Protect Your Data Wherever it Lives: A Data-First Strategy for Fully Integrated VxBlock Systems

March 2020

H18133

White Paper

Abstract

This white paper describes how customers can use a variety of flexible Dell EMC data protection options, such as backup, replication, business continuity, and security, to protect their environments in the data center and the cloud.

Dell Technologies Solutions

Copyright

Contents

Executive summary

Business case

Organizations have unique requirements for how their data is used and protected. No two customer environments are identical. Each is different in terms of vertical market, applications, size, recovery point objectives (RPOs), and recovery time objectives (RTOs). Organizations must define each of their requirements to design the best overall strategy for protecting their data.

Data protection challenges

As detailed in the Dell EMC Global Data Protection Index (GDPI), data protection challenges facing organizations today stem from multiple factors:

- The average volume of data that organizations are managing has increased by 569 percent from 2016 to 2018.
- Data volumes have grown from an average of 1.45 PB to 9.70 PB.
- Seventy-six percent of organizations use at least two data protection vendors.
- Data loss is twice as expensive as downtime.
- Ninety-eight percent of organizations that have public cloud use it for data protection.

Organizations are also treating data types differently when it comes to protection. For example, a healthcare organization might place more value on protecting their EPIC or Meditech applications than on their non-critical applications. Each organization sees distinct differences in the value of each application or set of data, and what is mission critical to one might not be to another. Thus, each organization must evaluate the cost of data loss to determine the resources that they should budget for data protection. The more you value data, the more it costs to lose it. Further, organizations in the European Union are subject to fines for not complying to General Data Protection Regulations (GDPR).

IT risk used to be thought of in terms of unplanned downtime; however, data loss is roughly twice as expensive as downtime, according to GDPI findings. Not only does the amount of lost data potentially increase the cost, so does the value of the data itself. One organization losing 5 TB of data might assess its loss at $3 million, while another organization could lose 50 TB worth of data but assess its loss at only $1.5 million.

The GDPI study showed that three out of four organizations use two or more vendors for data protection. This finding is significant because those who had two or more data protection vendors were twice as likely to experience a disruption in the form of data loss, unplanned outage, ransomware attack, or local disaster.

Regardless of how many vendors are used, dealing with the rising costs to protect a growing environment can be difficult. Using the public cloud is one of the primary strategies that organizations are using to address the challenge. According to the GDPI, 98 percent of organizations that use public clouds report that it is part of their data protection infrastructure.

Data protection as an integral part of IT transformation

Converged infrastructure (CI) customers face additional challenges when creating a data protection strategy. Organizations often move to a VxBlock System but retain a separate data protection solution, perhaps because it was already in place. In some cases, they purchase the CI system and then retrofit data protection after the CI system is in production.

Addressing data protection requirements at the same time as implementing or upgrading to a CI system is clearly not always possible. This might be due to budgeting or purchasing cycles, or because different teams are involved in evaluation and purchasing decisions. However, applying data protection as an afterthought to the CI system might limit the system's ultimate business value. Designing the solution with the appropriately sized backup systems is critical to optimizing the system's value. In addition, CI customers must ensure that they have the appropriate data protection solution for the types and value of workloads they are running or plan to run. Finally, they must ensure that the backup network is cost effective, is being used efficiently, and supports the backup volumes without creating a bottleneck.

Other typical challenges that emerge with a "build-it-yourself" approach to data protection include the time it takes to become operational and the overhead associated with running various disparate solutions. Consider the inherent benefits of CI, namely that it is designed, tested, and built as one solution, which is simpler and faster to deploy, less risky to run, and provides better total cost of ownership (TCO). All these benefits also extend to the integrated data protection infrastructure.

Additionally, the do-it-yourself data protection model can be difficult for IT organizations to support—especially as organizations are dealing with a growing data center or cloud environment. Backup and disaster recovery (DR) can become proportionally more difficult as the size and scope of the environment grows.

To avoid these pitfalls, data protection should be an integral part of each organization's overall IT transformation strategy and, thus, considered in conjunction with their CI system purchases.

Solution overview

Dell EMC Data Protection for Converged Infrastructure is a single-vendor data protection solution. Designed for VxBlock System customers worldwide, the solution provides flexible backup, replication, business continuity, and ransomware protection offerings to help keep data safe both in the data center and beyond.

The Dell EMC VxBlock System provides enterprises worldwide with the simplicity of a turnkey engineered CI system experience. VxBlock Systems enables customers to focus on innovating rather than spending time on maintenance.

VxBlock Systems combine multiple technologies—including powerful Dell EMC storage and data protection options, Cisco UCS blade and rack servers, Cisco LAN and SAN networking, and VMware virtualization—in one fully integrated system.

Document purpose

This white paper describes considerations for and benefits of incorporating data protection in a CI. It provides an overview of the data protection technologies in the Dell EMC Data

Protection for Converged Infrastructure solution and how the solution enhances the value of the Dell EMC VxBlock System.

Audience

This white paper is for IT professionals who are interested in learning about the benefits of integrating a data protection solution with their VxBlock System.

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.

Author: Jason Kahn

Contributors: Ignacio Borrero, Bob Percy, Karen Johnson

VxBlock System key values extended to CI data protection

Dell Technologies strives to provide value in its product and services offerings by making the “difficult” easy. To provide that value, Dell is changing the way it looks at each data set, by analyzing it and putting together a protection plan that is best suited for customer needs now and in the future.

VxBlock Systems provide five key values that extend equally to data protection. These foundational VxBlock System characteristics, or pillars of value, are:

- **Engineered**—Designed for CI, all data protection solutions are rigorously tested and documented to ensure that the solution is built correctly every time.
- **Manufactured**—Implementation and configuration are performed in the factory, using engineered standards that ensure an accurate physical and logical build.
- **Managed**—The data protection solutions are all supported by VxBlock Central, with inventory management and Secure Remote Services (ESRS), so that you always have a clear view into your data center infrastructure.
- **Sustained**—All VxBlock System and data protection components are validated with Release Certification Matrix (RCM) readiness to work together at peak performance. Each code version is documented as a unit, reducing risk to the customer and simplifying upgrades.
- **Supported**—Single call support ensures that if an issue ever occurs with either the CI or data protection, you can contact one vendor—Dell Technologies—to get it resolved efficiently.

Solution benefits

In addition to having the previously described key values at its core, Dell EMC Data Protection for Converged Infrastructure delivers the following benefits:

- **Dedicated configuration—**Integrated data protection with internal top-of-rack networking within VxBlock Systems reduces network costs (upwards of 50 percent, according to The Value of Dell EMC Storage, Data Protection, and Converged Infrastructure by Taneja Group), traffic on the network, and latency. This "switchless" interconnect also provides scalability. The configuration provides the opportunity over time to move data protection services from older third-party resources to one common CI environment, which helps to repurpose the network resources that were used to run backups through the customer's network. Integrated data protection with top-of-rack networking also reduces network resources and administrative overhead, allowing the network administrator to spend more time on strategic projects and less time on sustaining the infrastructure.
- **Storage-space and cost savings**—The Dell EMC PowerProtect DD deduplication system provides back-end data storage. As part of the Data Protection for Converged Infrastructure solution portfolio, the PowerProtect DD system is fully integrated into the VxBlock System environment and houses deduplicated data from the application environment that has been backed up. PowerProtect DD deduplication rates are the best in the industry—up to 55:1 (based on Dell Technologies' internal analysis of customer data as of May 2018), saving space and lowering the overall cost per gigabyte protected.

  Note: Deduplication rates depend on multiple factors including the type of data.

  According to the Enterprise Strategy Group (see Next-Generation Platform, Next-Generation Results), the latest PowerProtect DD models offer up to 38 percent faster backups, up to 30 percent more logical storage capacity, and up to 50 percent reduction in floor space requirements from the previous models.
- **Simplified management**— A single data-management interface supports all data protection software. Detailed and customizable reporting helps you to manage the backup infrastructure.
- **Predictive analytics and enhanced search of backup datasets**—Predictive analytics and enhanced search help spot potential risks and help find the source of any dataset that has been backed up.
- **Lower overall cost with appropriately sized and deployed software**—The software components are appropriately sized and deployed, using the shared elements of the VxBlock System management appliance (AMP Central). The system can scale out the data protection software environment as needed, lowering overall cost.

Solution components overview

Dell EMC Data Protection for Converged Infrastructure offers three categories of products and solutions:

- Data-management appliance, such as the Dell EMC PowerProtect X400. The PowerProtect X400, which is designed to be fully integrated with the VxBlock System 1000 infrastructure, provides scale-up and scale-out flexibility.
- Integrated data protection software that is tightly integrated into the VxBlock System 1000 environment and delivered fully operational from the factory:
  - **Dell EMC PowerProtect Data Manager**—The PowerProtect Data Manager software-defined platform is an integral part of the X400 appliance. It is used for both protection and management of data for VMware, SQL, and Oracle workloads.
  - **Dell EMC Data Protection Suite**—This data protection software is used for both on-premises and cloud workloads for a variety of use cases, including Microsoft and SAP workloads.

  Both products use Dell EMC PowerProtect DD as a back-end storage repository for data protection.
- High availability and security solutions:
  - **Dell EMC VPLEX**—For high availability, the VPLEX solution provides the ability to stretch clusters across a distance, giving organizations the flexibility and resiliency of having their data available in two separate locations. The solution ensures zero downtime in the event of a disaster. VPLEX also enables moving workloads to one or more sites without outages and performing nondisruptive upgrades.
  - **Dell EMC RecoverPoint for Virtual Machines**—This solution enables local, remote, and concurrent local and remote replication with continuous data protection for on-premises recovery to any point in time. Based on the VMware hypervisor, Dell EMC RecoverPoint for Virtual Machines is storage agnostic and application agnostic, with built-in orchestration and automation that are accessible though the VMware vSphere Web Client plug-in. As part of a disaster recovery strategy, Dell EMC RecoverPoint for Virtual Machines replicates to AWS and VMware Cloud on AWS.
  - **Dell EMC Cyber Recovery**—Cyber Recovery is a tailored solution that combines PowerProtect Data Manager or Data Protection Suite and PowerProtect DD. The solution provides an environment that is isolated from the production backup environment. If a cyber attack occurs, the Cyber Recovery software identifies the issue within the isolated vault environment, resolves the attack, and restores a clean copy of the backup to production.

The following sections describe these components in more detail.

PowerProtect X400 data-management appliance

The appliance offering from Data Protection for Converged Infrastructure is Dell EMC PowerProtect X400, an integrated appliance for data management. The appliance is backed by Dell EMC PowerProtect DD deduplication and the next generation of Dell EMC trusted protection storage. PowerProtect X400 is multi-dimensional, providing scale-up and scale-out flexibility and all-flash performance. Designed to be fully integrated with the VxBlock System 1000 infrastructure, PowerProtect X400 is built physically and logically in the factory so that it is ready for use in the data center.

Figure 1. Dell EMC PowerProtect X400

The PowerProtect X400 scales-out compute and capacity, and scales-up with grow-in-place capacity expansion. Available in both hybrid and all flash options, X400 provides the level of performance needed for even the most demanding workloads. The appliance is enabled with machine learning, and intelligent load balancing to provide optimal deduplication and performance.

The appliance's PowerProtect Data Manager software takes organizations from data protection to data management, providing the trusted protection in terms of backup, deduplication, and replication, but also operational efficiency in the form of self-service for application owners with IT or backup admin oversight.

PowerProtect Data Manager

PowerProtect Data Manager overview

The Dell EMC PowerProtect Data Manager software-defined platform delivers next-generation data management, addressing IT operational complexity and the propagation of new technologies. The platform enables organizations to transform IT faster and with confidence that their data is protected and available. With operational simplicity, agility, and flexibility at its core, PowerProtect Data Manager enables you to protect, manage, and recover data on premises, for virtualized and cloud deployments, with self-service capabilities for operational efficiency and IT governance controls to ensure compliance. This solution is ideal for environments with many applications running in a variety of configurations.

PowerProtect Data Manager key features include:

- Software-defined deduplication for data protection, replication, and reuse
- Self-service for data owners, combined with central IT governance
- Multi-cloud optimization with integrated cloud tiering
- Software-as-a-service (SaaS)-based management, compliance, and predictive analytics
- Modern services-based architecture for ease of deployment, scaling, and upgrading

PowerProtect Data Manager options

Application Direct

PowerProtect Application Direct integrates directly with enterprise applications, allowing application owners to have more control and visibility when backing up and restoring their applications. With more control, the database owner no longer has to go through the backup administrator, enabling faster recovery. The backup team can also perform backup and recovery operations centrally from the management console.

In addition, having client-side deduplication with a direct path between the application server and the PowerProtect DD system speeds backups and helps reduce bandwidth requirements.

Storage Direct

Sometimes, superior performance is needed. Customers with larger, fast-changing databases that require minimal application interruption can benefit from PowerProtect Storage Direct. When used with Dell EMC PowerMax or VMAX All Flash storage arrays, Storage Direct can provide faster backup and faster recovery and allow customers to meet even the strictest of service level objectives (SLOs).

As the PowerMax or VMAX array creates snapshots, Storage Direct protects the snapshots by replicating them to the PowerProtect DD system. Storage Direct then catalogs the snapshots for access in PowerProtect Data Manager.

PowerProtect Data Manager enables Oracle and Microsoft SQL DBAs to be in control of their backup and recovery practices using their native tools. PowerProtect Data Manager also provides a choice of centralized management by the backup team. VMware vSphere administrators can initiate restores directly through vSphere.

PowerProtect Data Manager centralized management and automation

PowerProtect Data Manager offers centralized oversight of all protected applications, including VMs and file system copies. This capability makes it simple to track and enforce SLO compliance for backup and recovery, RPOs, and PowerProtect DD retention lock. PowerProtect Data Manager discovers copies that are sent to data protection storage and catalogs to ensure protection compliance and quality of service.

PowerProtect Data Manager streamlines operations and ensures consistent service-level compliance. Automation delivers hands-off protection. Protection plans enable the automation of backups, which reduces administrative efforts and increases the platform's efficiency and performance.

Automated processes deliver faster time to value including automated discovery of databases, VMs, and protection storage. Discovered assets are automatically classified and assigned to preconfigured protection plans, helping enforce SLOs.

Data Protection Suite

Data Protection Suite overview

Dell EMC Data Protection Suite provides comprehensive data protection. This offering meets the needs of organizations of all sizes, protecting data and applications residing in on-premises or multi-cloud environments. Whether your environment is rich with mission-critical applications, fully virtualized, or moving to the cloud, Data Protection Suite provides the tools to meet your data protection requirements. If your environment requires multiple SLOs or entails many different use cases, Data Protection Suite offers the solution to address those needs.

Data Protection Suite includes:

- **Backup and recovery**—Provides data protection for a variety of enterprise organizations and their traditional applications such as Microsoft Exchange, SQL Server, SAP, and Oracle. The backup and recovery software is integrated with the PowerProtect DD system for a target storage deduplication rate for backups of up to 55:1 (based on Dell EMC internal analysis of customer data as of May 2018).
- **Disaster recovery**—Provides off-premises DR to the cloud with the flexibility and agility that is delivered by the cloud. Cloud DR integrates with the on-premise backup environment for space-saving replication to object storage in the cloud, with orchestrated DR and simple failover operations.
- **Continuous replication**—Offers any point-in-time recovery for the cloud and efficient replication to the cloud through Dell EMC RecoverPoint for Virtual Machines. You can set snapshot intervals from hours to seconds, depending on the workload. For example, a general-purpose interval might be every hour, while the interval for mission-critical applications would be more frequent.
- **Centralized monitoring and reporting**—Provides single-dashboard visibility, monitoring, and management across Dell EMC data protection software and protection appliances. Data Protection Central, along with Data Protection Advisor and Data Protection Search, provides a single interface for managing the backup environment for all systems, both physical and virtual.
- **Cyber Recovery**—Serves as the last line of data protection defense against cyber attacks. Dell EMC Cyber Recovery provides security to your backup infrastructure by first identifying an attack and then using automation to resolve and fail over from a clean copy that is isolated from the production environment.

Data Protection Suite use cases

The Data Protection Suite product mix for each organization depends on the organization's vertical market, use cases, and RPO and RTO targets. Examples include:

- A proven use case in the education market is to use Data Protection Suite plus PowerProtect DD to protect general-purpose workloads (Microsoft applications).
- In the pharmaceutical manufacturing industry, a customer is using Dell EMC RecoverPoint for Virtual Machines as a part of their converged environment to perform synchronous replication of their general-purpose workloads (Microsoft and Citrix). The customer has several manufacturing plants and must share data between them as well as back to the primary data center.
- In the healthcare market, a customer is using Data Protection Suite and the PowerProtect DD system for their general-purpose workloads, and they used the

VPLEX solution for their mission-critical application, Meditech. The organization saw 30 percent data growth and needed a long-term continuous availability and workload mobility solution. They couldn't afford the 4 hours of downtime per month for maintenance on their Meditech environment because it had a negative impact on patient care. Implementing the VPLEX platform with their VxBlock System infrastructure has provided a continuously available application for their caregivers in a seamlessly managed solution.

Data Protection Suite optimization for VMware environments

Data Protection Suite is optimized for VMware backup and recovery. It provides a variety of options, including image-based backup and guest-level virtual machine backup:

- Image-based backup is a backup process for a computer or virtual machine that creates a copy of the operating system and all the data associated with it, including the system state and application configurations. The backup is saved as a single file that is called an image.
- Guest-level virtual machine backup is similar to a physical host backup. Agent-based software that is installed on the guest operating system performs the backup process. Tight integration with VMware provides ease of managing backup and recovery through native VMware interfaces.

  Automated proxy management and virtual machine disk snapshots are just a couple of examples. In addition, dynamic policies ensure that each virtual machine automatically inherits the proper backup policy. Instant access to virtual machines that are protected on the PowerProtect DD system provides fast access to virtual machine images and data when there is no time to wait for a restore.

When integrated with Data Protection Suite, Dell EMC Cloud Tier natively tiers deduplicated data to the cloud. Native tiering means that an IT administrator can place a policy on one or more workloads, and, when backed up, the data is automatically sent to the cloud for long-term retention. Because no separate cloud gateway or virtual appliance is required, no additional physical footprint or management overhead is needed. A seamless process sends data directly from the PowerProtect DD system to the cloud through the central UI where the data movement policies are configured.

Data Protection Suite includes software-only continuous replication for any point-in-time recovery of on-premises VMware environments. Replication is simple and efficient over any distance with synchronous or asynchronous replication. A plug-in provides full integration with VMware vCenter and enables the administrator to manage data protection from vCenter. It also provides the ability to restore interdependent applications to a consistent state.

Advanced orchestration includes an automated workflow that enhances the operational and DR processes, reducing data loss and the time that is required for recovery.

Data Protection Suite for cloud workloads

Eighty-three percent of enterprise workloads will be in the cloud by 2020, according to Forbes, so customers need a data protection solution that supports traditional on-premises workloads as well as workloads that move to the cloud.

Data Protection Suite is optimized for the cloud and supports a wide variety of workloads. It offers comprehensive backup and recovery technology and mechanisms no matter where the data resides. Data Protection Suite with PowerProtect DD Virtual Edition

enables backup and recovery in Amazon Web Services (AWS) and Microsoft Azure. Client-side deduplication minimizes the bandwidth while reducing the protection storage requirements. You can also perform backups directly from the client to object storage.

DR is essential for applications that cannot afford downtime. However, DR can be costly and is often not configured for all mission-critical applications. Data Protection Suite offers cost-effective DR to AWS, Azure, and VMware Cloud on AWS. PowerProtect DD Cloud DR copies already-protected VMs from the on-premises PowerProtect DD system to the public cloud and directly onto object storage. In addition, Cloud DR replicates VMs from production storage to AWS. Orchestrated DR testing, failover, and automatic failback on-premises makes Cloud DR a cost-efficient solution using the agility and flexibility of the cloud.

The Data Protection for Converged Infrastructure solution currently supports several cloud-capable options to extend data protection beyond the data center. Options include Avamar Virtual Edition and PowerProtect DD Virtual Edition for cloud backup and recovery. PowerProtect DD Virtual Edition consists of a virtual appliance that is based on the PowerProtect DD physical appliance but runs on the cloud as VMs.

PowerProtect DD Cloud DR offers end-to-end orchestration, an efficient architecture that reduces resource needs, and simple operation through a standardized UI. Cloud DR in combination with Dell EMC RecoverPoint for Virtual Machines provides a cloud replication solution to help customers with tight SLOs in AWS environments.

Dell EMC RecoverPoint for Virtual Machines also offers easy and economical DR to the cloud, as shown in the following figure:

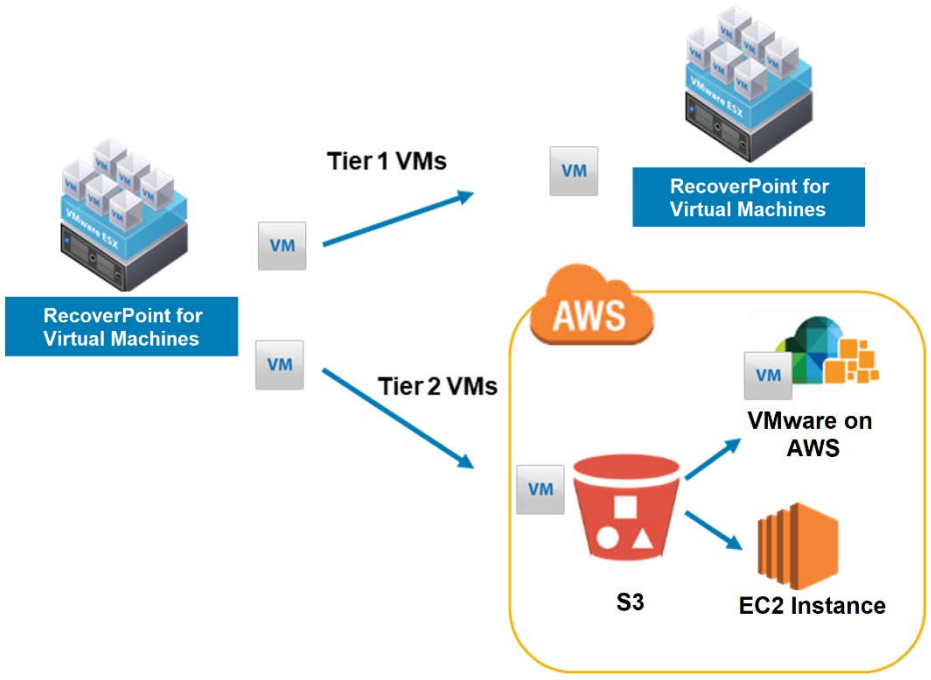

Figure 2. RecoverPoint for Virtual Machines: DR to the cloud

Using Dell Technologies' proprietary snapshot replication technology in conjunction with AWS S3, Dell EMC RecoverPoint for Virtual Machines achieves RPOs in minutes. You can combine cloud enablement with the solution's on-premises VM-based replication

capabilities, which allow sending multiple copies to the cloud and to either local or remote on-premises environments.

Dell EMC RecoverPoint for Virtual Machines with Cloud DR is cost-effective. Cloud capabilities require no additional licensing. Unlike other options that use continuous replication (which uses computing power and quickly becomes expensive), this solution transfers changes only after capturing a full copy.

VPLEX storage platform

VPLEX overview

Dell EMC VPLEX storage is designed for mission-critical applications requiring business continuity, when every bit of data must be duplicated in real time to ensure zero downtime. The VPLEX platform helps organizations modernize their data centers and optimize IT resource utilization. More than 50 percent of Fortune Global 500 companies have embraced VPLEX as part of the data infrastructure in their data centers. The solution is proven and reliable, with VPLEX market adoption exceeding 9,800 clusters globally and more than 260 million run hours.

The VPLEX platform:

- Provides availability for mission-critical applications, for which data must be consistent in two sites simultaneously
- Enables data mobility for workload balancing
- Accelerates storage array migration during a technology refresh with data mobility

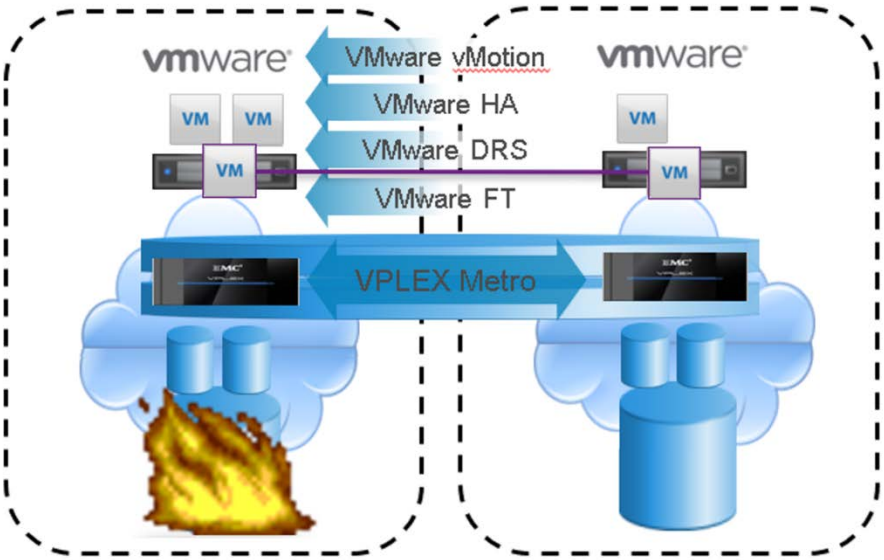

Figure 3. VPLEX topology

Application availability

For application availability, the VPLEX platform offers two deployment topologies, VPLEX Local and VPLEX Metro. VPLEX Local creates local mirrors across arrays. VPLEX Metro creates remote mirrors of the data and enables applications to seamlessly have access to the mirrored data in case of planned or unplanned downtime. Whether the downtime disruption is caused by a natural disaster, human error, or unexpected hardware failure, the VPLEX system provides organizations with uninterrupted access to their data.

Data mobility

The VPLEX platform enables customers to move data from one array to another or from one storage tier to another. This movement happens nondisruptively while the application is servicing requests. This capability creates an agile and flexible infrastructure that enables data placement that is based on optimal resource utilization.

Storage array migration

During a technology refresh that replaces older storage arrays with new all-flash arrays, the VPLEX platform helps migrate all the data nondisruptively while the application is online and business operations are running normally. VPLEX shortens the technology refresh process and speeds up time to value.

Cyber Recovery solution

The challenge: Cyber attacks on business-critical systems

No matter the industry or size of the organization, cyber attacks are on the rise. The frequency of attacks is growing exponentially, with hacking and malware making up 52 percent and 28 percent of attacks respectively, according to the *2019 Verizon Data Breach Investigations Report*.

According to the RSA Cybersecurity Poverty Index, 66 percent of organizations report that they have had a security incident that negatively affected their operations, and 72 percent of organizations say they are still "immature" (or worse) in capabilities involving incident response and recovery. Remediation from a destructive cyber attack is often painful and time consuming, with a direct negative impact on an organization's bottom line.

All organizations are concerned about a destructive cyber attack, and 59 percent of organizations believe that isolating affected systems and recovering from backups should be the response to ransomware, according to the *2017 State of Cybercrime Report* by Secureworks.

Hackers' primary entry mode is through an organization's many end-point devices. Alternatively, hackers resort to phishing techniques and zero-day malware that enters the environment through email. The likelihood that all malware will be discovered before harm is done is slim, and the discovery time for an attack is still likely to be measured in weeks or months. This time gap provides hackers with the opportunity to map the network, escalate privileges, and plan a devastating attack, ranging from extortion (ransomware) to outright destruction of business-critical systems. These types of cyber attacks can cripple an organization, leading to expensive remediation, revenue loss, negative publicity, and lasting customer distrust. As fast as organizations build defenses against different attack vectors, hackers devise new ways to circumvent them.

To create a more comprehensive approach to cyber-risk mitigation, organizations need to evolve and automate their business continuity and recovery strategies. Focusing on threat detection analysis and remediation. Dell EMC Cyber Recovery provides the power to enable an automated workflow to augment data protection infrastructure with true data isolation, data forensics, analytics, and—most importantly—data recovery for increased business resiliency.

Dell EMC Cyber Recovery software

Data Protection for Converged Infrastructure offers Dell EMC Cyber Recovery to combat ransomware attacks on enterprise backup environments.

Cyber Recovery combines PowerProtect DD or Data Protection Suite and the PowerProtect DD system to isolate the backup environment. The Cyber Recovery software identifies and resolves cyber attacks within the isolated environment. It then restores a clean copy of the backup to the production environment.

Recovery is the key when ensuring that business-critical data can withstand a cyber attack designed to destroy or cripple an organization's data including backups and replicas. The Dell EMC Cyber Recovery solution incorporates the following elements to build a final line of defense:

- **Solution planning**—Selection of application candidates, recovery time, and RPOs

- **Isolation and governance**—An isolated data center environment that is disconnected from the network and restricted from users other than those with proper clearance
- **Automated data copy and air gap**—Software to create WORM-locked data copies to a secondary set of arrays and backup targets as well as processes to create an operational air gap between the production environment and the isolated recovery zone
- **Integrity checking and alerting**—Workflows to stage replicated data in the isolated recovery zone and perform integrity checks to analyze whether the data is affected by malware, along with mechanisms to trigger alerts on suspicious executables and data
- **Recovery and remediation**—The use of dynamic restore processes and existing DR procedures to perform recovery/remediation after an incident

The centerpiece of Cyber Recovery is the CR Vault, an isolated and protected part of the data center. The CR Vault hosts the organization's critical data on Dell EMC technology that is used for recovery and security analytics. The goal of the CR Vault is to move data away from the attack surface, so that if a malicious cyber attack occurs, customers can resort to a valid copy of data to recover critical business systems. Using vault protections around the isolated data also protects it from insider attacks. Cyber Recovery automates the synchronization of data between production systems and the CR Vault and creates immutable data copies, as depicted in the following figure:

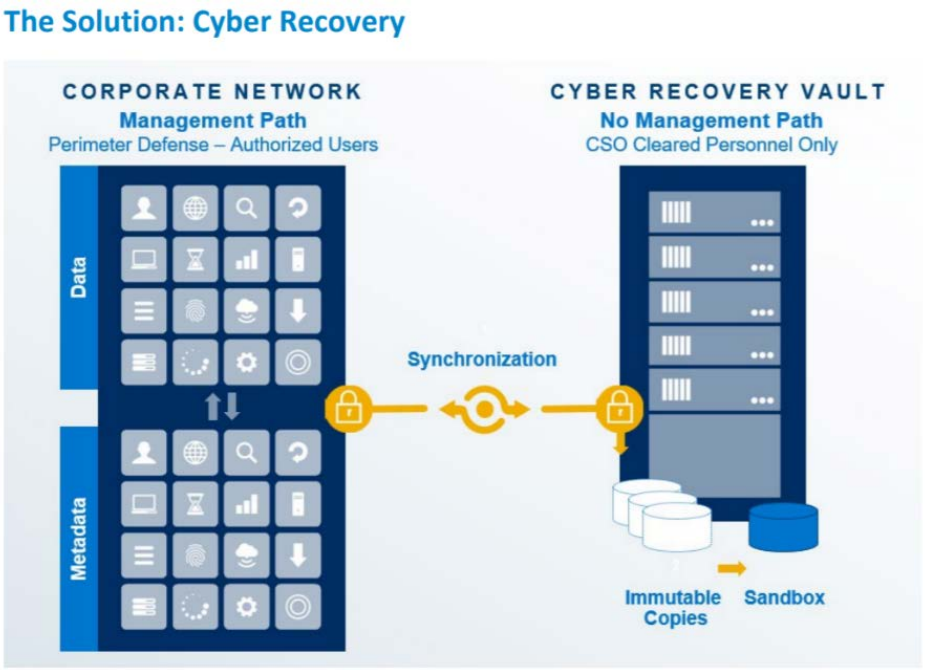

Figure 4. Cyber Recovery

Dell EMC Cyber Recovery combines Avamar, PowerProtect DD, and networking as well as a management host that houses the software components. This Cyber Recovery solution can be integrated into a customer's VxBlock System environment for both greenfield and brownfield deployments.

Summary

VxBlock System 1000 with Data Protection for Converged Infrastructure can greatly help an organization in its IT transformation journey. Data Protection for Converged Infrastructure solution components are engineered from the factory and integrated into the VxBlock System environment, reducing the load on the customer network. Solution components are supported and sustained as one offering.

Dell Technologies provides innovative and trusted products that meet customer needs in the data center and beyond for almost any mix of workloads. Dell EMC Data Protection for Converged Infrastructure can protect an enterprise organization’s data wherever it lives.