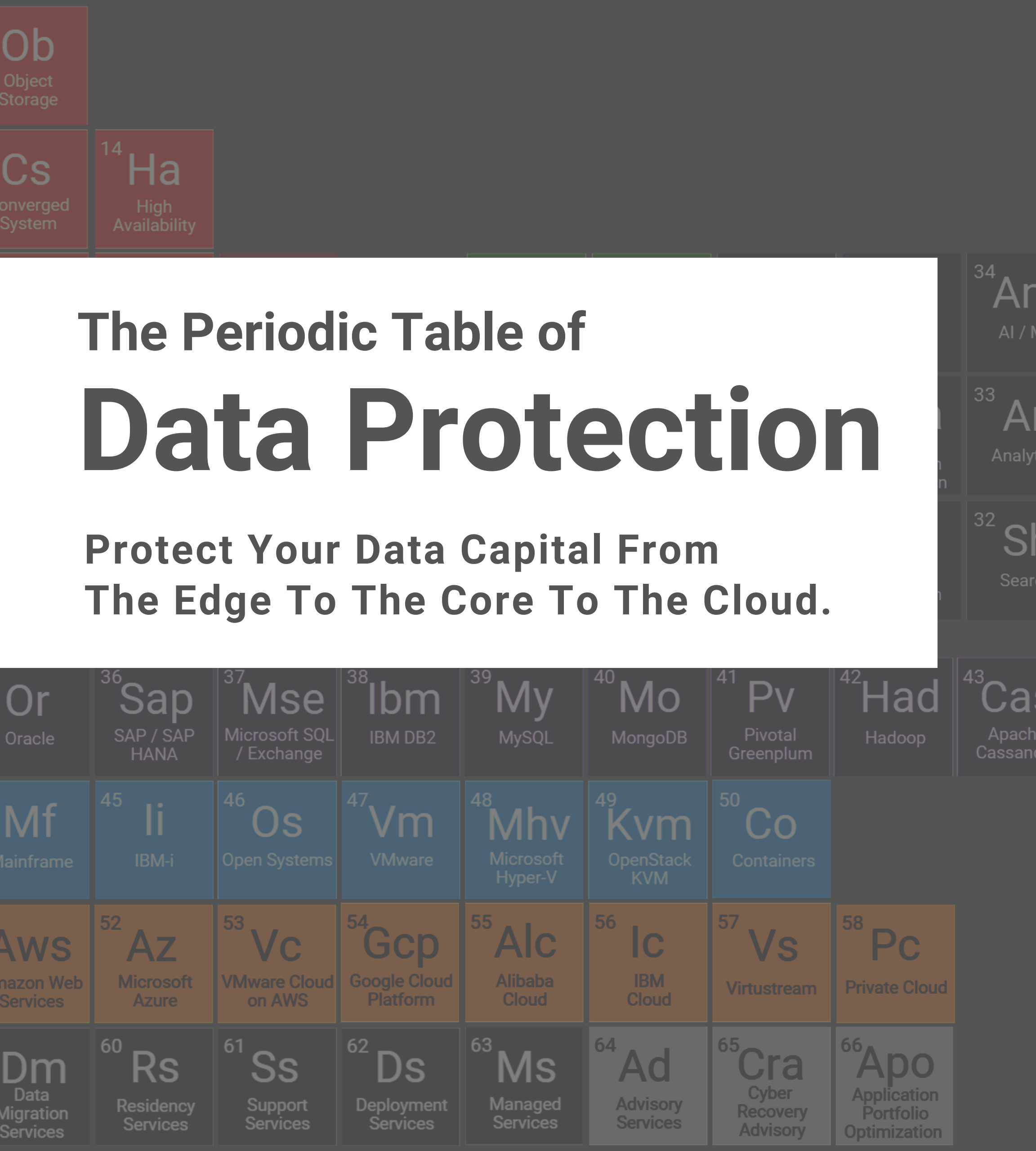
DELL EMC

The Periodic Table of Data Protection

Protect Your Data Capital From The Edge To The Core To The Cloud.



Foreword

Data protection is never an afterthought. It has to be on the checklist of any data center expansion and IT projects.

Based on today's increasing threats to data integrity on a number of fronts, the topic of data protection is a primary concern to many CTOs, CIOs, CDOs and DPOs[1]. If organizations are truly serious about monetizing their data assets, they have to put their IT investments in areas where it matters. And these include their data protection and cybersecurity framework. It’s about time that the executive board confronts the elephant in the room.

Businesses will not be able to monetize data if you cannot protect it. 40% of businesses surveyed recently, had suffered unplanned system downtime and 28% have suffered data loss in the last 12 months. Of these businesses, 41% reviewed that they encountered an external or internal security breach[2].

Let’s face it. There is no one-size-fits-all when it comes to data protection. It is a complex subject, especially when organizations are facing challenges in explosive growth in data volumes, cybersecurity threats and shifts in regulatory compliance requirements. Not only do organizations need to navigate the trends toward a multi-cloud world, they need to find effective ways to unlock and protect their Data Capital[3].

The job of the CTO, CIO and DPO is never done. You may find yourself struggling in fulfilling your data protection service level agreements and not having the confidence to recover your data in the events of a cyberattack, ransomware attack or even recovering from primary backups or your cloud service platforms. With evolving global and local data privacy laws and regulatory compliance requirements, you too need to ensure that your data protection strategy is regularly refined to meet those requirements.

[1] Data Protection Officer

[2] Source: Global Data Protection Index 2019, Dell EMC

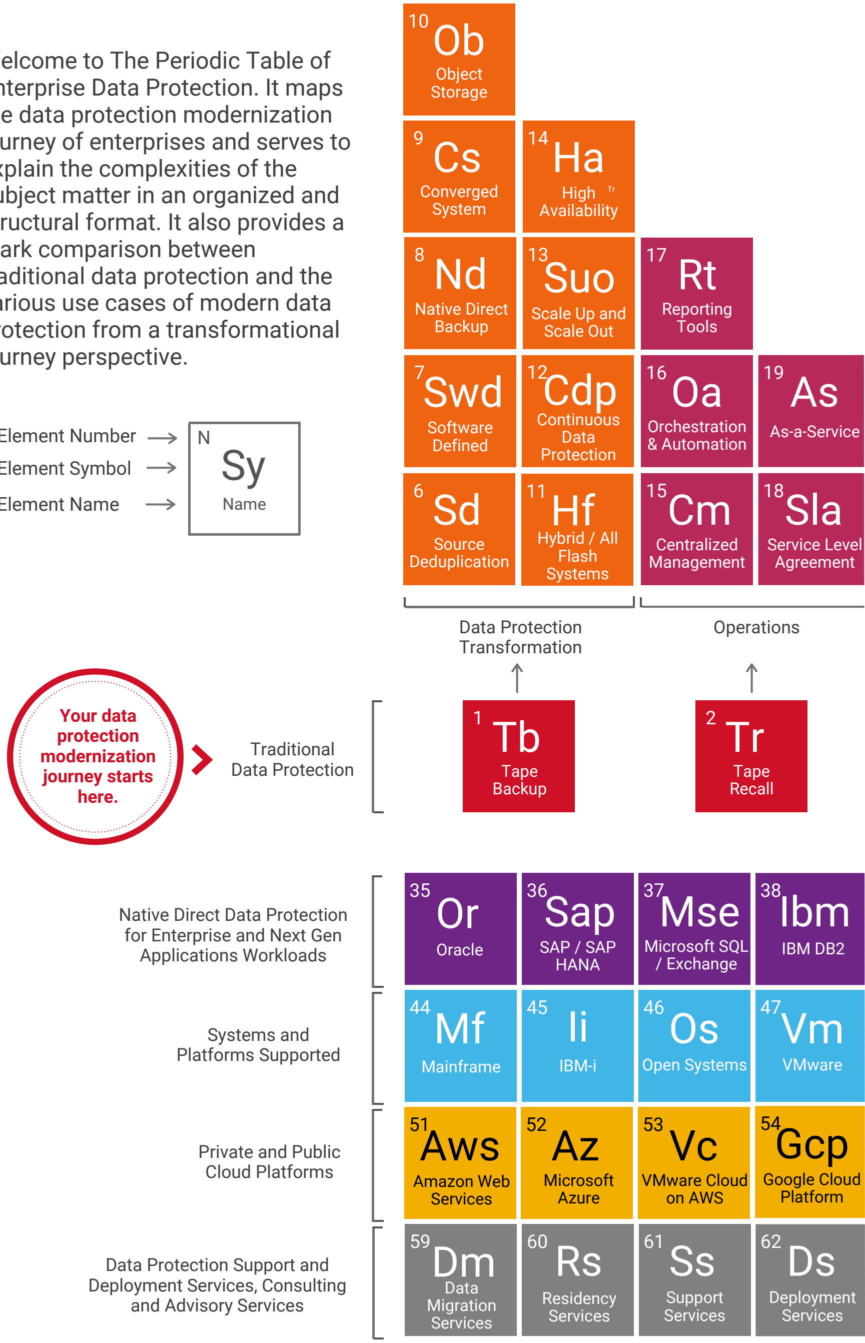
[3] Source: Unlock Your Data Capital with Dell EMC, 2019, Dell EMC

Starting from ground up, this guide serves to address the complexity of enterprise data protection and to help IT professionals and business IT users segue from legacy backup applications and systems to protect their Data Capital via data protection modernization.

I look forward to hearing from you your future state of enterprise data protection, and how Dell EMC can journey with you in achieving or enhancing that.

Alex Lei
Vice President
Data Protection Solutions
Asia Pacific and Japan
Dell EMC

Welcome to The Periodic Table of Enterprise Data Protection. It maps the data protection modernization journey of enterprises and serves to explain the complexities of the subject matter in an organized and structural format. It also provides a stark comparison between traditional data protection and the various use cases of modern data protection from a transformational journey perspective.



Element Number → N

Element Symbol → Sy

Element Name → Name

Data Protection Transformation

10 Ob Object Storage

9 Cs Converged System

14 Ha High Tr Availability

8 Nd Native Direct Backup

13 Suo Scale Up and Scale Out

7 Swd Software Defined

12 Cdp Continuous Data Protection

6 Sd Source Deduplication

11 Hf Hybrid / All Flash Systems

Operations

17 Rt Reporting Tools

16 Oa Orchestration & Automation

19 As As-a-Service

15 Cm Centralized Management

18 Sla Service Level Agreement

Your data protection modernization journey starts here.

Traditional Data Protection

1 Tb Tape Backup

2 Tr Tape Recall

Native Direct Data Protection for Enterprise and Next Gen Applications Workloads

35 Or Oracle

36 Sap SAP / SAP HANA

37 Mse Microsoft SQL / Exchange

38 Ibm IBM DB2

Systems and Platforms Supported

44 Mf Mainframe

45 Ii IBM-i

46 Os Open Systems

47 Vm VMware

Private and Public Cloud Platforms

51 Aws Amazon Web Services

52 Az Microsoft Azure

53 Vc VMware Cloud on AWS

54 Gcp Google Cloud Platform

Data Protection Support and Deployment Services, Consulting and Advisory Services

59 Dm Data Migration Services

60 Rs Residency Services

61 Ss Support Services

62 Ds Deployment Services

The Periodic Table of DATA PROTECTION

🟥	Tape-based Solutions
🟧	Disk-based Solutions
🟥	Data Protection Management
🟩	Data Security & Cyber Recovery
🟦	Cloud Data Protection
⬛	Data Management
🟪	Enterprise and Next Gen Apps
🟦	Systems and Platforms
🟨	Cloud Platforms
⬛	Support and Deployment Services
⬜	Consulting and Advisory Services

22 Rc Retention & Compliance	25 Irv Isolated Recovery Vault	28 Ltr Long Term Retention	31 Cdr Cloud Disaster Recovery	34 Am AI / ML
21 Er Encryption At Rest	24 Oc Offsite Copy	27 Mc Multi-cloud Protection	30 Cpa Cloud Protection Automation	33 An Analytics
20 Ep Endpoint Security	23 Km Key Management	26 Scm Single Centralized Management	29 Icp In-cloud Protection	32 Sh Search
Security		Cloud		Data Management
↑		↑		↑
3 Tle Tape Library Encryption		4 Ot Offsite Tape		5 Trm Tape Resource Management

39 My MySQL	40 Mo MongoDB	41 Pv Pivotal Greenplum	42 Had Hadoop	43 Cas Apache Cassandra
48 Mhv Microsoft Hyper-V	49 Kvm OpenStack KVM	50 Co Containers		
55 Alc Alibaba Cloud	56 Ic IBM Cloud	57 Vs Virtustream	58 Pc Private Cloud	
63 Ms Managed Services	64 Ad Advisory Services	65 Cra Cyber Recovery Advisory	66 Apo Application Portfolio Optimization	

Download e-Guide on the use of the Periodic Table of Enterprise Data Protection:

Read more:
DellEMC.com/dataprotection

DELL EMC

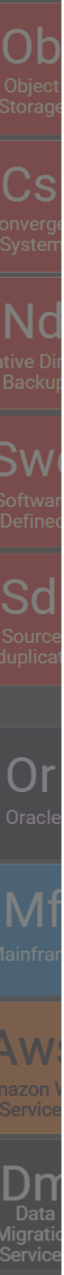


Table of Contents

Introduction

Welcome to “The Periodic Table of Data Protection”.

A visceral response from some CIOs or CTOs is very often, “speak with my IT director about data protection”. How I wish that is so straight forward!

With growing complexities in managing backups and recovery from the edge to the core, and to the cloud --- as well as meeting stringent service level agreements and regulatory compliance requirements, and data center consolidation --- the odds stacked against enterprise IT are growing like never before.

If you plan to work on digitalizing your business or transforming your data center, this guide is meant for you. As the technology industry continues to innovate amidst the evolving and disruptive trends and new use cases, Dell EMC is committed to bring on proven, best practices in helping our customers assess their state of data protection readiness and meeting their IT goals.

This Periodic Table of Data Protection is the first step in doing so. It aims to organize information in a thematic and easy-to-read format by categorizing the many aspects of data protection challenges into essential IT pillars such as data protection transformation, operations, security, cloud and Data Capital. Each of these pillars is by no means, the be-all and end-all as every IT organization is unique in their path and development towards IT transformation. This Periodic Table helps to bring into perspective, the modern data protection transformation journey, and to lead to discovery in gaps which then provides an opportunity to refine or fine tune your data protection strategy and framework.

Data protection is not an end game. Choosing the right data protection technologies is critical in unlocking your Data Capital for greater business impact and operational benefits.

BETH PHALEN
President & GM, Data Protection Division, Dell EMC | @bethphalen
theCUBE
LIVE from theCUBE Studios in Boston, MA
Sponsored By
DELLEMC

How To Use The Periodic Table

Inspired by the “Periodic Table of Chemical Elements”, this guide is curated to explain the data protection modernization journey starting with traditional tape backup, and navigating through the essential IT pillars comprising data protection transformation, operations, security, cloud and data management.

The reader is able to explore the various technologies and solutions to reduce or eradicate the reliance of tape backup infrastructure in order to resolve existing challenges associated with tape backups. Even if your data center has gone tapeless, there may be other possibilities found in this Guide that may be helpful in simplifying or fortifying your data protection strategy.

We recommend that you start with each element in sequential order. For instance, element numbers 1 to 5 gives an overview of traditional data protection. The arrows from each of these elements correspond to the 5 pillars of data protection transformation journey. The elements in each pillar are stacked according to their levels of maturity and sophistication. Under the pillar of "Data Protection Transformation" for example, the element of "High Availability" is considered in our opinion, having the highest level of sophistication for any IT organization to adopt. Of course, it is never intended to implicate that the solution is required as every IT organization and requirement is different. Where applicable, zoom into specific elements for more bite-sized narrations. For more information, there are hyperlinks on videos and solution web sites.

Go through each corresponding element and assess your current data protection strategy if there are gaps.

This Periodic Table is also designed to be printed as a poster. Pin it on your office wall or cubicle wall to kick start data protection conversations with your colleagues and managers, and score some brownie points along the way!

Enjoy your data protection transformation journey!

What is Data Capital?

Data is our most valuable asset. Data powers digital transformation. Nearly every business in the world are including Big Data, the Internet of Things, Artificial Intelligence, IT transformation, and improved digital experiences as elements of broader digital transformation strategies. Because of the important role data plays today, Data Capital is quickly becoming the most valuable asset in a company's portfolio. What is Data Capital? IDC defines it as "the wealth in the form of value derived from organizational data"[4].

Even when its value is recognized, current approaches to data and the inherent limitations of legacy data storage systems can pose serious challenges to companies looking to unlock and monetize their Data Capital. These challenges include:

- Silo-based data storage, which limits visibility and the ability to leverage data;
- Inability to cope and scale with exponential data growth;
- Ineffective data protection strategy to protect their data due to disparage data protection solutions and overheads; and
- Lack of insights into data for the conversion of data to impact business

To get value from your data, you must make it a foundational consideration in your strategic business planning. For most organizations, this means a paradigm shift and adopting new technologies. Organizations we have already helped have taken advantage of their data across their business to create a competitive advantage by improving their cost structures, enhancing productivity, and creating new services and revenue streams.

[4] Source: IDC Unlock the Power of Data Capital: Accelerate DX, November 2018. Sponsored by Dell EMC.

To fully unlock the value of Data Capital, attention must be paid to where data resides, how it is managed, and how it's protected. Therefore it is essential that organizations modernize IT.

Equally important is the need to secure and protect your Data Capital effectively. As data becomes an essential part of the business, IT must consider performance, cost, data protection, security, governance, and infrastructure management characteristics to decide what platform is best suited to leverage.

This means that enterprise IT needs to have visibility of where the data resides from the edge to the core, and to the cloud, and having 100% coverage across the data protection continuum.

Charting Your Data Protection Modernization Journey

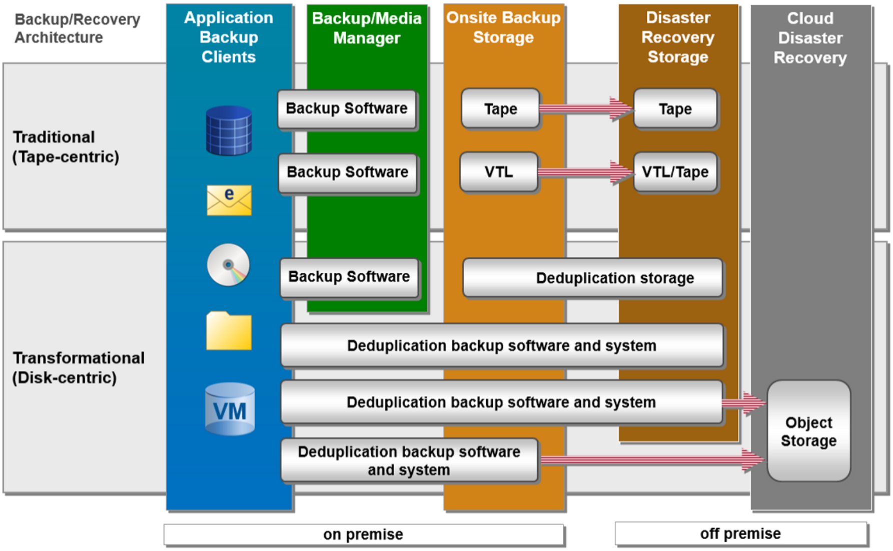
We recommend that you test out the Periodic Table of Data Protection -- to begin looking at a broader picture and identify some opportunities of enhancements for some of your pressing IT challenges.

Today, enterprise IT needs to manage their applications and data in multiple sites, from on-premise traditional infrastructures to virtualized environments, to hybrid clouds. You need to put in place a robust data protection strategy that acknowledges this complex landscape and eliminates accidental architectures across consumption models in order to avoid more silos and increase data visibility. Here's some of the characteristics of a modern data protection infrastructure:

- Open, efficient and high performance
- Wide service levels
- Scalable
- Automation and self-service capable
- Cloud-enabled
- Trusted, protected and safe

IT consolidation is a top priority for many enterprise IT organizations. Not only are we looking at storage silos, we need to streamline the data protection infrastructure and operations in order to support current and future IT expansions.

In the Periodic Table, we have outlined 5 essential IT pillars for data protection. Assess your current data protection state of health by going through each pillar and identify areas of enhancements based on your priorities and resources. It is not meant as a silver bullet for your data protection transformation but certainly a good start in taking stock of the mishmash of different backup systems.


Backup/Recovery Architecture
Application Backup Clients
Backup/Media Manager
Onsite Backup Storage
Disaster Recovery Storage
Cloud Disaster Recovery
Traditional (Tape-centric)
Backup Software
Tape
Tape
Backup Software
VTL
VTL/Tape
Transformational (Disk-centric)
VM
Backup Software
Deduplication storage
Deduplication backup software and system
Deduplication backup software and system
Deduplication backup software and system
Object Storage
on premise
off premise

Let's start with traditional backup infrastructure, which is tape-centric and operations intensive. If you have tape backup infrastructure in your data center, we recommend that you begin there and look at the benefits and TCO of disk-based backup solutions.

Disk-based data protection or protection storage opens up new capabilities and possibilities, including backup infrastructure consolidation, remote disaster recovery via secure replication and long term retention to the cloud.

You may wish to engage Dell Technologies in consulting and advisory services in meeting your IT transformation goals. Leveraging the Dell Technologies portfolio and partner ecosystem, we can help you achieve real business outcomes in your initiatives for multi-cloud, applications, DevOps, infrastructure, business resiliency, data center modernization, analytics, workforce collaboration, and user experiences.

Traditional Data Protection

1
Tb
Tape Backup

Tape Backup

Tape backup is generally viewed as the aphorism of cost effective archival and disaster recovery. This practice, which still exists in many enterprise data centers, is rapidly losing its shine due to the fall in disk prices and, the flexibility and economies of object-based cloud storage.

First of all, tape systems are inherited with proprietary formats. Tape backup also means that sensitive corporate records are found on transportable, degradable media. Tapes are susceptible to physical tape drive and media failures, lost tapes, and numerous points of failure, as well as isolated views of tape volumes. It has no support for retention or privacy policies, making compliance almost impossible. It also has limited disaster recovery capabilities – slow recovery, limited RTO/RPO granularity and cumbersome DR testing.

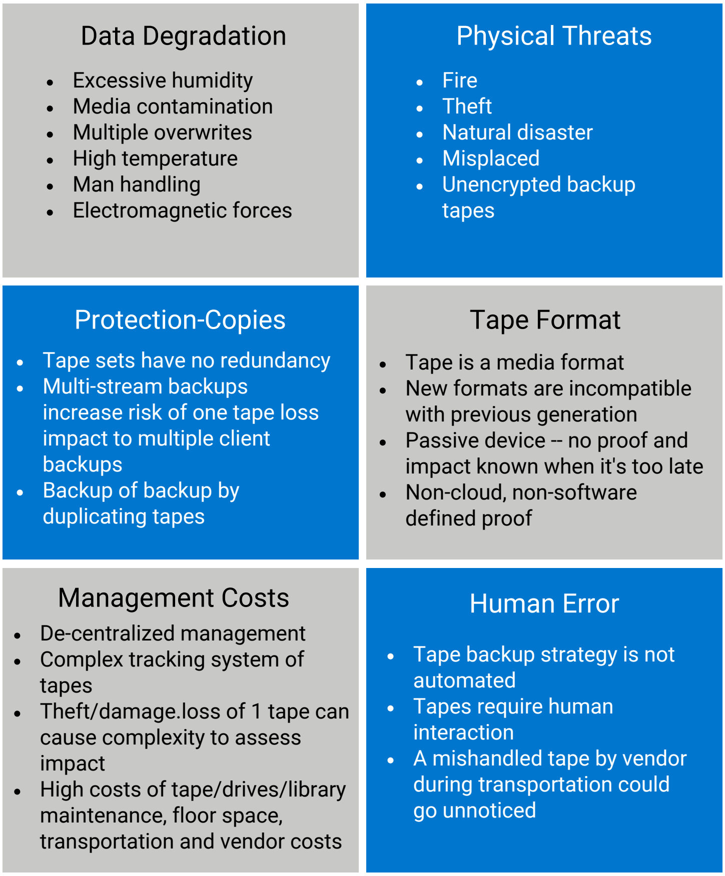
Tape Backup

- Read / Write
- Multiplexing
- Tape Encryption
- Compression

Disk-based Backup

- Read / Write
- Speed
- Data Encryption
- Life Cycle Management
- WORM
- RAID
- Deduplication & Compression
- Automated Disaster Recovery
- Cloud Ready
- Cyber Protection

Tape vs Disk-based Backup



Data Degradation

- Excessive humidity
- Media contamination
- Multiple overwrites
- High temperature
- Man handling
- Electromagnetic forces

Physical Threats

- Fire
- Theft
- Natural disaster
- Misplaced
- Unencrypted backup tapes

Protection-Copies

- Tape sets have no redundancy
- Multi-stream backups increase risk of one tape loss impact to multiple client backups
- Backup of backup by duplicating tapes

Tape Format

- Tape is a media format
- New formats are incompatible with previous generation
- Passive device -- no proof and impact known when it's too late
- Non-cloud, non-software defined proof

Management Costs

- De-centralized management
- Complex tracking system of tapes
- Theft/damage.loss of 1 tape can cause complexity to assess impact
- High costs of tape/drives/library maintenance, floor space, transportation and vendor costs

Human Error

- Tape backup strategy is not automated
- Tapes require human interaction
- A mishandled tape by vendor during transportation could go unnoticed

Other Tape Challenges

Last but not least, it comes with hidden costs to finding, managing and accessing legacy data, especially for long term retention.

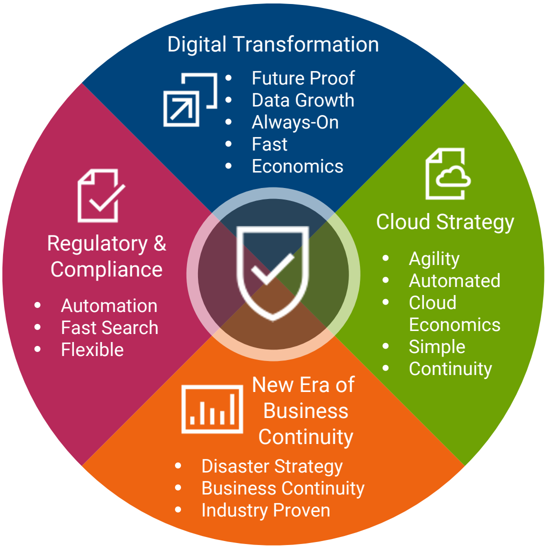
There is a secular shift from tape-centric to disk/network-centric approaches due to the advance of massive data deduplication and compression techniques. Unabating growth of enterprise data overwhelms legacy backup infrastructure. Server virtualization, cloud economies and regulatory compliance requirements accelerate IT decisions to move towards a tapeless infrastructure.

2 Tr
Tape Recall

Tape Recall

Tape recalls for data recovery are labor intensive. Time to recovery is exponential if full production site restore is required. There is also risks of data loss due to media damage, dead spots on tape, missing tapes and tapes out of sequence on restores.

Operationally, the backup team needs to maintain a system of tape tracking, especially if the internal system does not match that of the storage vendor. Backup window increases as data grows, requiring the addition of more tape drives to keep within the desired backup window. Many tapes will leave the tape library significantly less than 100% full, especially in environments with large tape libraries/drives and multiple data streams from multiple clients, which translates to reduced value in tape usage.



The Accelerators to Challenge Tape-based Backups and Recalls

Tape handling times by staff and tape library adds to backup/restore times. For example, when tape drive cleaning is in progress, that drive cannot be used.

3 Tle
Tape Library Encryption

Tape Library Encryption

Tape encryption solutions cannot deliver the scale, flexibility, or price performance requirements for large data volume requirement. Enterprise encryption key management solutions are lacking or inadequate for a distributed service instead of all-in-one solution.

New regulatory compliance requirements, such as EU General Data Protection Regulation (GDPR), require higher levels of data risk management for securing personal and critical data with the flexibility to provide the "right to erasure" service for individuals requesting for their records to be deleted permanently within a reasonable time frame regardless of where the data resides. This further strains IT security processes, especially when dealing with tape recalls and encryption key management. High performance tape library encryption solutions avoid bottlenecks but are not cost-effective and are operationally intensive.

4 Ot
Offsite Tape

Offsite Tape

Tapes are typically stored off-site for less frequently accessed data or archives. For long term retention, tape comes with major challenges:

- Lack of agility: Data retrieval needs to be planned and scheduled ahead of time as there is no transparent on-demand access capability
- High operating costs: Tape management and backup administration and audit cost far exceeds the perceived low media cost
- Poor reliability: Tape media, hardware, software, and human error increase restore failure rates
- High risk: Tapes in transit between data centers and offsite storage locations are at risk of loss and tampering

Efficient deduplication and network bandwidth utilization have given rise to better cost-effectiveness and operational efficiency with data replication between primary and secondary sites for disaster recovery.

5 Trm
Tape Resource Management

Tape Resource Management

Some tape library vendors offer tape resource management software which serves to report on tape capacity usage and manage tape encryption keys. In reality, such tools cannot address the challenges facing tape backup and provide an optimized tape operating environment where it matters.

What enterprise IT needs is a simple and effective tool to index and restore data so that there is no bottlenecks and without having to restore full data sets from tapes before searching and extracting the relevant data for recovery.

Data Protection Transformation

6 Sd Source Deduplication

Source Deduplication

This is a game-changer for the traditional backup architecture. Deduplication technology enables customers to store more data on the same amount of physical disk space. This reduces storage capacity requirements and drives down cost. Data deduplication implemented at the source or client side also helps with capacity savings, but with the added benefit of improving backup performance. With source-side deduplication, only unique data blocks are sent from the source to the target during the backup operation, which significantly reduces network traffic. This improved network efficiency allows for backup data growth using existing network infrastructure and possibly eliminates or postpones the need for expensive network upgrades. Obviously, the less data that needs to be transferred, the faster the backup performance. Shorter backup durations also allow customers to increase the frequency of backups, reducing the risk of data loss, which can be extremely costly to an organization.

Purpose-built backup appliances and integrated data protection appliances are designed to have both source- and target-based data deduplication natively integrated into the architectures. Dell EMC DD Boost software, PowerProtect DD and Integrated Data Protection Appliance systems support both source- and target-side deduplication, giving customers the flexibility to deploy deduplication where it makes the most sense for their environments. Inline deduplication is performed in CPU and memory as the backup stream is received by the system, thereby eliminating the need for a disk staging area and compute resources for post-process deduplication.

ESG's analysis of real-world data, including hardware, software, power, cooling, and deduplication, demonstrates that Dell EMC Integrated Data Protection Appliance systems are easily capable of serving storage to data protection environments for fractions of a penny per GB per month[5].

7 Swd
Software Defined

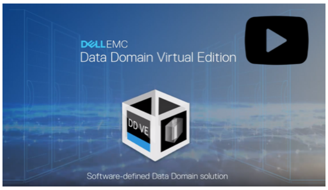
Software Defined

Dell EMC PowerProtect DD Virtual Edition is the ideal software-defined protection storage for your virtualized environments. PowerProtect DD Virtual Edition enables customers to quickly and easily deploy an industry-leading PowerProtect Software in a variety of new deployment models for the ultimate in flexibility.

It comprises core PowerProtect DD features including data deduplication, replication, data integrity, and encryption and it's ideal for Remote Office and Branch Office (ROBO), entry-level protection storage and cloud environments.Its benefits include:

Simple: Deploy in minutes
Flexible: Grow as you need
Efficient: Reduce resource requirement

PowerProtect DD Virtual Edition is available for download and evaluation at Dell EMC Software Download microsite, AWS Marketplace and Azure Marketplace.


DELL EMC
Data Domain Virtual Edition
DD VE
Software-defined Data Domain solution

[5] Source: The Economic Value of Dell EMC Data Domain and Integrated Data Protection Appliance (IDPA), ESG, June 2018

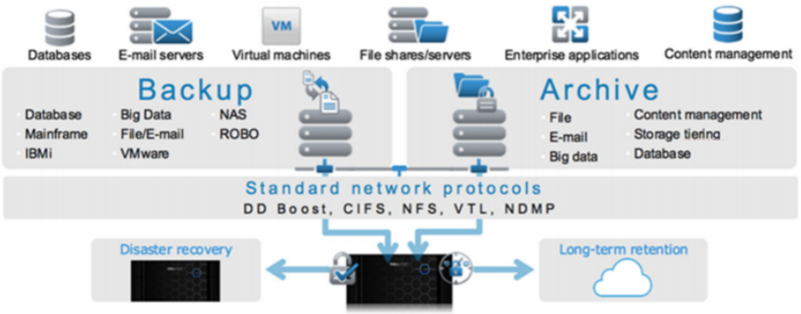
8 Nd
Native Direct Backup

Native Direct Backup

Fail to meet backup windows SLA? Dell EMC data protection solutions include native direct backup and recovery capabilities for storage-direct, VMware-direct and application-direct data protection.

Dell EMC PowerProtect DD systems integrate easily with existing infrastructures and can be used seamlessly with leading backup and archiving applications. Integrating a PowerProtect DD system into your environment does not require any change in process or infrastructure, so you can realize the value of deduplication quickly and efficiently. In addition, PowerProtect DD can integrate directly with leading enterprise applications such as Oracle RMAN or write directly over CIFS or NFS to support a variety of workloads.

A single PowerProtect DD can be used for backup and recovery of the entire enterprise applications environment (including Oracle, SAP, Microsoft and VMware, IBM i and mainframe environments) as well as protecting archive data (including file, e-mail, enterprise content management, database and Virtual Machine archiving).



Rather than sending all data to the PowerProtect DD system for deduplication processes, DD Boost enables the backup server or application client to send only unique data segments across the network to the PowerProtect DD system. This reduces the amount of data transferred over the network by up to 98%[6].

The DD Boost software provides:

- Faster, More Efficient Backup: Distributes parts of the deduplication process to backup server or application client - 50% faster backups and up to 98% less network bandwidth required.[6]
- Simplified Disaster Recovery: Enables application to control PowerProtect DD replication process with full catalog awareness.
- Advanced Load Balancing and Failover: Aggregates transport links for transparent load balancing and automatic link failover.
- DD Boost Everywhere: DD Boost File System Plug-in, which expands application support.

Converged System

One of the major challenges of today's data protection solutions is that setup is often complex and that there is often a need to deploy and manage multiple point solutions for different applications, platforms and data silos. Managing multiple products (for example, backup software, backup servers, search servers, backup hardware) and multiple vendors can result in lengthy and time-consuming deployment, and complex and expensive management of fragmented data protection environments.

[6] Source: The Economic Value of the Dell EMC Data Protection Portfolio, ESG, March 2019

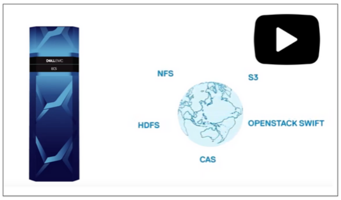
Dell EMC Integrated Data Protection Appliance (IDPA) is a pre-integrated, turnkey solution that is simple to deploy and scale, provides comprehensive protection for a diverse application ecosystem, and comes with native cloud tiering for long-term retention. IDPA combines protection storage, protection software, search, and analytics to reduce the complexity of managing multiple data silos, point solutions, and vendor relationships.

10 Ob Object Storage

Object Storage

Object storage provides organizations with an object-storage platform capable of supporting traditional and modern workloads alike. Dell EMC ECS Object Storage unlocks the potential of every business, powering critical use cases such as line-of-business applications, websites, mobile apps, IoT data stores, analytics initiatives, long-term archives, and much more. An enterprise-ready platform, ECS Object Storage empowers organizations to manage data at exabyte-scale, reduce security and compliance risks, and lower the total-cost-of-ownership, all at public cloud scale.

Long term data retention requirements continue to grow throughout all industries. Unstructured data, whether active or archive continues to accumulate at faster rates, and must be kept in readily accessible formats.



In order to keep data protection tools from getting overwhelmed by the enormous capacity requirements generated in today's data centers, technologies which enable data to be tiered from primary backup to secondary long term retention/archive are becoming more attractive.Dell EMC Cloud Tier technology integrates with an Dell EMC ECS Object Storage system (on premises or hosted private cloud) to provide a massively scalable architecture. By leveraging the capabilities of both of these platforms, IT administrators and architects can continue the path of consolidating critical backup processes, protecting complex environments mixed with unstructured data, database engines, virtual environments, while at the same time providing the ability to meet long term retention SLA's as required by the business. All of this capability is provided while not falling prey to the fallible nature of tape storage, or the risks of moving data offsite.

11 Hf
Hybrid / All Flash Systems

Hybrid / All Flash Systems Storage

All flash storage offers a number of advantages over other tape and disk storage technologies, in terms of lower total cost of ownership and greater storage density within a smaller footprint, which translates to reduction in costs for power, cooling, and floor space.

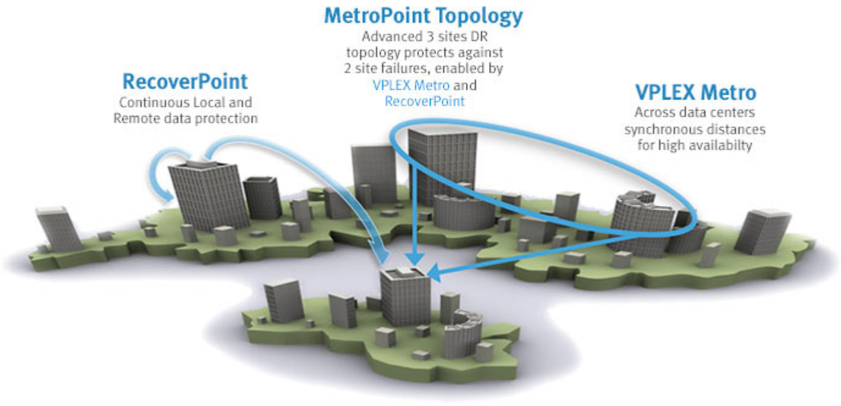
Dell EMC PowerProtect X400 appliance offers next generation data management, enabling faster IT transformation while assuring that you can easily guard and quickly unlock your data's value. PowerProtect X400, available in hybrid and all flash options, is a multi-dimensional, scaling out with linear performance and capacity increases while also delivering scale-up, grow-in-place capacity expansion.

12 Cdp Continuous Data Protection

Continuous Data Protection

Continuous data protection enables any point-in-time recovery for diversified storage environments both within and across data centers. This enhances operational recovery and disaster recovery for your mission-critical and business-critical applications and data. Should your data become compromised or lost, you'll be able to go back in time and recover that data in a consistent state.

Dell EMC RecoverPoint technology makes data loss reversible so you can be assured that your data is safe. It extends VMware Site Recovery Manager (SRM) functionality with any point-in-time recovery capabilities. Combining Dell EMC RecoverPoint and Dell EMC VPLEX MetroPoint topology enables data replication from an Dell EMC VPLEX Metro region of two data centers to a third site over distance and provides disaster recovery that can sustain two-site failures. It helps organization to achieve a new level of continuous availability, disaster recovery, and continuous data protection that can sustain multisite failures.


MetroPoint Topology
Advanced 3 sites DR topology protects against 2 site failures, enabled by VPLEX Metro and RecoverPoint
RecoverPoint
Continuous Local and Remote data protection
VPLEX Metro
Across data centers synchronous distances for high availabilty

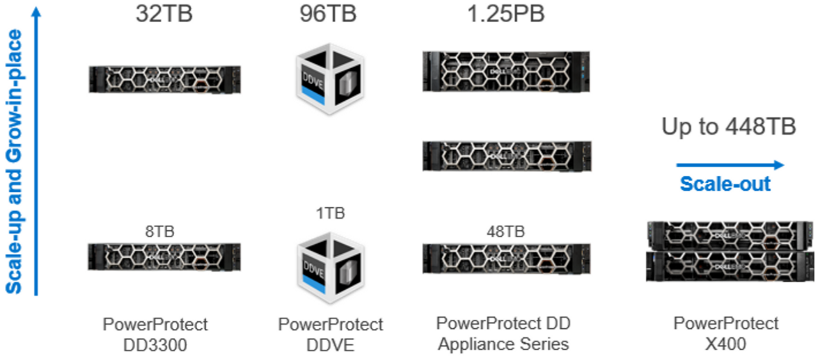
13 **Suo** Scale Up and Scale Out

Scale Up and Scale Out

Scalability is one of the check boxes for IT hardware specifications. You need a data management solution that gives you the flexibility to scale up and scale out in response to growing demands of your business.

The overall Dell EMC multi-dimensional data protection portfolio serves to meet future needs by flexibly deploying data protection storage via appliances or software-defined, on-premise or in-cloud. It maximizes agility by being able to either grow-in-place from 8TB to 32TB in a PowerProtect DD3300 appliance, or scale-up from 1TB to 96TB with PowerProtect DD Virtual Edition and maximize its capacity to 1.25PB with PowerProtect DD Series.

The portfolio also enables the customer to expand with the flexibility to scale out with the PowerProtect X Series Appliances. Dell EMC PowerProtect Appliances enable backup, recovery and replication, providing midsize and enterprise organizations with operational simplicity, agility, flexibility and IT governance controls.



14 Ha
High Availability

High Availability

Availability of business critical workloads is still a huge challenge to many organizations. Planned and unplanned downtime continues to cause undesirable disruption to operations with severe business impact.

Dell EMC PowerProtect DD system's high availability feature lets you configure two PowerProtect DD systems as an Active-Standby pair, providing redundancy in the event of a system failure. HA keeps the active and standby systems in sync, so that if the active node were to fail due to hardware or software issues, the standby node can take over services and continue where the failing node left off.

Dell EMC VPLEX maximizes the return on investments in all flash or hybrid storage arrays by providing continuous availability to business-critical workloads. VPLEX also creates a flexible storage architecture that gives IT teams the agility they need to respond to rapid business and technology changes while maximizing asset utilization across active-active data centers.

Dell EMC VPLEX's unique implementation of distributed cache coherency allows the exact same data to be read/write accessible across two storage systems at the same time. This in turn ensures uptime for business critical applications scenarios and enables seamless data mobility across arrays without host disruption. The storage systems can be in a single data center (VPLEX Local), or separated by distance (VPLEX Metro).

Here are some of the features that won the trust of IT organizations to deploy it successfully over thousands of data centers:

- Flash Optimized: Performance optimization for all-flash arrays, support for thin-provisioning space reclamation using UNMAP, XCOPY support on All-Flash.
- Scale-out: VPLEX scales up to four VPLEX engines in single cluster that can support multiple all-flash storage systems.
- Dedicated: VPLEX requires no compute resources from the application hosts or on the underlying array to maximize data availability.
- No single point of failure: All connectivity between VPLEX cluster nodes and across VPLEX Metro configuration is fully redundant, ensuring protection against single points of failure.
- Storage Monitoring and Reporting (M&R): Storage M&R for VPLEX is included with VPLEX systems, providing indepth views of all VPLEX components with long trends. It is easy to visualize the utilization, capacity, health and performance and to analyze the trends to optimize for best configuration.

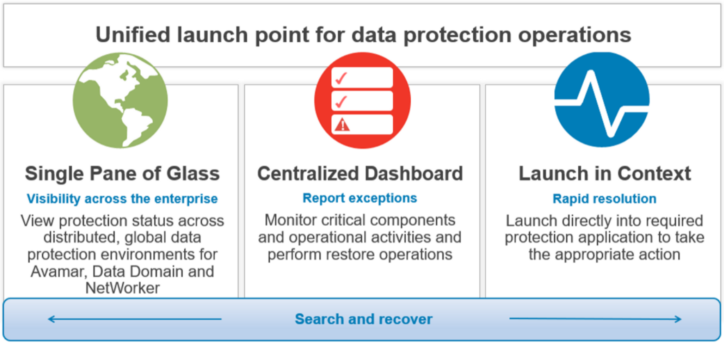
Operations

15 Cm
Centralized Management

Centralized Management

Governance and regulatory compliance require organizations to effectively manage, protect and recover their data whenever needed and wherever it resides. This means having visibility into your data protection operations across multiple systems and multiple sites.

Dell EMC Data Protection Central simplifies the management of data protection with visibility across distributed data protection software and protection storage, enabling customers the capability to quickly identify and resolve critical issues.



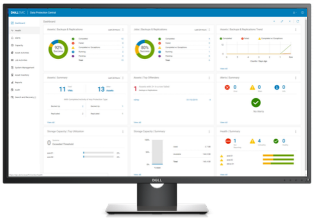
Unified launch point for data protection operations

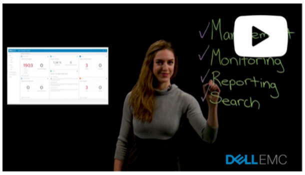
Single Pane of Glass
Visibility across the enterprise
View protection status across distributed, global data protection environments for Avamar, Data Domain and NetWorker

Centralized Dashboard
Report exceptions
Monitor critical components and operational activities and perform restore operations

Launch in Context
Rapid resolution
Launch directly into required protection application to take the appropriate action

Search and recover





16 Oa
Orchestration & Automation

Orchestration & Automation

Data is the heart of the modern enterprise. In order for businesses to innovate and scale, enterprises are finding the need to embrace applications being developed and executed in a variety of environments—on premises, traditional, cloud native, public cloud, service provider, Software-as-a-Service and other next gen platforms. With this data and application sprawl comes complexity. In order to safely unlock their data's full potential, enterprises will need to manage and protect that data wherever it is born, and as it flows across boundaries, from edge to data center to cloud.

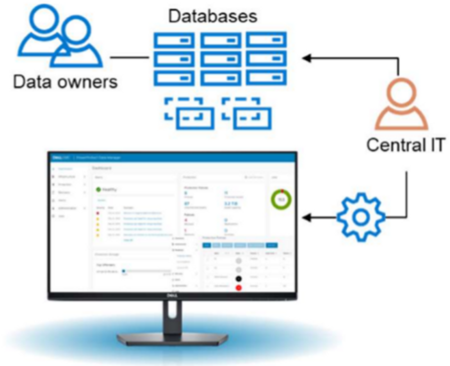
To solve the challenges of scale and complexity, we must eliminate manual tasks wherever possible and rely on software to run our systems. Complete IT transformation includes automated data protection with self-service capabilities. This means extending control to the VM administrator when it comes to backup and recovery operations, where VM policies will determine levels of data protection.

Dell EMC data protection solutions protect your VMs easily with tight integration with VMware in vCenter, vSphere, vRealize Automation data protection extension and extensible APIs, giving vAdmins control of the data protection of their applications and enable VMs provision with automated configurations. The factory-integrated data protection value includes lower operational costs, simplified management, increased productivity and decreased risk.

Dell EMC also offers Data Protection as-a-Service (DPaaS) which enables automation in the provisioning of protected applications, self-service capability for on-demand backup and restore, and enhanced governance through cloud management platform integration.

With operational simplicity, agility and flexibility at its core, Dell EMC PowerProtect Software enables you to protect, manage and recover data in on-premises, virtualized and cloud deployments. Self-service capabilities drive operational efficiency and IT governance controls ensure compliance, making even the strictest service level objectives easy to meet.

PowerProtect Software empowers data owners to perform self-service backup and recovery operations from their native applications, while at the same time providing IT with oversight and governance to ensure compliance.



PowerProtect Software provides

- IT automation services:
    - Centralized governance mitigates risk and assures compliance of SLAs and SLOs
    - Automated discovery and onboarding of databases, VMs and PowerProtect DD protection storage
- Self-service:
    - Self-service and centralized protection for MS SQL and Oracle residing on both physical and virtual machines
    - Enhanced user experience for backup and recovery for VMs, MS SQL and Oracle

17
Rt
Reporting Tools

Reporting Tools

Effectively managing your data protection environment is labor intensive and complex. It requires knowledge of backup applications, replication technologies, and the entire supporting infrastructure. Adding to the complexity, there are varying service-level objectives for backup and recovery, replication, and virtualization, as well as audit and compliance requirements to consider. And, with many IT organizations managing multiple data centers, combined with new hybrid computing models, data is often spread across a mix of private and public cloud resources, which increases the difficulty in managing data wherever it may reside.

With Dell EMC Data Protection Advisor, you can automate and centralize the collection and analysis of all of this data—and get a single, comprehensive view of your data protection environment and activities. With automated monitoring, analysis, and reporting across your backup and recovery infrastructure, replication technologies, storage platforms, enterprise applications and virtual environment, you will be able to more effectively manage service levels while reducing costs and complexity.

- Reduce Costs: Proactive monitoring and alerting of issues before impact
- Lower Complexity: Real-time protection assurance, scalability and resource optimization
- Increase Visibility and Insight: Provide the right information to the right people at the right time in the right format
- Automate Everything: Policy-based protection reduces risk and increases operational effectiveness
- Comply with Audits: Single click verification of service levels and recoverability

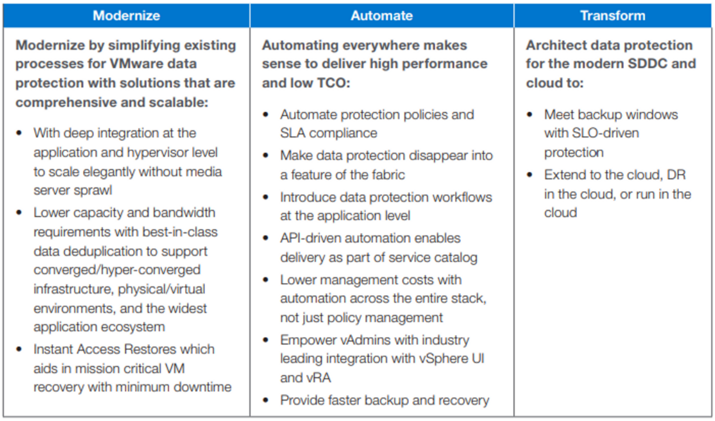
18 Sla
Service Level Agreement

Service Level Agreement

The shift towards modern data center has resulted in an increasingly converged and software-driven environment that empowers IT and organizational transformation.

Many of today's data protection solutions are limited by their inability to provide holistic data protection, which forces trade-offs between key requirements. Bottom line, common data protection architectures such as the traditional hardware and software model and initial approaches to converged hardware and software don't work well for larger VMware environments and are not designed to support the Software Defined Data Center (SDDC).

Constructed for today with tomorrow in mind, Dell EMC data protection is architected from the ground up to increase speed and agility for every business. By automating data protection, it offers IT, executive staff, and lines of business a competitive advantage, namely more time to be productive. Dell EMC Data Protection solutions deliver IT and storage admins the tools they need to manage uptime and increase service level agreements (SLAs), improve application performance, and lower the total cost of ownership of primary storage infrastructure and application data protection.



Modernize	Automate	Transform
Modernize by simplifying existing processes for VMware data protection with solutions that are comprehensive and scalable: • With deep integration at the application and hypervisor level to scale elegantly without media server sprawl • Lower capacity and bandwidth requirements with best-in-class data deduplication to support converged/hyper-converged infrastructure, physical/virtual environments, and the widest application ecosystem • Instant Access Restores which aids in mission critical VM recovery with minimum downtime	**Automating everywhere makes sense to deliver high performance and low TCO:** • Automate protection policies and SLA compliance • Make data protection disappear into a feature of the fabric • Introduce data protection workflows at the application level • API-driven automation enables delivery as part of service catalog • Lower management costs with automation across the entire stack, not just policy management • Empower vAdmins with industry leading integration with vSphere UI and vRA • Provide faster backup and recovery	**Architect data protection for the modern SDDC and cloud to:** • Meet backup windows with SLO-driven protection • Extend to the cloud, DR in the cloud, or run in the cloud

19
As
As-a-Service

As-a-Service

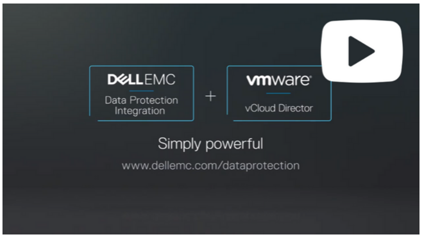
Driven by a strong customer demand, and an explosive increase in cloud workloads, Dell EMC is well-poised for the growth of cloud-ready data protection and recovery needs of customers. Data Protection as-a-Service (DPaaS) is a core requirement customers have when selecting a cloud service provider. However, until now, there have been no native solutions to address this need with existing solutions requiring a separate tenant portal or additional user interfaces, making the process more complicated for both cloud service providers and, most importantly, their customers.

VMware and Dell EMC have partnered to deliver tenant self-service DPaaS leveraging VMware's vCloud Director (vCD) platform. vCloud Director Data Protection is available directly within the vCD tenant portal UI, eliminating the need for tenants to access a separate user interface specific to Data Protection. For tenants or cloud providers interested in orchestrating via APIs, all Data Protection capabilities are also integrated directly into vCloud Director's REST API, via extensions.

Dell EMC Data Protection with vCloud Director delivers these advantages:

- Seamless user experience: Dell EMC provides data protection fully integrated into VMware vCloud Director without the need of a separate tenant portal, which often requires service user accounts to be created within the vCloud environment.
- Superior scale & performance: A scale-out architecture combined with Dell EMC Avamar's quick and efficient backups provides assurance that backups will complete within the scheduled window

- Costs up to 80% less to protect: Dell EMC's industry-leading de-duplication with a 55:1 deduplication rate greatly reduces protection storage requirements and minimizes operating costs
- Flexible Backup as-a-Service (BaaS): Flexible backup options enable backups to be run automatically through policies and/or on-demand. Self-service restores can be executed by tenants at the vApp-level, the VM-level, and even the individual file level.



Security

20
Ep
Endpoint Security

Endpoint Security

With the growing number of desktop and laptop users and the necessity of employees working outside of corporate offices, IT administrators are faced with the daunting task of ensuing that valuable data in all desktop and laptop systems are protected against data loss from disk corruption and failures, theft and human errors. IT investment costs, user productivity, data security and policy compliance are top concerns that IT administrators grabble with, when considering an effective desktop and laptop backup strategy.

Dell EMC Avamar backup software and Dell EMC PowerProtect DD effectively protects up to thousands of laptops and desktops across the enterprise. Unlike traditional backup methods, Avamar deduplicates data at the client and globally, delivering fast, daily and full backups over existing networks while dramatically reducing the amount of required backend disk storage. Avamar also enables data to be quickly recovered in just one step, and data can be encrypted in-flight and at rest for security.

21
Er
Encryption At Rest

Encryption At Rest

The proliferation of publicized data loss, coupled with new governance and compliance regulations, is driving the need for customers to encrypt their data at rest.

Dell EMC PowerProtect DD encryption software provides a way for organizations to enhance the security of of data that resides on their PowerProtect DD appliance using industry-standard encryption algorithms.

Encrypting data at rest protects user data against theft of the PowerProtect DD system, loss of the physical storage media during transit, and eliminates accidental exposure during the replacement of failed drives.

PowerProtect DD encryption seamlessly integrates with the high-speed, inline deduplication process used in PowerProtect DD appliances, and encrypts data before iit is written to disk. Similar to the advantages of inline deduplication, inline encryption requires minimal resources to provide fast, reliable and secure backup and recovery.

Unlike other encryption solutions that require additional hardware resources or processing power, PowerProtect DD encryption requires no additional hardware and has only moderate impact on performance. By leveraging the PowerProtect DD SISL scaling architecture, duplicate segments require no encryption processing. This optimization results in much lower resource consumption by the encryption process, thereby lessening the impact on overall performance. This also eliminates additional servers or appliances for encryption in the infrastructure.

22 Rc
Retention & Compliance

Retention & Compliance

Enterprises continue to see an exponential growth in the structured and unstructured data that is proliferating across their primary storage systems. Customers realize that the majority of this data is seldom accessed; yet they cannot delete this data given the compliance retention requirements for business records. As organizations drive formal adoption of archiving, IT administrators need cost-effective ways for their fast-growing archive storage needs, including compliance retention.

Dell EMC PowerProtect DD Retention Lock software provides immutable file locking and secure data retention capabilities for customers to meet both corporate governance and regulatory compliance standards such as SEC 17a-4(f).

PowerProtect DD Retention Lock enables IT administrators to apply retention policies at an individual file level and consolidate backup and archive data in accordance with governance and regulatory compliance standards.

23 Km
Key Management

Key Management

Basic key management functions combine simplicity with ease of use to provide data security at the appropriate level. PowerProtect DD appliance has one encryption key for all data on the system thereby making key management simpler. For reliability and security, the encryption key is also protected and stored encrypted. The PowerProtect DD Data Invulnerability Architecture with RAID 6 data protection safeguards the reliability and recoverability of the data and assures recoverability of the encryption key. Checksums and continuous end-to-end data integrity verification provide additional safeguards.

24 Oc
Offsite Copy

Offsite Copy

Increasing frequency of catastrophic events like hurricanes, floods and fire, have raised the urgency to have disaster recovery (DR) procedures. One of the most crucial steps for DR is to have a copy of the data at a remote site and/or in the cloud. To improve reliability of disaster recovery and meet stringent recovery time objectives (RTO) imposed by the business, organizations are increasingly replicating backups to create this offsite copy of their critical data.

Historically, backup tapes have been the primary method used to transport data to the DR site. However, in today's age of rapid data growth, handling and tracking tapes introduces a significant management cost and complexity. Furthermore, lost and misplaced tapes have forced IT to consider other approaches for disaster recovery.

Dell EMC DD Replicator software provides automated, policy-based, network-efficient and encrypted replication for disaster recovery and multi-site backup and archive consolidation. DD Replicator software asynchronously replicates only compressed, deduplicated data over the WAN. Cross-site deduplication further reduces bandwidth requirements when multiple sites are replicating to the same destination system. This improves network efficiency across all sites and reduces daily network bandwidth requirements up to 98%[7], making network-based replication fast, reliable and cost-effective. In order to meet a broad set of DR requirements, DD Replicator provides flexible replication topologies, such as full system mirroring, bi-directional, many-to- one, one-to-many, and cascaded. In addition, customers can choose to replicate either all or a subset of the data on the Data Domain system.

- Consolidates backup and archive data from hundreds of remote sites
- Efficient backup consolidation and on-prem disaster recovery
- Reduces bandwidth requirements up to 98%[7] -- low bandwidth throlling
- Protects sensitive data when replicating over untrusted networks
- Flexible replication topologies to meet broad DR requirements

[7] Source: The Economic Value of the Dell EMC Data Protection Portfolio, ESG, March 2019

Another DR solution gaining popularity is having a DR site in the cloud. Dell EMC Cloud Disaster Recovery (CDR) allows enterprises to copy backed-up VMs from their on-prem environments to the public cloud (AWS and Azure) for the orchestration and automation of DR testing, DR fail-over and failback of Tier 2 workloads to/from the cloud in a disaster scenario.

Extension of the existing data protection from the customers' premises to the cloud provides a familiar user experience, thus requiring minimal education and training. Additional benefits of the CDR include minimal cloud footprint in the cloud (no additional compute is required until a failover occurs, and minimal compute is required in case of test or recovery), and orchestrated test, recovery and failback of workloads.

Key features:

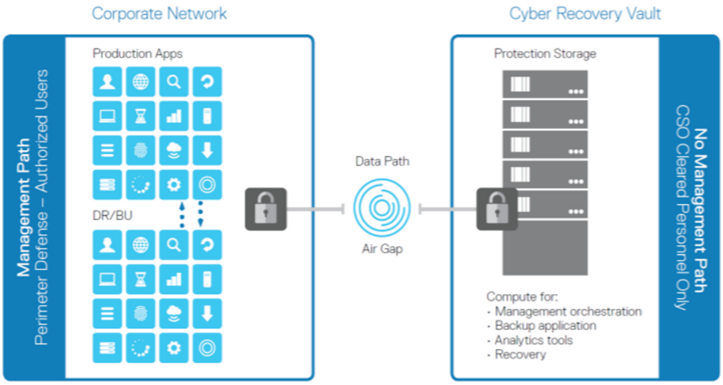
- Secure, simple & economic disaster recovery
- Protect directly from on-prem to AWS and Azure
- Complete orchestration for test, failover and failback

25 Irv
Isolated Recovery Vault

Isolated Recovery Vault

Across industries and among organizations of every size, cyber attacks are on the rise. Until recently, organizations have focused on trying to prevent cyber attacks, which come primarily from hacking and malware. However, the likelihood that all malware will be discovered before harm is done is slim, particularly for slow-moving and sophisticated attacks such as ransomware. The difficulty of detecting malware early gives hackers time to orchestrate attacks ranging from extortion to outright destruction of mission-critical systems. Such cyber attacks cripple an organization, leading to revenue loss and reputation damage.

Besides threat detection and remediation, organizations need to further develop and coordinate their incident response and associated data recovery strategies.



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

PowerProtect Cyber Recovery enables robust business resiliency through automated data isolation, analytics, and recovery:

- Planning and Design: Optional Dell EMC Advisory Services determine which business critical systems to protect and creates dependency maps for associated applications and services, as well as the infrastructure needed to recover them. The service also generates recovery requirements and design alternatives, and it identifies the technologies to analyze, host and protect your data, along with a business case and implementation timeline.

- Cyber Recovery Vault (CR Vault): The centerpiece of PowerProtect Cyber Recovery is the CR Vault, an isolated and protected part of the data center. The CR Vault hosts your critical data on Dell EMC technology used for recovery and security analytics. The goal of the CR Vault is to move data away from the attack surface, so that in the event of a malicious cyber-attack you can quickly resort to a good clean copy of data to recover your critical business systems. Using vault protections around the isolated data also protects it from insider attacks. PowerProtect Cyber Recovery automates the synchronization of data between production systems and the CR Vault and creates immutable data copies.

- Security Analytics: PowerProtect Cyber Recovery's automated workflow includes the ability to create sandbox copies that you can use for security analytics. Analytics can automatically be performed on a scheduled basis using integration provided through native REST APIs. PowerProtect Cyber Recovery applies over 40 heuristics to determine indicators of compromise and alert the user.

The rapidly changing threat landscape demands an adaptive analytics framework; so PowerProtect Cyber Recovery stays ahead of the bad actor by enabling tools incorporating Artificial Intelligence (AI) and Machine Learning (ML) analytics methods to the CR Vault.

- Recovery and Remediation: PowerProtect Cyber Recovery allows customers to leverage dynamic restore / recovery procedures using existing Disaster Recovery procedures that bring business critical systems back online. Dell EMC and its Ecosystem partners provide a comprehensive methodology for protecting data, as well as performing damage assessments and forensics to either recover your systems or remediate and remove the offending malware.

DELL EMC
ISOLATED RECOVERY ADVISORY SERVICE
ASSESS YOUR SYSTEM
ADVISE YOU ON AIR GAPPED VAULT
BUSINESS CASE -ESTIMATED COSTS
IMPLEMENT AIR GAP

Cloud

26 Scm
Single Centralized Management

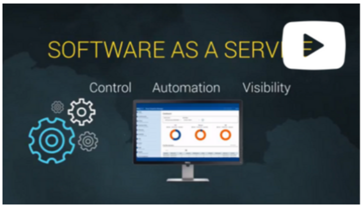
Single Centralized Management

Organizations find it difficult to manage workloads and the proliferation of snapshots with the native tools offered by most infrastructure as a service (IaaS) cloud providers. What's required is an automated, enterprise-grade solution for protecting workloads and instances running in the public cloud.

Dell EMC Cloud Snapshot Manager (CSM) is a SaaS solution making it easy for customers to protect workloads in public cloud environments (AWS, Azure) – without requiring installation or infrastructure. Customers can discover, orchestrate and automate the protection of workloads across multiple clouds based on policies for seamless backup and disaster recovery. Dell EMC breaks cloud silos and enables customers to use one tool for the protection of workloads, regardless of which public cloud they reside in.

CSM provides the following benefits to customers:

- Automated cloud protection from one pane of glass, breaking cloud silos
- Protection, compliance, and disaster recovery of public cloud workloads
- Multi-tenancy capabilities enabling multiple accounts and users
- Automatic deletion of snapshots per retention policies for cost savings
- Auto scaling, audit logs, and reports for business growth
- Application consistent framework in AWS and Azure for consistent restores
- Email reports for visibility into the health and overall status of your CSM environment
- Discovery of existing snapshots in AWS for better control over snapshot sprawl

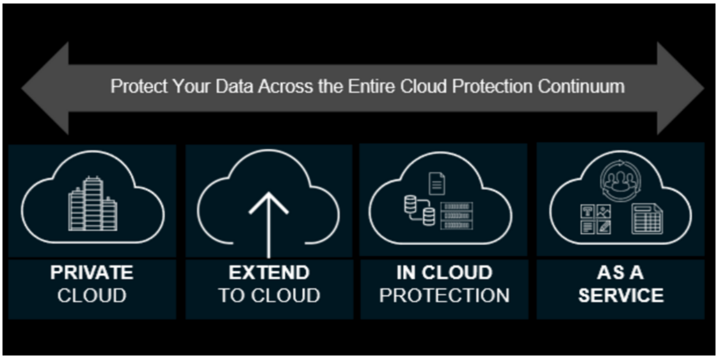


27
Mc
Multi-cloud Protection

Multi-cloud Protection

You need to manage workloads across files, applications, databases, hypervisors and multiple clouds. All need to meet GDPR requirements, compliance, security and data backup requirements. To effectively manage data in the cloud and on-premises, Dell EMC has you covered no matter where your data Iresides.

Cloud protection solutions from Dell EMC help customers transform their data centers to enable greater operational efficiency, resiliency and scalability throughout the entire cloud journey. No one offers a more complete portfolio of hardware, software, solutions, and services for protecting our customers' data as they embark upon their digital transformations to the cloud.



Protect Your Data Across the Entire Cloud Protection Continuum

PRIVATE CLOUD

EXTEND TO CLOUD

IN CLOUD PROTECTION

AS A SERVICE

28
Ltr
Long Term Retention

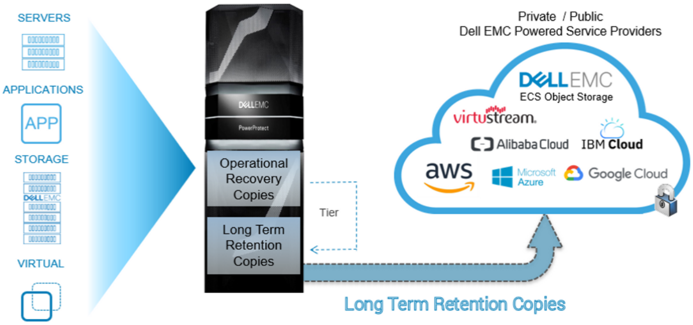
Long Term Retention

With the advent of cost-effective disk-based backup with deduplication technology and teh means for mult-site replication at near-zero recovery point objective (RPO) and near instantaneous recovery time objective (RTO), a compelling use case exists to store data with longer life-cycles on disk.

Dell EMC Cloud Tier provides best of breed technology that will allow businesses to gain the advantages of cloud while lowering overall TCO. With Cloud Tier, data is natively tiered to the public, private or hybrid cloud for long-term retention. Only unique data is sent directly to the cloud and data lands on the cloud object storage already deduplicated.

Dell EMC's advanced deduplication, storage footprint is greatly reduced for cost-effective long-term retention in the cloud. A broad ecosystem of backup and enterprise applications and a variety of public and private clouds are supported with Cloud Tier including Dell EMC Elastic Cloud Storage, Amazon Web Services, Microsoft Azure, IBM Cloud, Google Cloud Platform and Alibaba Cloud.

- Cost-effective, modern long-term retention
- Effective and efficient management of capacity across on-prem and cloud that optimizes the amount and reduces the overall cost of cloud storage
- Simple, native cloud tiering with no external appliance or cloud gateway required
- Efficient data transfer to and from the cloud with less bandwidth due to industry-leading source side deduplication technology.
- Broad support across backup applications and cloud providers
- Seamless management with supported applications



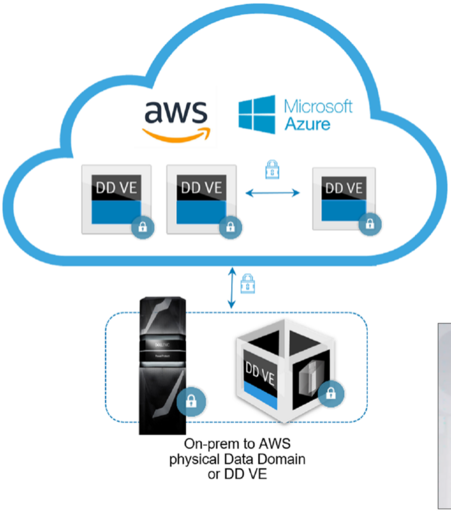
29
Icp
In-cloud Protection

In-cloud Protection

As more and more applications are built as cloud native applications, traditional data protection methods to protect the "born-in-the-cloud" applications are no longer manageable and scalable. While your infrastructure and services shifts to the public cloud, the responsibility to secure and protect all data assets remains that of the customer and not the cloud service provider.

Dell EMC offers optimized client direct backup to object storage for "born-in-the-cloud" applications that spans across on-premise, direct-to-cloud and within the cloud, bringing high backup performance, scalability and low cost cloud storage.

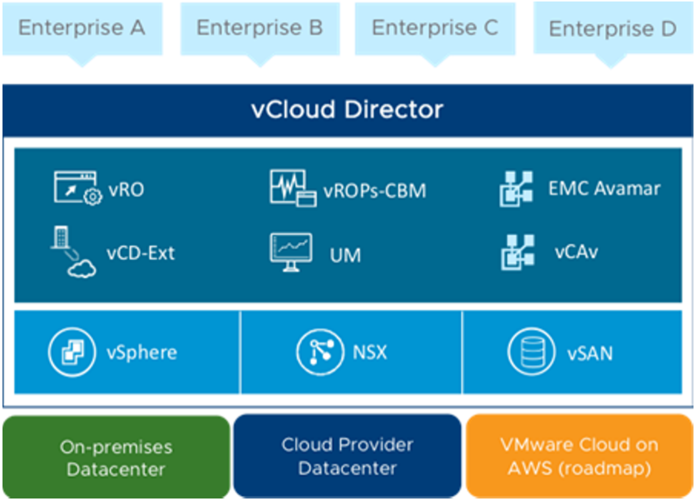
Dell EMC PowerProtect DD Virtual Edition runs in Amazon Web Services and Microsoft Azure and provides replication between cloud and on-premise, and within the cloud with encryption (at rest and over the wire) and bandwidth efficiency.



30 Cpa Cloud Protection Automation

Cloud Protection Automation

Dell EMC provides VMware certified data protection for VMware Cloud on AWS with our Data Protection software that provides enterprise-grade data protection, best-in-class deduplication, and an integrated management tool for on premise and cloud workloads. We also provide Cloud Disaster Recovery to VMware Cloud on AWS, enabling you to copy backed up data to AWS S3 object storage and, in case of a disaster event, spin off VMs on demand in your own VMware Cloud on AWS environment. Use vMotion to simply transfer the VMs back to your on premise VMware environment when ready.



Tightly integrated with VMware vCloud Director, VMware administrators benefit from Dell EMC's data protection automation capabilities:

- Enables service providers to convert physical data centers into highly elastic virtual data centers (VDCs).

- Converts physical resources (network, storage and compute) into VDC resources, which service providers make available as catalog-based services to users through a web portal
- Policy controls apply pre-determined limits on users to regulate consumption of resources and restrict access

31 Cdr
Cloud Disaster Recovery

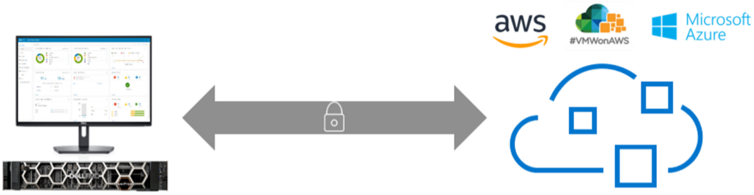
Cloud Disaster Recovery

For organizations looking to leverage the cloud as a disaster recovery option, Dell EMC views the Cloud as a deployment choice that can be fundamental and vital as customers embark upon their IT, Digital, Workforce, and Security Transformation initiatives. Whether your data and applications reside on-premises or moving into the public cloud, Dell EMC enables cloud protection across the entire protection portfolio while creating a new class of data protection cloud solutions and services – including backup to the cloud, backup in the cloud, long-term retention to cloud and DR to the cloud.

Cloud Disaster Recovery (Cloud DR) allows enterprises to copy backed-up VMs from their on-premises Dell EMC PowerProtect DD appliance or Dell EMC Integrated Data Protection Appliance (IDPA) and Avamar environments to the public cloud (Amazon Web Services, Microsoft Azure) and to orchestrate DR testing, failover and failback of cloud workloads in a disaster scenario. Extension of the existing data protection from the customers' premises to the cloud provides a familiar user experience, thus requiring minimal education and training. Additional benefits of Cloud DR include minimal cloud footprint during routine operation and orchestrated recovery.

Ob Object Storage
Cs onverge System
Nd ative Di Backup
Sw Softwar Definec
Sd Source duplicat
Or Oracle
Mf lainfrai
Aws nazon V Service
Dm Data Migratic Service
4 Ar AI / M
3 Ar Analy
2 Sl Sear
Ca Apach assan

- Secure, Simple & Economical Disaster Recovery
- Protect directly from Data Domain on-prem to AWS, Azure
- Complete orchestration for test, failover and failback



Orchestrated DR

- End-to-end orchestration
- DR plans
- Rapid recovery

Efficient Architecture

- Extend on-premises data protection
- Minimal cloud cost & footprint
- Eliminate DR data center costs

Simple operation

- Use familiar on-prem UI
- Direct in-cloud access
- 3 clicks failover, 2 clicks failback

Data Management

32
Sh
Search

Search

IT infrastructure is no long about data center management --- it's about delivery value and services to meet business demands. Businesses can only unlock their Data Capital if data can be leveraged and monetized whenever it's required. Being able to discover, locate and analyze data efficiently gives businesses a competitive edge over others. Likewise, data needs to be protected and be recovered efficiently wherever it resides.

Dell EMC Data Protection Search is a scalable index and search appliance that integrates with Dell EMC Avamar and Dell EMC NetWorker. Through scheduled collection activities, backup content of one or more Avamar or NetWorker servers is gathered, indexed, and stored within the Data Protection Search node. This allows users to perform searches across the backup environment from which the user can then preview, download, or restore the backup content.

The Data Protection Search index capability allows the following:

- Process content from multiple input sources
- Index only metadata or full content
- Leverage scalable, fault tolerant open source indexing technology

Data Protection Search allows the following:

- Search using an easy to use interface
- Perform advanced and powerful searches
- Perform cross-server, cross-platform searches
- Preview backup file content without downloading
- Download backup files locally
- Restore backups to original or alternate locations
- Apply visual filters to search results

33
An
Analytics

Analytics

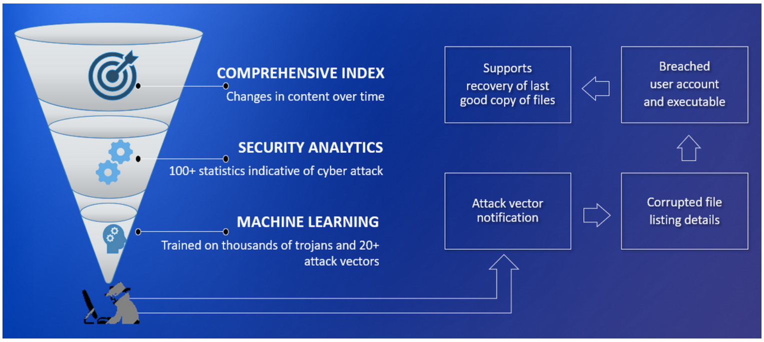
Effectively managing your data protection environment is labor intensive and complex. It requires knowledge of backup applications, replication technologies, and the entire supporting infrastructure. Adding to the complexity, there are varying service-level objectives for backup and recovery, replication, and virtualization, as well as audit and compliance requirements to consider. And, with many IT organizations managing multiple data centers, combined with new hybrid computing models, data is often spread across a mix of private and public cloud resources, which increases the difficulty in managing data wherever it may reside.

With Dell EMC Data Protection Advisor, you can automate and centralize the collection and analysis of all of this data—and get a single, comprehensive view of your data protection environment and activities. With automated monitoring and reporting across your backup and recovery infrastructure, replication technologies, storage platforms, enterprise applications and virtual environment, you will be able to more effectively manage service levels while reducing costs and complexity.

34
Am
AI / ML

AI / ML

Dell EMC PowerProtect Cyber Recovery’s automated workflow includes the ability to create sandbox copies that you can use for security analytics. Analytics can automatically be performed on a scheduled basis using integration provided through native REST APIs. PowerProtect Cyber Recovery applies over 40 heuristics to determine indicators of compromise and alert the user. The rapidly changing threat landscape demands an adaptive analytics framework; so PowerProtect Cyber Recovery stays ahead of the bad actor by enabling tools incorporating Artificial Intelligence (AI) and Machine Learning (ML) analytics methods to the CR Vault.



COMPREHENSIVE INDEX
Changes in content over time

SECURITY ANALYTICS
100+ statistics indicative of cyber attack

MACHINE LEARNING
Trained on thousands of trojans and 20+ attack vectors

Supports recovery of last good copy of files

Breached user account and executable

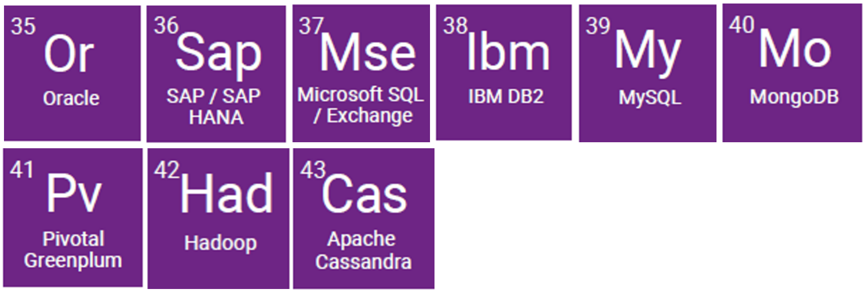
Attack vector notification

Corrupted file listing details

The analysis of 100+ statistics using trained machine learning algorithms analyzes how data changes in the following areas:

- Entrophy
- Similarity
- Deletions
- Creations
- File Corruption
- File Type Mismatch
- Ransomware Extensions
- And more...

Native Direct Data Protection for Enterprise and Next Gen Applications Workloads


35 Or Oracle
36 Sap SAP / SAP HANA
37 Mse Microsoft SQL / Exchange
38 Ibm IBM DB2
39 My MySQL
40 Mo MongoDB
41 Pv Pivotal Greenplum
42 Had Hadoop
43 Cas Apache Cassandra

Your company's operational databases aren't just important: They're critical. Pair that criticality with exponential growth, and meeting your businesses strict protection SLOs becomes challenging. Allowing database admins (DBAs) to do their own backups, which is the growing trend, saves time – but ensuring those backups are in compliance isn't easy.

Dell EMC Data Protection Suite delivers a high performance, self-service data protection solution for mission-critical databases that ensures SLO compliance through IT governance and automation.

Dell EMC PowerProtect DD Boost software provides advanced integration between leading backup and enterprise applications, and Dell EMC PowerProtect DD appliances and Dell EMC Integrated Data Protection Appliances. With PowerProtect DD Boost, parts of the deduplication process are distributed to the backup server or application server, enabling client-side deduplication so only unique data segments are sent to the PowerProtect DD appliance. This enables 50% faster backups and reduces network bandwidth requirements by up to 98%[8]. PowerProtect DD Boost provides advanced load balancing and failover, which further improves throughput and resiliency.

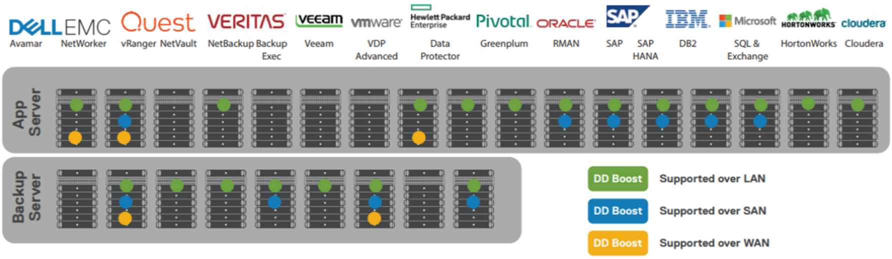
[8] Source: The Economic Value of the Dell EMC Data Protection Portfolio, ESG, March 2019

In addition, PowerProtect DD appliances can grant secure access to multiple PowerProtect DD Boost users per system for data protection-as-a-service in private and public cloud deployments. Providing PowerProtect DD Boost users secure access to their data lays the foundation for logical data isolation enabling secure multi-tenancy on a PowerProtect DD appliance in PowerProtect DD Boost environments.

PowerProtect DD Boost also enables backup administrators to control replication between PowerProtect DD appliances providing administrators a single point of management for all backup copies. This also provides more flexible retention management by enabling backup administrators to set retention periods for each backup copy individually.

Database and next gen applications supported include Oracle, SAP/SAP HAHA, Microsoft SQL, Microsoft Exchange, IBM DB2, MySQL, MongoDB, Pivotal Greenplum, Hadoop and Apache Cassandra.

For applications not currently supported with DD Boost, Dell EMC offers DD Boost file system plug-in known as BoostFS. BoostFS is cost-effective and simple, and provides everything you would expect out of DD Boost. BoostFS is supported for any application that supports NFS.



🟩 DD Boost Supported over LAN

🟦 DD Boost Supported over SAN

🟨 DD Boost Supported over WAN

For everything else , use the DD Boost file system plug -in

Systems and Platforms Supported

44
Mf
Mainframe

Mainframe

Dell EMC has been a provider of mainframe storage for nearly 30 years and continues to innovate across primary disk storage (DASD), data protection storage (DLm virtual tape), connectivity (Connectix) and automated failover for critical events and testing (GDDR for both disk and tape). Dell EMC makes DASD and tape more affordable while providing the ultimate in data protection through innovations like Universal Data Consistency, deduplication, zDP data protection and enhanced IBM compatibility features.

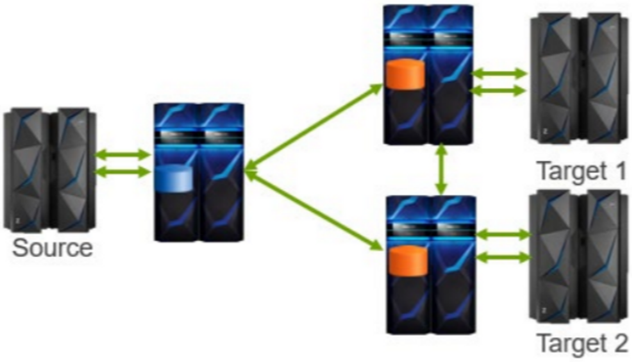
Dell EMC Disk Library for mainframe (DLm) makes synchronous tape and cloud a mainframe reality, enabling organizations to:

- Consolidate data
- Eliminate costly storage silos
- Modernize storage infrastructure to support digital transformation

DLm offers IBM z Systems and Unisys Dorado / Clearpath mainframe customers the ability to replace their physical tape systems, including traditional virtual tape servers such as the IBM TS7700 family and Oracle/STK VSM, with a dynamic virtual tape solution, eliminating the challenges tied to traditional tape-based processing.

DLm offers IP-based remote replication for DLm employing both primary and deduplication storage, which uses the customer’s IP network infrastructure and eliminates the need for channel extension equipment. The replication is storage-based and therefore has no impact on mainframe host operations or performance.

Customers can define the Recovery Point Objective (RPO) in minutes or hours and DLm will perform the replication to meet the defined RPO. Customers can also define different RPOs for different VOLSER ranges based on information criticality, which allows them to better tune their system and not overload the network. For example, critical information may have a low RPO (minutes), whereas less critical information can have a higher RPO (hours). DLm replication also enables the customer to define quality of service (QoS), which optimizes the network traffic to prevent network overload during peak hours.



DLm Remote Replication

45 Ii IBM-i

IBM-i

Thousands of companies around the world have deployed IBM i operating environments for managing their high transaction business applications. These deployments can be found in most verticals including banking, financial services, retail, insurance, automotive and transportation. Given the business-critical nature of their IBM i data and restricted IT budgets, companies are looking to improve backup and recovery and eliminate security risks associated with traditional data protection strategies -- while managing costs.

IBM i users can now leverage these operational and cost benefits with the Dell EMC PowerProtect DD Virtual Tape Library software option for IBM i.

Integrating a PowerProtect DD appliance with PowerProtect DD VTL for IBM i requires no changes to the existing IBM i operating environment. The IBM i server simply connects to the PowerProtect DD appliance over the fibre channel SAN infrastructure and the server treats the PowerProtect DD appliance as a physical tape library. The IBM Backup Recovery and Media Services (BRMS) application can then create backup policies to protect IBM i business application data with the PowerProtect DD appliance. There are no additional software components to install on the IBM i server, and all data movement between the server and the PowerProtect DD appliance is managed by BRMS or native IBM i operating system commands. Up to 540 virtual tape drives can be easily configured to maximize performance throughput. This allows for seamless integration and deployment of the PowerProtect DD appliance into an existing IBM i environment.

46 Os Open Systems

Open Systems

Dell EMC supports next-generation backup, recovery and archive solutions with its Dell EMC Disk Library, an open systems virtual tape library, which supports RAID 6 protection for improved availability and 1 TB disk drives that provide 30% more capacity and improve the overall economics of online backup by further lowering the cost per gigabyte of storage.

47
Vm
VMware

VMware

Today, most workloads run on VMware virtual machines (VMs). Protecting these environments can get complicated as the amount of data, applications, and VMs continues to increase. The movement of both data centers and the data protection environment as users adopt cloud technologies further complicates matters as organizations deal with siloed data, as well as multiple solutions and vendors.

Dell EMC and VMware offer solutions for customers with the deepest integration points to accelerate IT transformation and enable data protection for VMware environments that are easy, secure and cost-effective. Dell EMC portfolio of data protection products provides the enterprise-class user experience for VMware users with automation and orchestration across the entire VMware stack.

VMware Data Protection for Larger Enterprises:

- Dell EMC Data Protection solutions, which are architected for the modern and SDDC, delivers scalability and faster performance, ensuring that your entire VMware environment is protected and can scale easily as the amount of data you need to protect inevitably continues to increase.
- Dell EMC Data Protection solutions, including PowerProtect DD appliance, PowerProtect DD Virtual Edition and Integrated Data Protection Appliance, automate the data movement from proxies to protection storage -- providing and enabling VM backup policy management, deploying and configuring virtual data movers/proxies, and directing data from VMs to backup storage.

Dell EMC Integrated Data Protection Appliance (IDPA) DP4400:

- IDPA DP4400 is designed for mid-size organizations. It is a converged platform that combines compute, storage, and network together with backup and replication software to create a complete backup and recovery solution.
- The DP4400 is easy to deploy, can scale from 8TB to 96 TB with no additional hardware purchase, and is multi-cloud ready for long-term retention and cloud disaster recovery.
- It is optimized for VMware, protecting up to 5x more VMs in a single 2U appliance[9].

VMware Data Protection in the Cloud:

- Dell EMC Data Protection solutions support native backup tiering to public or private clouds for cost-effective storage of long term backup retention data, eliminating the need for physical tape infrastructure.
- For customers looking to extend their data protection to the cloud, we provide support for most cloud providers (AWS, Azure, Google, Alibaba, etc).

Disaster Recovery to VMware Cloud:

- For customers looking to protect VMware Cloud on AWS, Dell EMC was the first data protection provider for VMware Cloud workloads on AWS, providing fast, efficient, and secure image and guest level backup and recovery.
- Compressed data is still copied to AWS S3 for minimal cost and footprint. If a disaster event occurs, VMs are spun off on demand either in your own VMware Cloud on AWS. You can simply transfer the VMs back to your on-premises VMware environment using vMotion for even simpler management and orchestration.
- Tight integration into VMware enables self-service protection within native VMware interfaces.

[9] Based on Dell internal testing and comparing against nearest competitor's published performance data in 2U, February 2018.

VMware Integrated Data Protection as a Service:

- VMware vCloud Director and Dell EMC Data Protection Software have greatly enhanced their integration, making it easier for service providers to jointly deliver VMware and Data Protection-as-a-Service.
- Our leading VMware integration extends data protection into the vCloud Director tenant UI. Dell EMC eliminates the need for a separate backup-as-a-service portal. Service providers and their customers benefit from Dell EMC Data Protection solutions which provide low operating costs and high scalability and performance.

48 Mhv Microsoft Hyper-V

Microsoft Hyper-V

As Microsoft environments scale, ensuring fast, reliable recovery becomes even more critical—but it will be harder to achieve due to the amount of data that will need to be backed up if traditional backup methods continue to be used.

Dell EMC solutions for Microsoft backup provide automated, efficient, online protection and granular recovery on Microsoft Azure, Hyper-V, Exchange, SQL Server, and SharePoint environments.

Dell EMC solutions are completely integrated with Microsoft applications through Microsoft Volume Shadow Copy Service (VSS), Database Availability Groups (DAGs), AlwaysOn Availability Groups, Active Directory, SQL Server VSS Writer, and more.

49
Kvm
OpenStack
KVM

OpenStack KVM

OpenStack KVM is gaining popularity due to its vendor-agnostic cloud framework. Organizations need an enterprise-class data protection solution for OpenStack environments.

Dell EMC Avamar Virtual Edition (AVE) is a single-node non-RAIN (Redundant Array of Independent Nodes) Avamar server that runs as a virtual machine in an OpenStack cloud environment. AVE integrates the latest version of Avamar software with SUSE Linux as an OpenStack instance.

The Dell EMC OpenStack Data Protection Extension (Dell EMC OpenStack DPE) allows backup administrators to manage backup and restore operations for projects in an OpenStack cloud infrastructure. The backup administrator role is performed by an OpenStack administrator who has access rights to projects and associated instances that need to be backed up or restored. The backup administrator can manage the protection provider (currently an Avamar server), all projects that will be protected by the protection providers, and configure backup policies for scheduling backups of a particular project.

The backup administrator also manages the backup proxies that are deployed in the OpenStack cloud and are used to perform backup and restore operations. The Dell EMC OpenStack DPE provides project administrators the ability to manage instances they want to be protected, and browse the backup inventory of a protected instance. The project administrator can then select a backup and restore it to replace the original instance, or restore it to a new location. Progress of the backup or restore operation can be monitored.

50 Co Containers

Containers

The adoption of Docker container keeps booming for organizations, especially for large organizations. Oftentimes data-protection is an afterthought, hence despite the huge growth in adoption, data protection for applications running on containers still lags behind.

Dell EMC Avamar is a world-leading data protection software designed to protect various client types. Avamar client is a lightweight software and available for cross platforms, including Linux and Windows. By Docker-izing Avamar client aoftware, the container workloads can be well protected in application-consistent level. Dockerized Avamar client is maintained within the Docker image and will be deployed automatically together with a container startup.

Docker-izing Avamar client to protect container workloads leverages unique Avamar advantages in data protection as well as docker convenience in containter management and maintenance:

- Dockerized Avamar client will auto install, startup and then register to Avamar server at the time when container is deployed and activated.
- Avamar guarantees data integrity through various methods. Avamar backup is application-consistent other than crash-consistent. Avamar checkpoint HFS check feature and replication feature also help data integrity.
- Avamar Web GUI provides centralized client manageement.
- Avamar employs patented variable-length global deduplication, which significantly reduces backup time by only storing unique daily changes.
- In-flight encryption occurs during a backup or restore. If encryption at rest is enabled, all data is stored in an encrypted format so that even if data on disk was compromised, it would be unreadable.

Dell EMC PowerProtect with Data Protection for Kubernetes allows you to protect your production workloads in Kubernetes (K8s) environments, ensuring that the data is easy to backup and restore, always available, consistent, and durable in a Kubernetes workload or DR situation.

Benefits:

- PowerProtect with Data Protection has a Kubernetes-native architecture developed for Kubernetes environments
- Easy for the IT Ops team to use and is separate from the dev ops environment; allows centralized governance from the dev ops environment
- Users are protecting into PowerProtect DD, benefiting from secondary storage with unmatched efficiency, deduplication, performance and scalability -- and near-future plans to protect to object storage for added flexibility
- Jointly engineered with VMware
- PowerProtect Software offers centralized management, automation, multi-cloud options and advanced VMware integration for ease and simplicity for managing workloads.

Private and Public Cloud Platforms

51 Aws Amazon Web Services

Amazon Web Services

Together, Amazon AWS and Dell EMC create a powerful cloud backup and recovery solution so you can deploy and scale the right-sized cloud data protection no matter where data lives. Dell EMC accomplishes this by providing direct backup from Amazon Elastic Cloud Compute (EC2) instances to Amazon Simple Storage Services (S3) without the bottleneck of a media server. Through exceptional client-side deduplication of 6:1 and compression, Dell EMC PowerProtect Software boosts performance and throughput while reducing the consumption of object storage required by up to 71% when doing a backup. Best yet, all data is sent encrypted to Amazon S3.

Dell EMC protects your data for any cloud strategy in Amazon AWS:

- Extend to the Cloud: Leverage the elasticity, agility and low cost of cloud storage
  - Backup direct to cloud
  - Disaster recovery to cloud
  - Long term retention to cloud
  - Desktop/Laptop backup to cloud
- In Cloud Protection: Protect data and application born in the cloud or that have been moved there
  - Protection storage in the cloud
  - Backup in cloud
- As A Service: Gain enterprise protection solutions that are delivered as a service
  - Backup as a Service
  - SaaS data protection
  - Service/Solution providers powered by Dell EMC Technologies

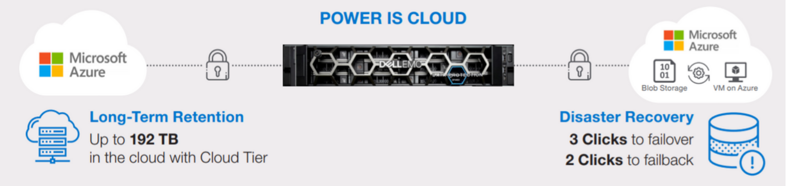
Dell EMC Managed Services provides enhanced operations and data protection solutions to help customers meet their business outcomes and removed the risk and burden of managing the cloud environment themselves

52
Az
Microsoft Azure

Microsoft Azure

As companies look to cloud-based data protection to minimize complexity, optimize costs, and ensure disaster recovery capabilities, Microsoft Azure enables the benefits of moving to cloud while protecting against the potentially devastating impact of data breaches, malicious attacks and system failures. Cloud disaster recovery (DR), also known as disaster recovery-as-a-service (DRaaS), enables IT admins to back up data and applications to a secure off-premises location, providing off-site protection that enables virtual machines to quickly be brought up and running again in minutes in the case of a disaster – minimizing downtime and keeping your business up and running.

The Dell EMC PowerProtect DD and Integrated Data Protection Appliance (IDPA) natively provide the ability to protect your on-premises environment. By combining enterprise-grade technology with simplicity and ease of use, PowerProtect DD and IDPA help organizations take advantage of cloud efficiencies for data protection, disaster recovery, and long-term retention, all in a single appliance.



PowerProtect DD and IDPA can store directly to Microsoft Azure to optimize costs, only using more expensive compute services when a recovery process leverages virtual machines. Because data is compressed before sending it over to the cloud repository and change block tracking is deployed to only send new data, there is no need to purchase or deploy a separate cloud gateway.

53 Vc
VMware Cloud on AWS

VMware Cloud on AWS

Together, VMware and Dell EMC enable enterprise IT and operations teams to continue to add value to their business in the AWS cloud while maximizing VMware investments and eliminating the need to buy new hardware. Customers can confidently scale capacity up or down without change or friction, and can modernize their applications with native AWS services.

Cloud Migrations

- Accelerate cloud migration without complex conversions. Dell EMC providers VMware Cloud on AWS customers with confidence to move production workloads to the public cloud.
- Ideal for customers who want to move to the cloud without having to re-architect applications.

Data Center Extension:

- Ideal for customers who want to expand their on-premises footprint with cloud capacity for specific needs.
- Accelerate speed of provisioning.
- Seamless integration with on premises data protection.

Disaster Recovery:

- Ideal for customers who want to implement a DR solution for the first time.
- Reduce secondary DR site costs by moving DR operations to the cloud or by modernizing existing DR solutions.
- Complement existing DR with a cloud-based DR solution for specific applications.
- Lower monthly in-cloud data protection costs

Backup to Cloud and General Cloud Protection:

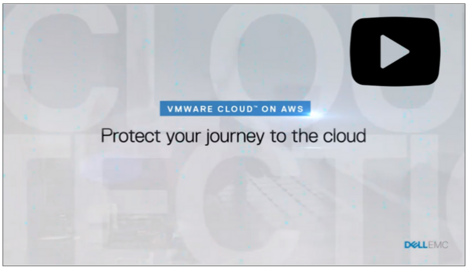
- Minimize cloud cost and footprint with on-demand recovery and direct in-cloud access

The value propositions of Dell EMC data protection for VMware Cloud on AWS are:

- Architecture Matter
  - Deduplication / protect directly to Amazon S3
  - Scales to 96 TB with Dell EMC PowerProtect Virtual Edition (DD VE)

- Cloud DR
  - 3 click failover, 2 click failback
  - Cloud DR - recovery to VMware Cloud on AWS
  - Cloud DR - rapid recovery reduces RTO

- Automated and Simple
  - Easily add new capabilities in the cloud
  - vMotion makes moving to the cloud easy



54 **Gcp** Google Cloud Platform

Google Cloud Platform

Dell EMC Cloud Tier provides best of breed technology that will allow businesses to gain the advantages of cloud while lowering overall TCO. With Cloud Tier, data is natively tiered to the public, private or hybrid cloud for long-term retention. Only unique data is sent directly to the cloud and data lands on the cloud object storage already deduplicated. Dell EMC's advanced deduplication, storage footprint is greatly reduced for cost-effective long-term retention in the cloud such as Google Cloud Platform.

55 **Alc** Alibaba Cloud

Alibaba Cloud

Dell EMC PowerProtect DD and Integrated Data Protection Appliance (IDPA) provide customers with choices to extend their data protection to public clouds with expanded Cloud Tier support to Alibaba Cloud, thereby, enabling more flexibility for long-term retention.

56 **Ic** IBM Cloud

IBM Cloud

Dell EMC Cloud Tier enables businesses to leverage the economies of cloud for long-term retention. Only unique data is sent directly to the cloud and data lands on the cloud object storage already deduplicated. Dell EMC Cloud Tier's ecosystem of supported public cloud platform includes IBM Cloud object storage.

57 **Vs** Virtustream

Virtustream

Virtustream is the enterprise-class cloud solutions provider focused on delivering mission-critical public, private, and hybrid cloud technologies and services to enterprises, governments, and service providers worldwide. Virtustream Storage Cloud is best-suited for long-term storage archive workloads with Dell EMC Cloud Tier solution.

58 **Pc** Private Cloud

Private Cloud

Dell EMC ECS Object Storage is an object store designed to support modern archiving. The benefits of ECS include cost-efficiency due to built-in disaster recovery and storage capacity elasticity, and simplified common archive for all data within the data center. Dell EMC Cloud Tier moves infrequently accessed data to ECS as a lower-cost option for long term retention.

Data Protection Support and Deployment Services, Consulting and Advisory Services

59 Dm Data Migration Services

Data Migration Services

Accelerate your time-to-value, at a lower cost and with minimal disruption to your environment. Data Migration Services allows you to focus on your business, while Dell Technologies manages your migration. This approach to data migration is proven, standardized, and platform and vendor agnostic, making migrating data from any storage array simple. With over 30 years of data migration experience under our belts and over one exabyte of data migrated annually, you're in good hands with Dell EMC.

60 Rs Residency Services

Residency Services

Dell EMC Residency Services provide technology experts to optimize configurations, processes and procedures, and share knowledge with IT staff. Transition to new capabilities quickly, while keeping your data center running at its peak. You control these experts' priorities and time, and you'll have the flexibility to adjust resources and budget. Free your IT staff from the tactical to give them more time to innovate.

61 Ss Support Services

Support Services

Dell EMC Support Services are built on a foundation of artificial intelligence (AI), machine learning and data analytics. Our Support Services are changing the way you look at saving time and increasing availability. Maximize productivity and uptime with the support expertise, insights and technologies we're known for across the globe.

Our ProSupport Enterprise Suite doesn’t just extend your IT team, it enables you to address issues before they impact your business. We are taking the “break” out of “break-fix".

62 Ds Deployment Services

Deployment Services

To get the most out of new technology and start realizing a return on investment, you need systems out of the box and into optimized production – fast, without risk or downtime. Whether you are adding new equipment to a data center or migrating end users to the newest laptops, you can count on Dell EMC ProDeploy or ProDeploy Plus Enterprise to execute quickly and correctly the first time. We’ve spent over 30 years building deployment practices backed by elite professionals with broad and deep experience utilizing best-in-class processes. Our established global scale drives consistent deployments to help you drive greater business results, around the clock and around the globe.

63 Ms Managed Services

Managed Services

End-to-end Dell EMC Managed Services include multi-cloud optimized solutions for data storage, backup, converged infrastructure and more. With our unique expertise, processes and IP, we help you realize business and technology value faster by handling the burden of daily complex operations. And we back our solutions with the service levels you need to run and transform your business.

64 Ad
Advisory
Services

Advisory Services

Dell Technologies ProConsult Advisory Services facilitate a plan for beneficial and lasting change. Our AS-IS/TO-BE methodology, the foundation of our services, can help you realize the business benefits of transformation faster, more reliably and with lower risk. Our services are designed to help assess and plan transformations that achieve measurable outcomes aligned to your corporate vision and strategy.

Using facilitated workshops and stakeholder interviews, our consulting services experts work with your team to capture the AS-IS current state of the environment under review to develop topology diagrams and document information on key technical systems. We help your team to understand related projects in progress, with a summary of objectives, approximate duration and team structure. We will also help you determine the strategic vision and guiding principles for the future environment aimed to develop a holistic roadmap with actionable initiatives for migrating from the AS-IS to the TO-BE state.

65 Cra
Cyber
Recovery
Advisory

Cyber Recovery Advisory Services

Dell Technologies' Cyber Recovery Solution enables the recovery of your most critical information by utilizing an air-gap to separate the Cyber Recovery Vault from production networks. The latest approach emphasizes keeping an isolated copy of your most critical data off the production network and isolated from production backup systems. Our Consulting experts work with you and your teams to conduct a Cyber Recovery workshop and to develop processes and procedures that enable you to protect and recover your critical data in the event of a destructive cyber attack.

Dell Technologies Consulting accelerates the solution in customer environments through two key phases—Advisory and Implementation. The Advisory phase focuses on providing recommendations to quickly integrate and optimize the Cyber Recovery Solution in your data protection environment. We have broken down the advisory phase into three tiered services to align to your goals and business requirement – Workshop, Advisory and Advisory and Roadmap which includes developing a cyber recovery maturity model report to benchmark your current state against industry best practices. The Implementation phase integrates the Cyber Recovery Solution into your data protection environment. In this phase we can use information gathered through the advisory phase to further tailor the solution to your exact needs. We can also integrate additional technologies and capabilities with your Cyber Recovery environment such as creating Cyber Recovery Vault to include multiple platforms, heterogeneous technologies, retentions policies and applications.

66 Apo
Application
Portfolio
Optimization

Application Portfolio Optimization Services

The Dell Technologies Application Portfolio Optimization Services capture your key business and technology drivers to evaluate applications. It offers cost and saves time by leveraging semi-automated tools that accelerate analytics-based decision-making. We conduct workshops to evaluate and gather data on the applications and services with key stakeholders and service delivery managers.

Looking at both business and IT alignment, we determine how best to invest in each application based on the four investment categories for traditional applications - build new/modernize, migrate, retire or retain. We also investigate which cloud option is best suited for your application and how readily will the application move to the new cloud platform.

Leveraging findings from disposition analysis, we dive more deeply into application workload characteristics to determine the best cloud model; public, private or hybrid. Based on the analysis, we generate a financial analysis which provides a holistic view into the total cost of ownership for the application. The final application portfolio transformation roadmap will be built once we factor in the business case for the application portfolio being analyzed. Dell Technologies' Application Portfolio Optimization Services assure fast, consistent, and less resource intensive results than traditional manual services. In our experience, clients arrive at application disposition recommendations 50% faster using 75% fewer client resources than typical market services.

Throughout the process of profiling applications, you must also consider the criticality of each application to your business stakeholders to ensure an appropriate level of data protection and availability considerations are applied to each. This will ensure your applications are available to business stakeholders despite an outage.

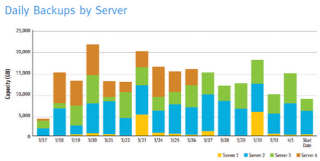
Recovery Readiness Assessment

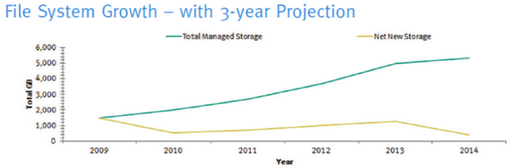
How confident is your enterprise IT in recovering data and meeting service level agreements in today's multi-vendor and multi-faceted user environment?

Organizations need regular assessments of their data protection environment, as the size and complexity of IT infrastructure is constantly evolving due to data growth, adoption of new technologies, and the deployment of next-gen mobile and cloud-based applications. Dell EMC Recovery Readiness Assessments can be done quickly and in a non-intrusive manner, to help you achieve your IT and business objectives by identifying risks, resolving problems and formulating a plan of action to optimize your data protection infrastructure.

You make informed decisions and choices based on insights into:

- Inventory of existing backup media systems and their configurations, backup software
- Status of servers not protected (including Active Directory servers, file and email servers)
- Deduplication rates and workloads of backups in analyzing data as good fit for backup to deduplication storage systems
- Backup capacity and backup jobs in a specific timeframe, in identifying areas of backup failures due to narrow backup windows, unreliable clients, backup server workload issues or performance of tape drives
- Data and storage usage, and file aging patterns (email, file systems and Sharepoint deployment) for archiving possibilities
- Capacity, performance and configuration details on Oracle backups via Oracle RMAN
- Mainframe tape capacity, bandwidth and workload information


Daily Backups by Server


File System Growth – with 3-year Projection

Further Reading: Products and Solutions

Data Capital - Primary Storage and Data Protection

Dell EMC Data Protection and Data Management

Dell EMC PowerProtect Software

Dell EMC Data Protection Suite

Dell EMC PowerProtect Appliance

Dell EMC Integrated Data Protection Appliance

Dell EMC PowerProtect DD Appliance

Dell EMC PowerProtect Cyber Recovery Solution

Dell EMC Data Protection for VMware

Dell EMC Cloud Data Protection

Dell EMC Data Migration Services

Dell EMC Residency Services

Dell EMC Deployment Services

Dell EMC Support Services

Dell EMC Managed Services

Dell Technologies ProConsult Advisory Service

Dell Technologies Cyber Recovery Advisory Services

Dell Technologies Application Portfolio Optimization Services