Reference Architecture: Dell EMC PowerProtect Cyber Recovery for Converged Infrastructure

September 2021

H18876

White Paper

Abstract

This white paper describes Dell Technologies PowerProtect Cyber Recovery solutions and services, which enable you to recover your most critical data and systems quickly after a cyber or other disruptive event, as part of a modern and powerful cyber resilience strategy.

Dell Technologies Solutions

Copyright

Contents

About this document

In this document, we describe Dell EMC PowerProtect Cyber Recovery, what it provides, and why it is necessary as part of a digital transformation strategy. From a converged infrastructure perspective, we specify which components work together as a solution to provide the benefits of Cyber Recovery. We also detail the baseline testing that customers can use as a starting point to design a Cyber Recovery solution for their specific use cases and applications. We also provide Dell EMC- and VxBlock-specific best practices for Cyber Recovery solutions that center around backup management, networking, and the recovery environment.

Audience

The audience for this document consists of current and prospective converged infrastructure customers looking to protect their production application environments from cyberattacks, and as recovery if a destructive attack occurs.

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 by email or provide your comments by completing our documentation survey.

Authors: Jason Kahn, Joe Boyd

Note: For links to additional documentation for this solution, see the Dell Technologies Info Hub for VxBlock 1000.

Executive summary

Cyber threats are becoming more sophisticated. It is not a matter of “if” but “when” you will face such an attack.

Cyber threats do not cause mere thousands of dollars of loss—the damage is in the trillions of dollars. Accenture forecasts more than five trillion dollars of global value at risk over the next five years.

Attacks are virtually nonstop, and the cost per attack continues to increase. While there is a common misconception that only certain sized businesses or industries are attacked, the reality is that no enterprise is immune. Bad actors target businesses of all sizes and across all industries.

Regardless of the industry, be it healthcare, financial services, or local, state, or national governments, every business is a data-driven enterprise today. This scenario presents ample opportunity for criminals using modern tools and tactics to leverage this data for various purposes or to destroy and ransom it for some agenda or benefit. According to Accenture, 68 percent of business leaders state that their cyber security risks are increasing.

The modern threat of cyberattacks and the importance of maintaining the confidentiality, availability, and integrity of data requires modern solutions and strategies to protect vital data and systems.

Because having a cyber resilience strategy is becoming a mandate for all business and government leaders, this strategy can be seen as a competitive advantage in today’s data-driven world.

We found that a combination of Dell EMC products integrated into a solution such as a Cyber Recovery appliance can combat an attack to the on-premises environment and recover critical business applications best. This solution includes a combination of backup management, target storage, networking, a recovery environment, and recommendation for a firewall or a data diode.

Introduction

Over the past three years of helping our customers protect their critical data and recover their businesses following a successful cyberattack or ransomware incident, we have found that there are three main common characteristics of a Cyber Recovery solution:

- **Isolation**—Physical (using a locked room on-premises or in an off-premises or cloud-based vault) and logical (data and management path or command and control access) separation of the Cyber Recovery vault from the attack surface of production and backup infrastructure
- **Immutability**—As defined by Dell Technologies, hardware and software, and additional controls that ensure that the original integrity, confidentiality, and availability of the vault data is preserved

- **Intelligence**—Application of innovative and comprehensive tools and analytics, machine learning, and AI within the security of the Cyber Recovery vault to identify potential cyber threats or corruption and to ensure that vaulted data is recoverable

It is significant that these three components work independently and collectively in an integrated solution to provide the maximum levels of security and protection for vaulted data. They provide the best possible chance to recover vaulted data with integrity and confidence if an attack penetrates the data center.

Solutions that offer one or two of these common characteristics as features of backup or disaster recovery (DR) products and services, while useful, cannot be expected to provide the same levels of protection of critical data when a sophisticated attack impacts production, backup, and perhaps DR.

Features such as storing backups in some immutable form provide an incremental amount of protection over nonimmutable backups. This feature alone does not withstand insider credentialed attacks or network time protocol (NTP) attacks. These NTP attacks trick many software-defined storage systems into releasing the retention period if cyber criminals tamper with the NTP setting to indicate falsely that the retention period has expired.

While intrinsic security provides a foundation for our overall security and cyberrelated standards across Dell Technologies, our Cyber Recovery solutions and services provide the highest levels of protection, integrity, and confidentiality for your most valuable data and critical business systems. Due to the most sophisticated cyber threats, we are not focusing on preventing ransomware or cyberattacks but on protecting critical data or applications and enabling you to recover those assets with integrity so that you can resume normal business operations with confidence.

Our Cyber Recovery solution protects the most critical data in a vault environment. Ideally, the Cyber Recovery vault is physically isolated – a locked cage or room – and is always logically isolated using an operational air gap. The Cyber Recovery vault components are never accessible from the production system. When the air gap is unlocked, access to the Cyber Recovery vault target system is extremely limited. This feature is a key to the maturity of our solution. The Cyber Recovery vault is not an extra data center but is usually located at the production or corporate data center.

The Cyber Recovery vault operates by using four basic steps:

- Data representing critical applications is synchronized through the air gap, which is unlocked by the management server, into the Cyber Recovery vault and replicated into the Cyber Recovery vault target storage. The air gap is then relocked.
- A copy of that data is created. Vault retention is configurable. Most customers keep about a month's worth of copies.
- The data is retention locked to further protect it from accidental or intentional deletion.
- Optionally, the CyberSense analytics engine analyzes the data.

Recovering data from the Cyber Recovery vault after a cyberattack or for recovery testing procedures is critical. There are several ways to perform a recovery. The following figure highlights the basic recovery steps:

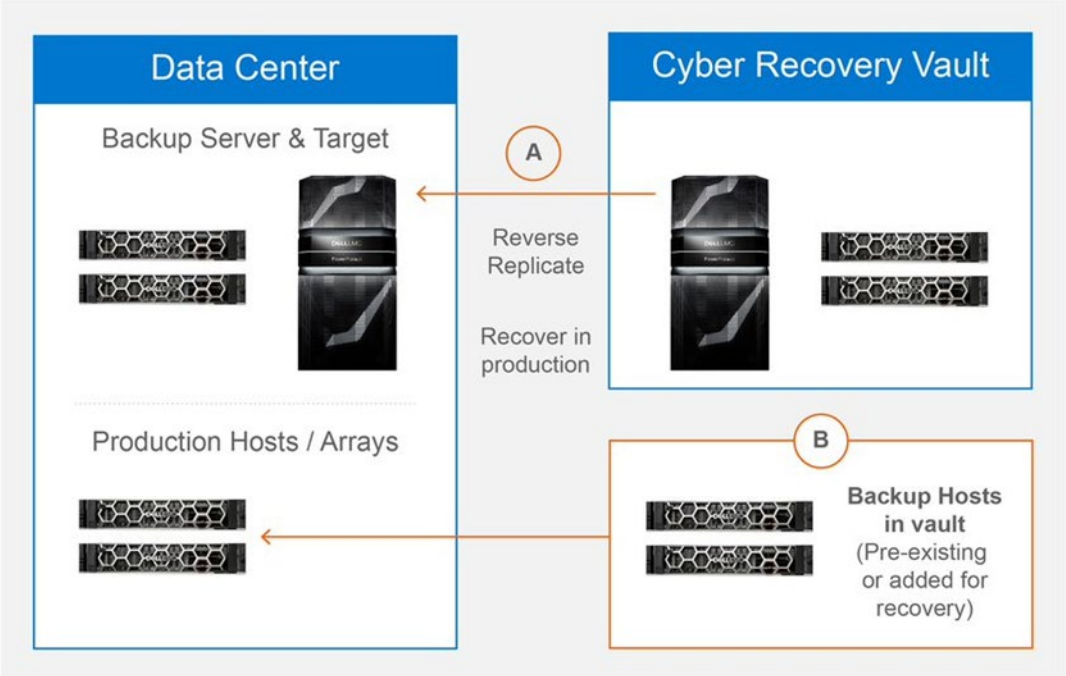

Figure 1. Basic recovery steps

The recovery steps include:

- Evaluate analytics results
- Select restore points
- Restore data with the original backup application, using the Cyber Recovery vault data and catalog
- Cleanse and update impacted applications as necessary

Solution overview

The Dell EMC VxBlock 1000 is a fully engineered and integrated converged infrastructure system combining storage, compute, and virtualization. The VxBlock 1000 also allows for fully engineered and integrated data protection solutions that consist of Dell EMC best of breed data protection technologies.

The Dell EMC data backup solutions that are integrated and supported with VxBlock 1000 are:

- Dell EMC Avamar software
- Dell EMC NetWorker software
- Dell EMC PowerProtect Data Manager software
- Dell EMC PowerProtect DD systems

For most enterprise and midsize businesses, having a data backup solution is essential, but it might not be enough to protect against all types of data loss including compromised data due to ransomware and other sophisticated cyberattacks. This scenario is ideal for a Cyber Recovery solution to protect an organization's assets or applications. The Cyber Recovery solution protects and isolates business critical data from these cyber threats to enable recovery of known good data and the ability to resume normal business operations with confidence.

Cyber Recovery provides:

- An operational air gap with data isolation and immutability
- CyberSense analytics and machine learning to monitor data integrity
- The ability to accelerate cyber and ransomware attack data recovery

For more information about Cyber Recovery and how it can help protect your organization's valuable data, see the Dell EMC PowerProtect Cyber Recovery Solution Brief.

The Cyber Recovery solution for Dell EMC Avamar Virtual Edition (AVE), Dell EMC NetWorker, Dell EMC PowerProtect Data Manager, and Dell EMC PowerProtect DD has not been engineered as an integrated, supported, and orderable VxBlock 1000-integrated data protection solution. However, VxBlock-integrated data protection engineering has configured, tested, and documented a Backup and Recovery Design Center (BRDC) - approved Cyber Recovery solution design in a lab environment.

Use cases

Customers are unique in terms of the data-sets that they want to protect in their air-gapped vault environment. However, they all need to protect business critical data and applications. What is each application or set of data worth? What is the cost of down-time or data-loss? How much is the organization willing to pay in ransom for their data?

The Cyber Recovery use case is centered around the types of bad actors and the broad spectrum of potential attacks, as well as their motivations, techniques, and goals:

- **Crime**—Theft and extortion for financial gain
- **Insider**—Theft and extortion by trusted insiders for personal, financial, and ideological reasons; increasingly targeted because of privileged access to systems
- **Espionage**—Theft of valuable data by corporate or nation-state actors
- **Hacktivism**—Advance of political or social causes
- **Terrorism**—Sabotage and destruction to instill fear
- **Warfare**—Nation-state actors with destructive cyber weapons

Test configuration

The following figure shows the lab configuration used for Cyber Recovery testing with VxBlock 1000 Integrated Data Protection with one exception. The lab environment did not include a firewall between the customer network and the Cyber Recovery network for the management data path. The Cyber Recovery vault was managed entirely from within the vault. For remote management of the Cyber Recovery vault, a firewall, as shown, is required to ensure a secure environment.

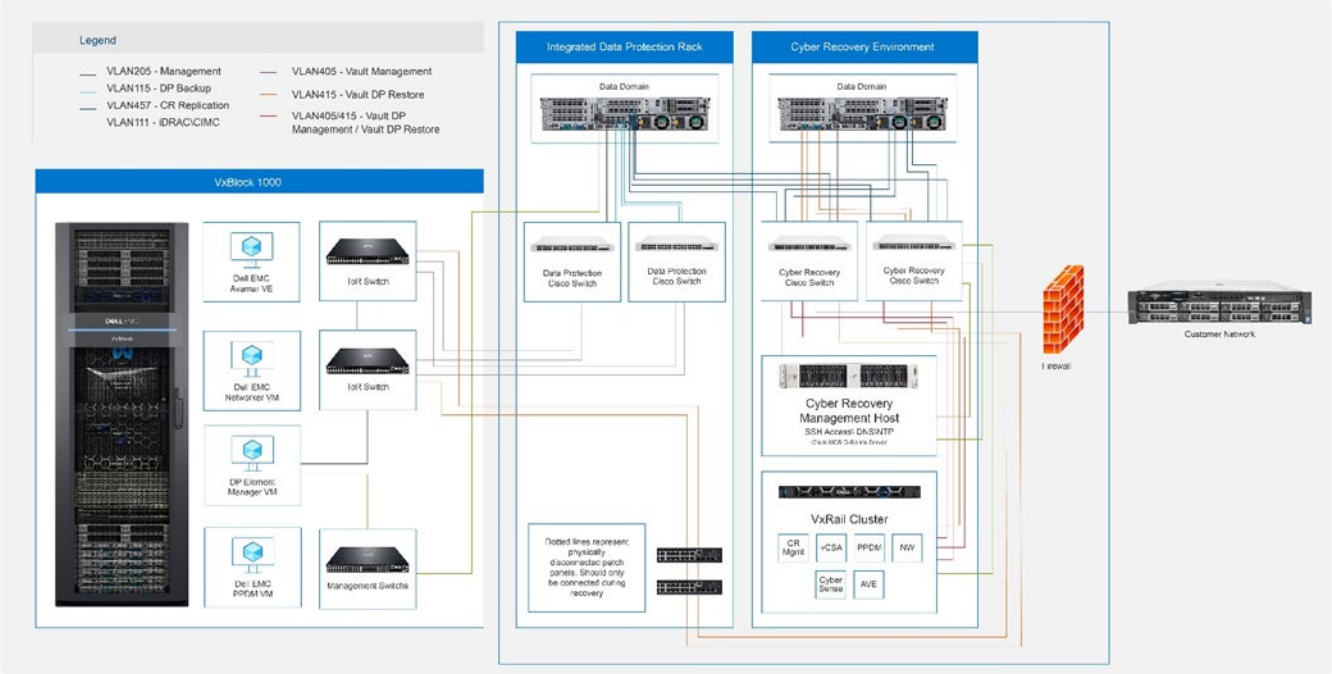

Figure 2. Lab configuration for Cyber Recovery testing

Note: This lab configuration is an example of a Cyber Recovery vault environment; do not implement this environment without engaging a DPS Sales Engineer (SE) and the BRDC to ensure a properly sized and secure Cyber Recovery vault environment. Engage a DPS SE early enough to determine the front-end data sizing for any Cyber Recovery solution. Possible design changes might have to be considered for the DPS backup application and CyberSense sizing requirements.

The VxBlock integrated data protection system is configured and integrated like a typical data protection backup integration. However, there is one key difference with the integration of Cyber Recovery; the production PowerProtect DD6900 system has an additional pair of 25 GbE IO modules that are configured for LACP and are used strictly for replication to the Cyber Recovery vault environment. These connections are made directly to the Cyber Recovery environment Cisco Nexus 93180YC-FX switches. By not connecting directly to the integrated data protection Cisco Nexus 93180YC-FX switches, you can avoid creating uplinks from the Integrated Data Protection switches to the Cyber Recovery Nexus switches to eliminate another possible attack vector.

As with the production DD6900 connections for production backup and restore operations, the connections for replication to the Cyber Recovery vault are configured as LACP hash XOR-L2L3 and are tagged with the Cyber Recovery replication VLAN ID. The interfaces on the Cyber Recovery Cisco Nexus 93180YC-FX switches are configured as a Virtual Port Channel (VPC) to provide both bandwidth aggregation and redundancy. The port

channel is also configured to only allow the Cyber Recovery replication VLAN ID, which helps reduce the attack vector of the Cyber Recovery vault environment.

The Cyber Recovery vault DD9900 system includes two pairs of 25 GbE IO modules. Both pairs of 25 GbE IO modules connect directly to the Cyber Recovery Cisco Nexus 93180YC-FX switches and are configured as LACP hash XOR-L2L3. One virtual interface is used for Cyber Recovery restore, and is tagged with the Cyber Recover restore VLAN ID. The other virtual interface is used for Cyber Recovery replication and is tagged with the Cyber Recovery replication VLAN ID. The Cyber Recovery Cisco Nexus 93180YC-FX switch interfaces to which the DD9900 systems are connected are configured as VPCs to provide both bandwidth aggregation and redundancy. These port channels are also configured to only allow the respective VLAN IDs for Cyber Recovery restore and replication; this configuration also helps reduce the attack vector of the Cyber Recovery vault environment. For DD9900 management, the ethMa and iDRAC interfaces are both connected to the Cyber Recovery Cisco Nexus 93180YC-FX switches. This connection allows in-band and out-of-band management.

A three-node VxRail cluster is also deployed in the Cyber Recovery vault environment. Each VxRail node has four physical connections alternating between the two Cyber Recovery Cisco Nexus 93180YC-FX switches to provide for the vSphere ESXi host uplinks. The VxRail cluster has a dedicated vCenter virtual appliance to manage the VxRail data center, cluster, and vSAN. The Cyber Recovery management virtual appliance is also deployed to the VxRail cluster. For Cyber Recovery restore purposes, AVE, a CentOS Linux-based NetWorker Server virtual machine, and a PowerProtect Data Manager virtual appliance are also deployed and configured on the VxRail cluster according to the *Dell EMC PowerProtect Cyber Recovery Product Guide*. For analytics and analysis, a CentOS Linux virtual machine installed with CyberSense is also deployed to the VxRail cluster.

The Cisco UCS C220-M5 rackmount server is a bare-metal system deployed with the CentOS 7.9 Linux operating system. The Linux operating system is configured to provide both DNS and NTP services for the entire Cyber Recovery vault environment. These services are key to the successful deployment and configuration of the VxRail cluster.

Test results

Cyber Recovery tests performed in the lab environment

Before performing tests, the following tasks were performed:

- Configuration of the Cyber Recovery Cisco Nexus 93180YC-FX switches including basic configuration, configuration of access ports, VPCs, and HSRPs for intravlan routing.
- Configuration of the production DD6900 system virtual LACP interface tagged with VLAN 457.
- Configuration of the vault DD9900 system, which includes basic DD configuration such as ethMa, iDRAC, File System, and Encryption. Configuration of the virtual LACP interfaces for both restore and replication, each tagged with the appropriate VLAN IDs, 415 and 457 respectively.
- Configuration of AVE, NetWorker, and PowerProtect Data Manager MTrees as described in the *Dell EMC PowerProtect Cyber Recovery Product Guide*

- Installation and configuration of CentOS 7.9 on the Cisco UCS C220 M5 rack mount server, including configuration of DNS and NTP services.
- Deployment and configuration of the VxRail cluster according to the VxRail Appliance Installation Procedures as generated from SolVe Online.
- Deployment and configuration of the PowerProtect Cyber Recovery virtual appliance on the VxRail Cluster.
- Configuration of the assets, storage, vCenter, and replication policies on the PowerProtect Cyber Recovery virtual appliance as described in the *Dell EMC PowerProtect Cyber Recovery Product Guide.*
- Configuration of AVE, NetWorker, and PowerProtect Data Manager on the VxRail cluster as described in the *Dell EMC PowerProtect Cyber Recovery Product Guide.*
- Deployment, configuration, and installation of CyberSense on a CentOS 7.9 Linux virtual machine.

Note: These tasks might not include all required tasks and details. When configuring the environment, review and consult the vendor-provided installation and administration documentation for all components of the Cyber Recovery environment described above. Professional service engagement along with BRDC guidance, especially for Cyber Recovery, is required for design and implementation.

NetWorker test

Test #1: Perform an automated recovery of the NetWorker server in the Cyber Recovery vault virtual infrastructure environment using the Cyber Recovery UI.

- The NetWorker server recovery is an automated process that is initiated through the Cyber Recovery UI
- The NetWorker server instance that is deployed and configured on the VxRail cluster is added manually to the Cyber Recovery environment as an application object
- Initiate the NetWorker Server recovery by clicking **Recovery** and selecting the NetWorker copy from which to recover the NetWorker server. Then, select the NetWorker instance as added to the Cyber Recovery UI and click **Apply**.

Result: The NetWorker server is recovered using the Cyber Recovery automated recovery process.

Test #2: Perform a recovery of a production VM in the Cyber Recovery vault virtual infrastructure environment using the recovered NetWorker server instance.

- From the Cisco UCS C220 server, launch the NetWorker NMC console and log in as administrator
- Delete the existing vProxy entry
- Deploy a new vProxy to the VxRail Cluster vCenter Server Appliance
- Restore a production VM using the newly deployed NetWorker vProxy appliance

Result: The production VM is successfully restored in the Cyber Recovery virtual infrastructure environment.

PowerProtect Data Manager Test

Test #1: Perform an automated recovery of the PowerProtect Data Manager virtual appliance in the Cyber Recovery vault virtual infrastructure environment using the Cyber Recovery UI.

- The PowerProtect Data Manager recovery is an automated process that is initiated through the Cyber Recovery UI
- The PowerProtect Data Manager instance that is deployed and configured on the VxRail Cluster is added manually to Cyber Recovery Management as an application object
- Initiate the PowerProtect Data Manager recovery by clicking **Recovery** and selecting the PowerProtect Data Manager copy from which to recover. Then, select the PowerProtect Data Manager instance as added to the Cyber Recovery UI and click **Apply**.

Result: The PowerProtect Data Manager virtual appliance is recovered using the Cyber Recovery automated recovery process.

Test #2: Perform a recovery of a production VM in the Cyber Recovery vault virtual infrastructure environment using the recovered PowerProtect Data Manager instance.

- From the Cisco UCS C220 server, launch the PowerProtect Data Manager UI and log in as admin.
- From the PowerProtect Data UI, perform the following:
  - Add the VxRail vCenter Server Appliance to Asset Sources
  - Delete the existing PowerProtect Data Manager VM Direct Engine
  - Create new PowerProtect Data Manager VM Direct Engine and deploy to VxRail vCenter Server
- Restore a production VM using the newly deployed PowerProtect Data Manager VM Direct Engine

Result: The production VM is successfully restored in the Cyber Recovery virtual infrastructure environment.

Avamar Virtual Edition

Test #1: Manually recover AVE in the Cyber Recovery vault virtual infrastructure environment

- AVE recovery is a manual process using an AVE instance that is configured with the same Avamar version and hostname as on the production system.
- The manual process used to recover AVE is based on the Avamar Checkpoint restore procedure, which can be found in the *Dell EMC PowerProtect Cyber Recovery Product Guide*.

Result: The AVE instance is successfully recovered using the manual recovery process described in the *Dell EMC PowerProtect Cyber Recovery Product Guide*.

Test #2: Recovery of a production VM in the Cyber Recovery vault virtual infrastructure environment using the recovered AVE instance:

- From the Cisco UCS C220 server, launch the AVE UI and log in as MCUser
- From the Avamar UI, perform the following:
  - Add the VxRail vCenter Server as an Avamar Client
  - Delete the existing Avamar Proxy
  - Deploy a new Avamar proxy to VxRail vCenter Server
- Restore a production VM using the newly deployed Avamar proxy

Result: The production VM is successfully restored in the Cyber Recovery virtual infrastructure environment.

Recommended best practices

The VxRail cluster was included in this design to provide a virtual infrastructure for recovery and restoration. A two-node VxRail cluster may be used but note that this configuration does not scale. For scalability, we recommend starting with a three-node minimum VxRail cluster. Due to VxRail requirements, the first three nodes of a VxRail cluster must be the same node type and configuration. In this lab environment, the VxRail E560H node was used, however, any supported VxRail configuration may be implemented to support this use case.

Note the following factors when considering scalability of a VxRail cluster in the Cyber Recovery vault environment:

- Cyber Recovery vault DD quantity and connectivity model (10 GbE compared to 25 GbE compared to 100 GbE)
- Production DD quantity and connectivity model (10 GbE compared to 25 GbE compared to 100 GbE)
- VxRail node type and connectivity model (10 GbE compared to 25 GbE and two uplinks compared to four uplinks)
- Quantity of Cyber Recovery network switches (one compared to two)

Table 1. Example environment #1

Component	Interface purpose	Switchport interfaces available	Switchport interfaces consumed
Cisco Nexus 93180YC-FX (Qty 2)	Ethernet switches	96	
Production DD6900 system	Cyber Recovery replication – 25 GbE		4
Cyber Recovery DD9900 system	Cyber Recovery replication – 25 GbE		4
	Cyber Recovery restore – 25 GbE		4
	In-band management – 10 GbE		1
	Out-of-band management – 1 GbT		1
Cyber Recovery jump server - Cisco C220	CIMC – 1 GbT		1
	Cyber Recovery vault management -1 GbT		1

Component	Interface purpose	Switchport interfaces available	Switchport interfaces consumed
VxRail 3-node cluster (4 NICs per VxRail node)	ESXi uplinks – 10 GbE		12
	VxRail node iDRAC - 1GbT		3
Firewall	LAN interface – 10 GbE		1
Restore uplinks to VxBlock 1000	Restore data from vault to production – 10 GbE		2
	Total interfaces consumed		34
	Interfaces available for VxRail cluster expansion		62

This example environment consumes 34 out of the 96 10/25 GbE switchports available, leaving 62 switchports available. Considering that each VxRail E560H node consumes five switchports, this VxRail cluster can scale by an additional 12 VxRail nodes.

This example consists of VxRail nodes with four uplinks per node, however VxRail nodes can be supported with as few as two uplinks. This configuration changes the required number of switchports for each node from five (four uplinks and one iDRAC) to three (two uplinks and one iDRAC).

The following table shows a configuration similar to the first example, except that the VxRail nodes are configured with two 25 GbE uplinks instead of four 10 GbE uplinks. The available switchport interfaces increase to 68. This increase might not seem significant, however, the VxRail nodes now only require three switchport interfaces and the VxRail cluster can scale out to 22 additional nodes.

Table 2. Example environment #2

Component	Interface purpose	Switchport Interfaces available	Switchport interfaces consumed
Cisco Nexus 93180YC-FX (Qty 2)	Ethernet switches	96	
Production DD6900 system	Cyber Recovery replication – 25 GbE		4
Cyber Recovery DD9900 system	Cyber Recovery replication – 25 GbE		4
	Cyber Recovery Restore – 25 GbE		4
	In-band management – 10 GbE		1
	Out-of-band management – 1 GbT		1
Cyber Recovery jump server - Cisco C220	CIMC – 1 GbT		1
	Cyber Recovery vault management -1 GbT		1
VxRail 3-node cluster (2 NICs per VxRail node)	ESXi Uplinks – 25 GbE		6
	VxRail node iDRAC - 1 GbT		3

Component	Interface purpose	Switchport Interfaces available	Switchport interfaces consumed
Firewall	LAN interface – 10 GbE		1
Restore uplinks to VxBlock 1000	Restore data from vault to production – 10 GbE		2
	Total interfaces consumed		28
	Interfaces available for VxRail Cluster expansion		68

Data protection of the Cyber Recovery vault environment

Protect against failures of the Cyber Recovery virtual appliance, the VxRail vCenter Server Appliance, and Platform Services Controller. These systems can be manually configured to perform backups using their native backup utilities.

The backups for each of these systems are directed to and stored on the Cyber Recovery vault DD MTree NFS shares as listed in the following table:

Table 3. Backup information

System	DD MTree	Data Domain NFS share	Frequency	Retention period
Cyber Recovery virtual appliance	create /data/ col1/cr-dr-backup	cr-dr-backup	One backup per day	14 days
VxRail vCenter Server Appliance	create /data/ col1/cr-vcenter- backup	cr-vcenter-backup	One backup per day	14 days
VxRail Platform Services Controller	create / data/col1/cr-psc- backup	cr-psc-backup	One backup per day	14 days

Note: This table provides example data and recommended values. Create the MTrees and NFS shares manually on the Cyber Recovery vault DD system. The frequency and retention period for the backups may be adjusted to individual business needs or preferences.

Additional security options and considerations include:

- When configuring a Cyber Recovery environment, you must engage a DPS SE and the BRDC to size and ensure maximum security of the Cyber Recovery vault environment properly.
- Engage a DPS SE early for proper discovery of the front-end data sizing for Cyber Recovery solutions. Possible design changes might have to be considered for the DPS backup application and CyberSense sizing requirements.
- Use of a firewall to secure the management network between the customer network and the Cyber Recovery vault network.
- Use a VPN to secure management communication to and from the vault.
- Use a jump server to mask the Cyber Recovery vault from the production system and provide a mechanism to access hosts in the Cyber Recovery vault.

- Use a data diode to provide secure one-way communication out of the Cyber Recovery vault.
- Use an in-vault patch panel to physically disconnect the network between the Cyber Recovery vault and the production system.
- Install the Cyber Recovery vault in a dedicated room or cage with physical access controls such as key access and video surveillance at entry points.
- Provide access to Cyber Recovery software only by physical access through a dedicated keyboard and mouse.

Conclusion

Cyber Recovery is an important solution that protects your organization and business from potential destruction. Our Cyber Recovery for converged infrastructure solution can be used as a baseline for any organization that is looking to protect itself from bad actors and ransomware artists, even potential internal threats. Our use of a true logical air gap, architected for converged infrastructure using our flagship data protection products, stands out from the crowd of competitors. When considering cyber resilience, remember the three common characteristics described earlier: isolation, immutability, and intelligence. Then, use Dell EMC Cyber Recovery as a key component of your organization's cyber resilience strategy.

Configuration details

This section provides configuration details about the test environment.

VxBlock 1000 CI system

- AMP-3S with Dell EMC Unity 300 storage
- Dell EMC backup solutions configured on the AMP-3S
  - Dell EMC Avamar Virtual Edition 19.4
  - Dell EMC NetWorker 19.4
  - Dell EMC PowerProtect Data Manager 19.7
- 2 x Cisco Nexus 3064-T management switches
- 2 x Cisco Nexus 93180YC-FX Top-of-Rack switches

Integrated Data Protection Cabinet

1 x PowerProtect DD6900 system

- DD OS 7.5
- iDRAC for out-of-band management
- ethMa for in-band management
- One pair of 25 GbE IO modules for production backup and restore operations
- One pair of 25 GbE IO modules for replication to the Cyber Recovery vault environment
- Licensing for DD Boost, Replication, Retention Lock Governance, and Retention Lock Compliance
- 2 x Nexus 93180YC-FX Ethernet switches

Cyber Recovery Cabinet

- 1 x PowerProtect DD9900 system
  - DD OS 7.5
  - iDRAC for out-of-band management
  - ethMa for in-band management
  - One pair of 25 GbE IO modules for Cyber Recovery restore operations
  - One pair of 25 GbE IO modules for replication from the production backup environment
  - Licensing for DD Boost, Replication, Retention Lock Governance, and Retention Lock Compliance
- 2 x Cisco Nexus 93180YC-FX Ethernet switches
- 1 x Cisco UCS C220 Rackmount Server
  - CentOS 7.9
  - DNS services
  - NTP services:

Table 4. NTP services configuration

Component	Description
CPU	2 x Intel Xeon Gold 6126 2.6GHz 12c/24t
Memory	96 GB
Storage	32 GB
Network	Out-of-band management (CIMC) – 1 GbT

- VxRail three-node cluster
  - VxRail E560 hybrid nodes with the following configuration

Per-node resource configuration

Table 5. VxRail E560 hybrid node configuration

Component	Description
CPU	Single 2.4GhZ 24C/48T Processor
Memory	256 GB
Internal SD module	2 x 64 GB microSDHC/SDXC Cards
Cache Tier storage	2 x 400 GB SSD
vSAN storage	8 x 2.4 TB SAS Drives (vSAN usable capacity of approximately 52 TB in a three-node cluster)
Network	4 x 10 GbE SFP+

- VMware vCenter Server Appliance 7.0
- VMware ESXi 7.0
- Dell EMC Cyber Recovery management appliance 19.7
- CyberSense
- Dell EMC Backup applications
  - Dell EMC Avamar Virtual Edition 19.4
  - Dell EMC NetWorker 19.4
  - Dell EMC PowerProtect Data Manager 19.7

Options

- The Cyber Recovery software may be installed on a physical host instead of a VMware Virtual appliance.
- The virtual environment may be a VxBlock or other CI\HCI option. It may also be a build-your-own environment if it supports the Cyber Recovery components and configuration.
- CyberSense may be installed on a physical host or hosts.
- Other supported Dell EMC DD systems include:
  - DD3300, DD6300, DD6800, DD9300, DD9400, and DD9800

- The capacity of the Cyber Recovery vault DD system must be the same or larger than the production DD system.

Lab environment network configuration

There are four distinct VLAN IDs that are used in the lab:

Table 6. VLAN IDs

VLAN	Description
457	VLAN used for the replication traffic between the production and Cyber Recovery vault DD systems.
405	VLAN used for management traffic between the devices in the Cyber Recovery vault.
411	VLAN used for out-of-band type access such is iDRAC and CIMC
415	VLAN used to restore data traffic in the Cyber Recovery vault.
3939	VLAN for VxRail discovery. Only configured in NetWorker or PowerProtect Data Manager Cyber Recovery environments.

- All five of these VLAN IDs must be defined on the Cyber Recovery Cisco Nexus 93180YC-FX switches.
- VLAN ID 457 is configured on the VPCs defined for both the production and Cyber Recovery vault DD virtual interfaces defined for Cyber Recovery replication. This VLAN ID is also tagged on those same DD LACP virtual interfaces.
- VLAN ID 405 is configured on the Cyber Recovery Cisco Nexus 93180YC-FX switch access ports for DD ethMa, LAN1 on the Cisco UCS C220-M5 rack mount server, and management VMkernel ports on each of the VxRail Cluster nodes.
- VLAN ID 411 is configured on the Cyber Recovery Cisco Nexus 93180YC-FX switch access ports for the DD iDRAC, Cisco UCS C220-M5 CIMC, and iDRAC ports on each of the VxRail Cluster nodes.
- VLAN ID 3939 is defined on the Cyber Recovery Cisco Nexus 93180YC-FX switches. This VLAN is only used for discovery of the VxRail nodes during the VxRail deployment and configuration process.

The following figure provides a visual representation of the Cyber Recovery network, including VLAN IDs.

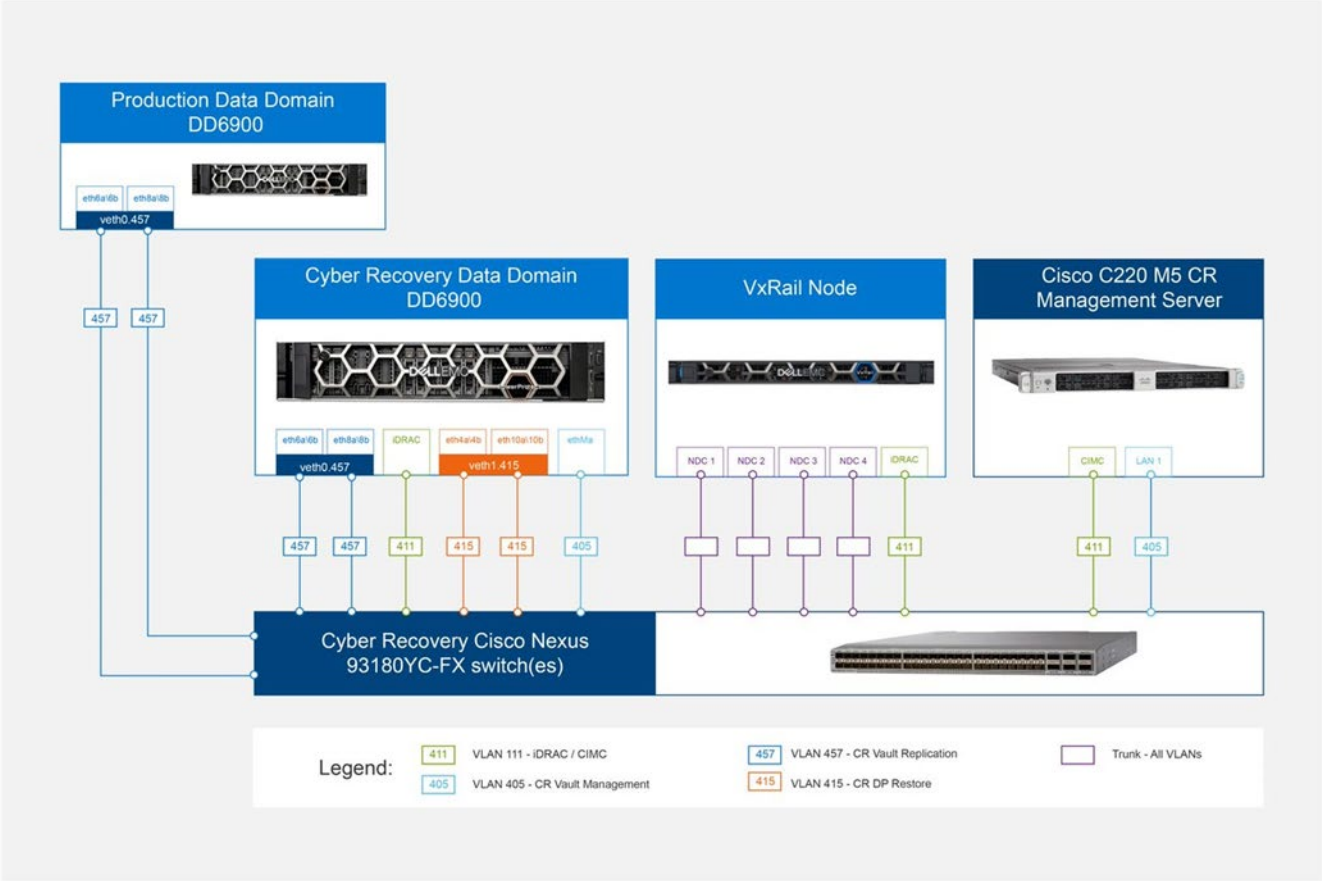

Figure 3. Cyber Recovery network

References

Dell.com/support is focused on meeting customer needs with proven services and support.

Dell Technologies documentation

The following Dell Technologies documentation provides additional and relevant information. Access to these documents depends on your login credentials. If you do not have access to a document, contact your Dell Technologies representative.

- Dell Technologies Info Hub for Integrated Products
- Dell EMC PowerProtect Cyber Recovery Solution Brief
- Dell EMC PowerProtect Cyber Recovery documents