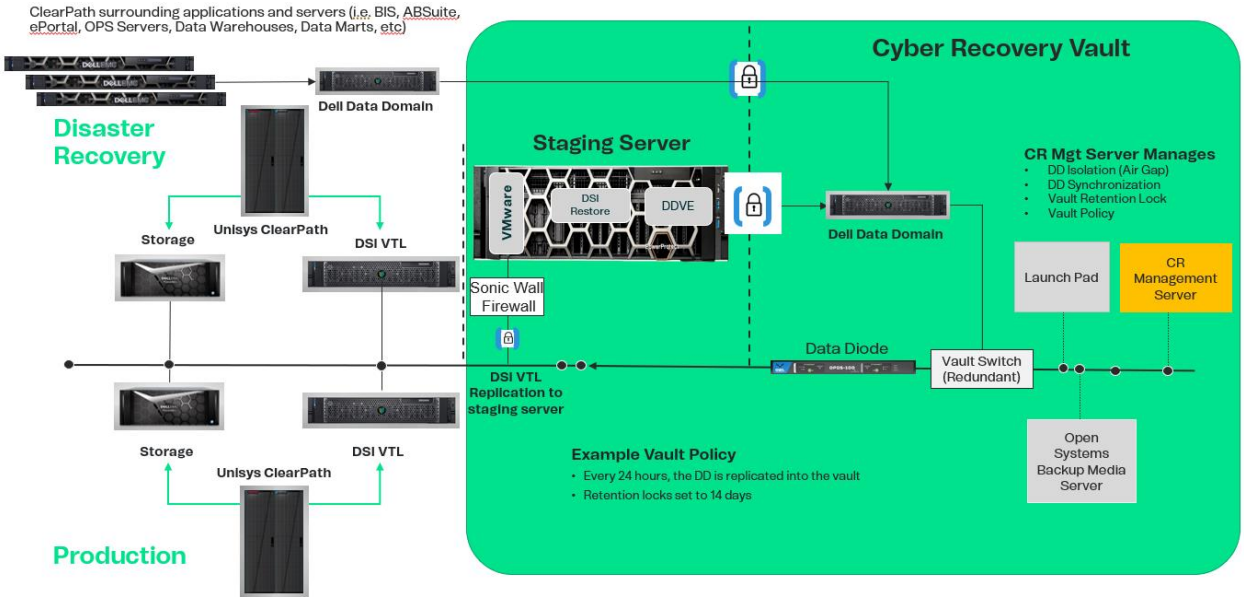
The above architecture uses a physical DSI VTL appliance as the backup target for ClearPath OS 2200 data in a production environment. A staging environment with DSI Restore on VMware replicates data from the DSI VTL to a Data Domain in the vault. A VM running Data Domain Virtual Edition (DDVE) presents a data store to DSI Restore. When the DSI VTL replicates to the DSI Restore, data is written directly to the DDVE-presented data store. This data is then replicated to the Data Domain inside the vault. (The vault operation is as described in the other scenarios.)

Unisys Cyber Recovery for ClearPath OS 2200 with DSI VTL and data validation



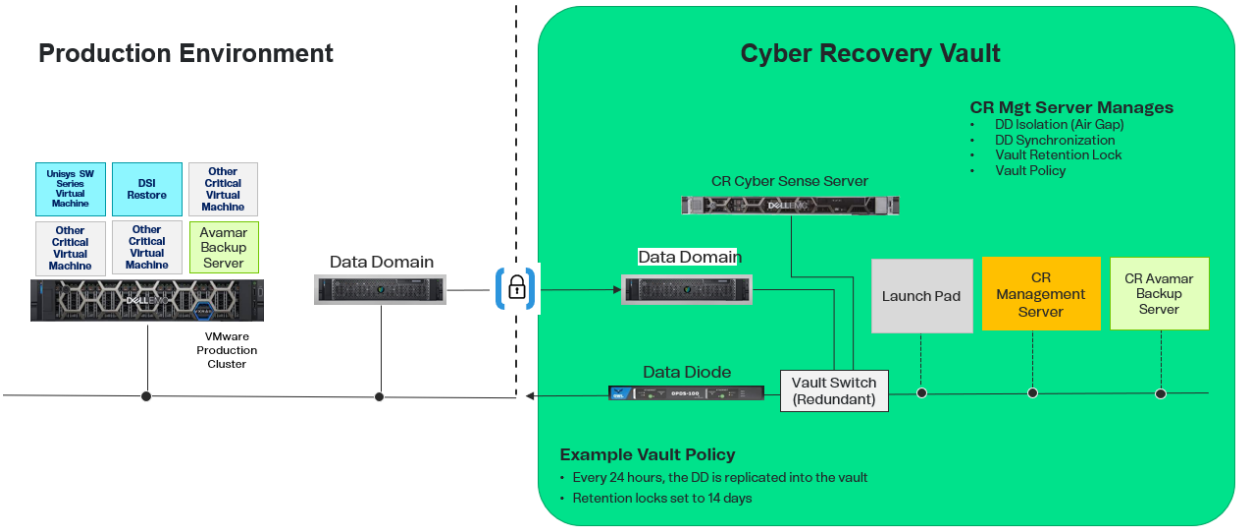
The above architecture is like the previous one with the addition of data validation. Once the data has been replicated into the staging environment, a ClearPath OS 2200 host mounts the replicated data and validates it. Using an airgap, this data is also replicated into the physical Data Domain.

Unisys Cyber Recovery for ClearPath OS 2200 with DSI VTL and surrounding systems



In the above hybrid model, open systems data is backed up to the production Data Domain, while ClearPath OS 2200 data is backed up to a DSI VTL appliance. Open systems data replicates directly to the vault's physical Data Domain, whereas the DSI VTL appliance replicates to a staging server running a DSI Restore instance on VMware. In addition, another VM running Data Domain Virtual Edition (DDVE) presents a data store to DSI Restore. When the DSI VTL replicates to the DSI Restore, it writes directly to the data store by the DDVE. This data is then replicated to a physical Data Domain inside the vault, where a snapshot is taken and made immutable for future recovery.

Unisys ClearPath OS 2200 Software Series on VMware Cyber Recovery with DSI Restore



In this hybrid model, a virtual instance of DSI Restore is used to back up OS 2200 Software series data. Dell Avamar then performs a VM-level backup of OS 2200 Software series and DSI Restore. This data is backed up to the production Data Domain and replicated across the airgap to the Data Domain inside the vault. A Cyber Sense server verifies the integrity of the open systems data within the vault.

Unisys Cyber Recovery for ClearPath features

ClearPath 2200 data validation process

Sample gold copy creation

The following presents the steps to perform ClearPath OS 2200 data validation:

- Production ClearPath data is replicated into the vault.
- An immutable snap is taken and immutable retention locks are set in the vault – this is the candidate gold copy.
- The candidate gold copy is restored to the recovery-ready storage array in the vault.
- The vault ClearPath system is rebooted.
- The boot process validates the MFD.
- DMS/ RDMS Data Bases are validated using the:
    - VERIFY command in the DMU Utility, which verifies page structure, chain sets, and index sequential records. DMU makes a sequential pass through the areas involved, extracting the information required to perform all verifications.
    - The Relational File Analyzer (RFA) program has a comprehensive validation algorithm and provides statistical and diagnostic information. It analyzes Exec and UDS/TIP files assigned to UDS Control.
- TIP FCSS Files and PCIOS Indexed Sequential Files are validated by inspecting known sample files.
- TIP files registration is confirmed (SSG script provided by client).
- Additional validation provided by the client may be included.
- Operations Sentinel logs all activities.
- Upon successful data validation, the candidate copy becomes the gold copy.

Vault policy

A vault policy can be created to identify critical data and systems to be protected, identify the frequency of both full and incremental backups, and provide details for retention. For example, the vault policy could be stated as follows:

- ClearPath production data is replicated into the Cyber Recovery vault every 24 hours (or as configured in the vault management system).
- Tape snapshots have retention locks applied to create immutable copies.
- Tape snapshots are held for a configurable number of days and then deleted, with a 14-day default window.

ClearPath OS 2200 critical data to store in the vault

The most important aspect of any cyber recovery solution is ensuring that the necessary data is stored in the vault. Without this, a successful recovery is impossible. Unisys will work with you to ensure your backup routines capture the correct data, which can then be copied into the vault. Below is an example of the data that needs to be stored in the vault:

- FAS backup of all non-database files
- Database backup of database files
- Boot tape with 2200 Exec level of existing system
- SOLOR tapes containing all applications that were installed
- Third-party installation tapes
- Save SEC$@USERID$ file
- Save system critical files (depends on site environment)
- Save transaction environment files, such as the VALTAB file

ClearPath OS 2200 Recovery Run Book

“The Run Book” is a procedure guide used to recover the OS 2200 environment in the event of an attack. Unisys services are also available to execute the recovery procedure. “The Run Book” outlines the steps to restore the OS 2200 hardware and firmware to factory settings. Once this step is complete, the guide explains how to restore data from the vault, restart your applications and return to normal business operations.

Enhanced secure recovery option

Additional Unisys ClearPath OS 2200 in the vault

Optionally, Unisys will provide secured, recovery-ready ClearPath infrastructure that can be deployed in an attack for quicker recovery. An additional ClearPath OS 2200 Software Series can be placed inside the vault for loading a clean image. The alternative is to wipe the existing environment before restoration. Regardless of the method chosen, ensuring that you can quickly recover your most critical data and systems after a cyberattack or other disruptive event is critical for resuming normal business operations.

Additional recovery services from Unisys

If desired, Unisys can provide additional services to assist your team in recovery from a cyber event including:

- Hardware recovery process
    - Validate the ClearPath Dorado System operations server is functional. If not, Unisys will rebuild it.
    - Validate that the ClearPath Dorado System firmware is functional. If not, Unisys will rebuild it.

    - Validate that the production DLM and Data Domain are functional. If not, Unisys or Dell will rebuild them.
- Software recovery process
    - Boot the system using the saved boot tape with JK 4,13 set to reinitialize mass storage.
    - Load SEC$@USERID$ file during recovery.
    - Optionally, “PREP” non-fixed disks as an extra precaution.
    - Load library tapes.
    - Restore system-critical files.
    - Use SOLOR to install applications.
    - Install third-party software.
    - Use FAS to reload all non-database files.
    - Use FREIPS to reestablish the transaction environment.
    - Reload database files.
    - Start applications.

Automated replication protection

Unisys Cyber Recovery provides your organization with prompt malware detection and notification when data is replicated into the Cyber Recovery vault. This automated monitoring ensures quick recovery from a cyberattack using the gold copy of data secured in the vault.

The ClearPath software series inside the Cyber Recovery vault validates your data each time a snapshot is created without impacting your production environment's performance. With the support of recovery-ready procedure guides and professional services, Unisys can help you recover from cyberattacks with the least recovery time objective (RTO) possible.

Where to begin

1. Start with a consulting workshop to define what should be stored in the vault. Then, review your backup process(es), adjusting them to ensure this required data is backed up and replicated to your disaster recovery location.

2. Invest in a vault to store an isolated gold copy of your backup data. This ensures you can successfully recover in the event of a cyber incident that compromises the production and disaster recovery locations.

3. Invest in data validation as a second step. This will reduce your RTO should a cyber event occur.

4. Train your team to ensure they understand how to execute the recovery procedure effectively.

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

unisys.com