DELL Technologies

OEM Solutions White Paper

Differentiating Your Solution by Adding Modern Data Protection and Cyber Resilience

Accelerate your revenue stream, differentiate your solution, and improve your customer relationships by adding advanced data protection and cyber-resilient technologies.

Abstract

This white paper describes how Dell Technologies OEM Solutions helps our OEM customers accelerate the design of their solutions and why adding advanced data protection and cyber-resilient capabilities allows them to further differentiate their solutions in the market.

November 2021

H19000

Revisions

Date	Description
November 2021	Initial release

Table of contents

Executive summary

High availability and reliability are already paramount requirements and key tenets for today's leading solutions. With cyberattacks occurring in increasing ferocity and speed across enterprises worldwide, consensus is building that businesses must plan for how to respond (Figure 1). The business mindset has transitioned from if an attack will occur to when it will occur.

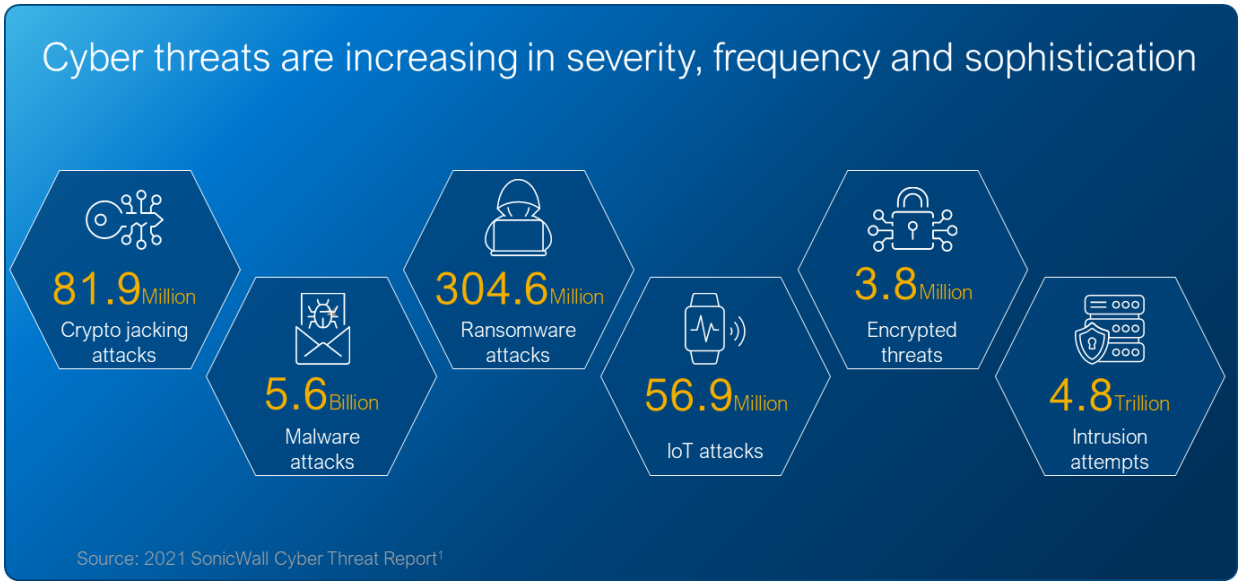

Figure 1: Massive cyberthreat acceleration is underway as outlined by the 2021 SonicWall Cyber Threat report[1]

Rather than waiting for a cyberattack or a downtime event, our original equipment manufacturer (OEM) customers are working with Dell Technologies OEM Solutions to design and integrate advanced data protection and cyber-recovery technologies into their solutions from the start. No longer is building conventional recovery options, such as hardware-based redundancy, into solutions adequate to protect your customers.

With Dell Technologies' data protection technologies, access to advanced engineering and customization resources, our OEM customers are often surprised how seamlessly these advanced capabilities can be integrated into their solutions. Not only do these capabilities differentiate our customers' solutions, but they also offer increased revenue streams and improved protection. More importantly for your end customers, Dell Data Protection Solutions (DPS) work to minimize their financial losses and remediation costs when operational downtime or a cyber incident occurs.

1 Introduction

As ransomware shutters businesses for days or weeks and costs millions of dollars in losses, traditional backup and disaster recovery strategies no longer suffice. For example, a retail store's smart cash register can become the entry point for a cyberattack that leads to affecting back-end systems and causing broader downtime and greater revenue loss. Such a scenario also can burden the retailer with high legal fees, regulatory costs, and a damaged brand. In addition, if the attack spreads to the retailer's backup copies, operational recovery, if still feasible, will take longer and incur additional financial losses.

Our OEM customers realize that selling solutions with conventional built-in redundancy and expecting their customers to handle comprehensive data protection after delivery of their solutions are risky strategies (Figure 2). In addition, when an attack occurs, your customer may lose confidence in your solution and seek a new partner.

Figure 2: Concern among IT decision makers globally about conventional protection options grows. Results were derived from a recent Dell Technologies commissioned research paper of 1,000 IT decision makers worldwide from private and public organizations with 250+ employees[2].

Instead of waiting for the next downtime event, our forward-thinking OEM customers are designing modern data protection into their solutions from the start. Dell Technologies OEM Solutions offers our customers a broad spectrum of advanced data protection and cyber-resilient technologies, along with expertise and services making integration easier and faster.

2 Dell Technologies OEM Solutions: Fast on-ramp to built-in data resiliency

Whether you are a global company or a small-to-medium-size business, OEM Solutions can extend our data protection and cybersecurity capabilities and resources in a meaningful and strategic way. Not only do you have access to the 160,000+ employee Dell Technologies organization, but 1,000+ engineers, program managers, analysts, and sales and marketing professionals, focus exclusively on our OEM business where you are at the center.

The many advantages of partnering with Dell Technologies OEM Solutions include:

- Access to top-tier data protection, cyber-resilient, storage, server, and client technologies
- World-class global supply chain, service, and support infrastructure that prioritizes data security
- Advanced data protection and cybersecurity expertise with access to OEM-specific engineers and architects
- Dedicated OEM engineering and program management organization with 30-year history
- Competitive advantage with fast time-to-market of custom innovation
- Rebranding and de-branding options across our data protection hardware, documentation, and packaging

3 Dell Technologies' comprehensive data protection and cyber-recovery portfolio

Dell Technologies OEM Solutions offers our customers several options for integrating data protection into their solutions for all of today's demanding next-generation workloads running on VMware and Kubernetes, as well as legacy and custom applications. With data protection outside the data center or IT closet commonplace today, Dell Technologies has you covered whether your workload and data reside across the edge, data center, or cloud.

Dell Technologies data protection and cyber-resilient solutions span a broad spectrum of recovery point objective (RPO) and recovery time objective (RTO) requirements, as well as deliver on leading protection requirements and capabilities that are industry proven and trusted by leading solution providers. RTO is the timeframe in which an application or system must be restored after an outage. RPO is the time between protection points or the amount of data that will be lost if there is a service interruption.

In a recent Dell Technologies commissioned economic validation paper, ESG analyzed the economic and operational benefits of Dell EMC PowerProtect[3]. Benefits included cost reduction, improvement in recovery times, and an overall reduction in administrative effort.

Dell Technologies solutions align especially well with today's challenges for data protection and cyber recovery by offering flexible consumption models to fit your solution design (Figure 3).

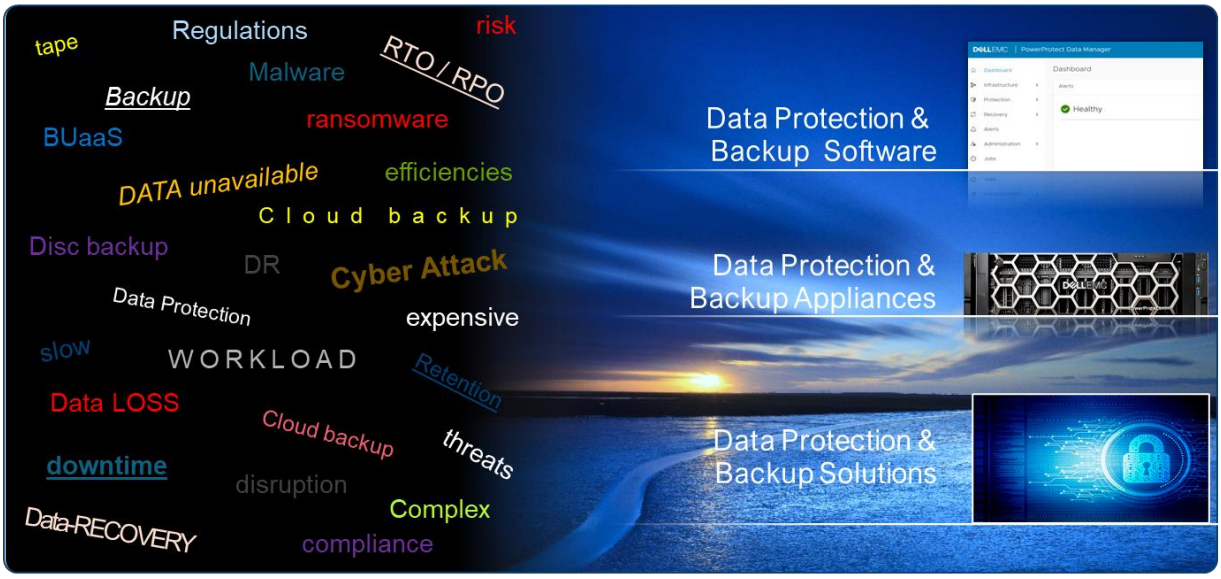

Figure 3: Aligning data protection and cyber-recovery challenges with Dell Technologies solutions

Data Protection and Backup Software

- **Dell EMC PowerProtect Backup Service** is a cloud data protection solution designed to deliver endpoint and SaaS-based protection without increasing IT complexity while ensuring predictable, controllable costs. PowerProtect Backup Service deploys in minutes and provides unlimited on-demand scaling to ensure growing data volumes are always protected. An intuitive web-based experience provides centralized visibility and management of SaaS apps, endpoints, and hybrid workloads, providing peace of mind that data is always protected. PowerProtect Backup Service is a strong data protection tool for Dell Precision workstations.

- **Dell EMC PowerProtect Data Manager backup software** is a next-generation data protection management and orchestration tool set that provides software-defined, autonomous protection of containerized workloads, such as Kubernetes, databases, virtual machines, and file systems. Optimized for multi-cloud, hybrid cloud, and on-premises environments, PowerProtect Data Manager delivers self-service backup and restore, data deduplication, and cloud-based monitoring analytics.

- **Dell EMC Data Protection Suite** is a comprehensive backup solution designed to protect proven and modern workloads by using technologies, such as replication, snapshot, backup, and disaster recovery. Data Protection Suite delivers protection based on the value of the data and service levels that align to business objectives.

- **Superna Eyeglass Ransomware Defender for PowerScale** is a highly scalable, real-time event processing solution that applies user behavior and data analytics to detect and halt a ransomware attack on data stored on Dell EMC PowerScale scale-out unstructured storage.

- **Dell EMC PowerProtect DD Virtual Edition (DDVE)** is a software-defined data protection management solution for the Dell EMC PowerProtect DD series. DDVE provides excellent operational efficiency, high reliability, and low total cost of ownership.

Data Protection and Backup Appliances

- **Dell EMC PowerProtect DP Series** is an all-in-one integrated data protection appliance that accelerates backup and recovery, as well as provides replication, deduplication, and instant access and restore capabilities with tight VMware integration. This one-stop integrated data protection appliance delivers low protection costs with long-term retention and disaster recovery to the cloud.

- **Dell EMC PowerProtect DD Series** is a target appliance providing physical or virtual protection storage for up to 1.5 petabytes and incorporates exceptional deduplication, scalability, performance, and data integrity capabilities. Designed to meet backup, archive, disaster recovery, and cyber-recovery needs for organizations of all sizes, PowerProtect DD Series easily integrates with Dell EMC and third-party backup software.

Data Protection and Backup Solutions

- **Dell EMC PowerProtect Cyber Recovery** is a solution that can be integrated and built with your existing data protection workflows to proactively automate protection and isolation of critical data from ransomware and other sophisticated threats. Sophisticated machine learning identifies suspicious activity and allows you to recover quality data from efficient, immutable storage to resume normal business operations with confidence. With the use of data isolation, air gap, intelligent analytics, recovery, and remediation tools, you can now adopt a proven and automated cyber resiliency strategy in your solution.

- **VMware Backup, Recovery and Data Protection** solutions protect VMware workloads in a multi-cloud world, optimize data protection for VxRail systems, protect your Kubernetes workloads, and take the guesswork out of data protection and automation with storage policy-based management from within vSphere.

4 High-value use cases for modern data protection

There are numerous compelling use cases for advanced data protection. In this paper, we highlight four examples of them, including edge, cyber recovery, smart industry, and business intelligence.

4.1 Automated data protection at the edge

As the traditional cash register has become a smart point-of-sale system, retailers capture valuable sales and customer data at multiple stores that typically are not staffed by IT specialists. Yet, retailers must protect this data in the same way and with the same policies implemented in data centers for corporate-based information. Additional edge-based environments typically requiring modern data protection include factory floors, remote oil and gas facilities, warehouses, and distribution centers, among others.

PowerProtect Backup Service provides our customers with a way to offer 24x7 backup services via the cloud without any infrastructure to manage. With PowerProtect Backup Service, you can provide your customers with streamlined compliant, scalable, and cloud-based data protection with predictable costs.

For customers preferring to maintain protection copies on their own edge infrastructure, OEM Solutions offers customized solutions based on Dell PowerEdge Servers that run PowerProtect Data Manager and PowerProtect DD Virtual Edition. PowerEdge solutions are easy to deploy and manage and do not require IT expertise onsite since they offer remote management. Available at capacities starting at two terabytes or less, PowerEdge solutions offer a small footprint to enable a fast and simplified recovery.

4.2 Effective recovery from cyberattacks

Dell Technologies offers a holistic cyber-resilient strategy that incorporates technology and solutions for detection, prevention, backup, and recovery. A key differentiator in Dell's cyber-recovery approach provides for in-depth and content aware intelligence and insights about backup datasets. In addition to a primary backup copy for operational recovery, another backup copy is logically isolated from production. This way, the PowerProtect Cyber Recovery solution runs analytics on backup copies and pinpoints any anomalies that may require further investigation or forensic investigation. When required, the solution offers quick recovery of the production system from the isolated backup and offers other remediation capabilities.

With PowerProtect Cyber Recovery, you can protect and recover backups of structured data, databases, and analytics stored on Dell EMC PowerProtect appliances. Similarly, Dell has a solution intended for unstructured data, such as radiology images, videos, and file system data. Dell Technologies also offers Superna Eyeglass Ransomware Defender for Dell EMC PowerScale using snapshotting and replication for cyber recovery, ransomware remediation, and detection.

PowerProtect Cyber Recovery and Superna Eyeglass Ransomware Defender for PowerScale solutions are based on the NIST Cybersecurity Framework (Figure 4).

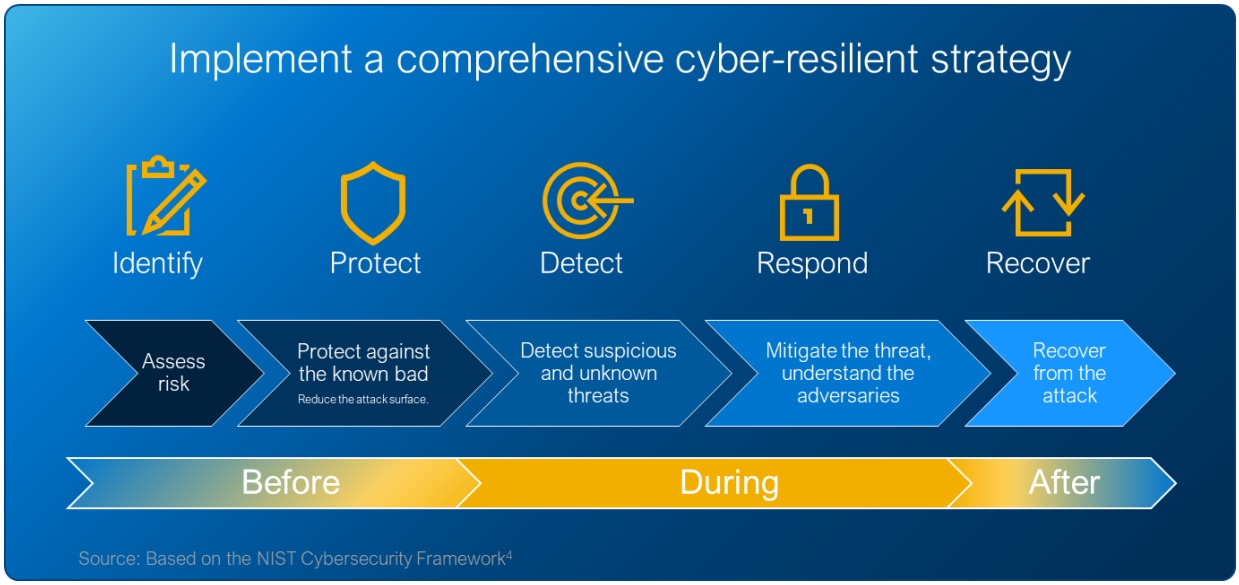

Figure 4: Based on the NIST Cybersecurity Framework[4]

4.3 Smart industry uptime vital to supply chains

With smart automation, data controls every step in the manufacturing process. Any interruption to accessing that data can stymie the flow of critical products and services to customers and shut down operations for days or weeks, disrupting supply chains and revenue streams. For example, downtime of control systems along an oil refinery pipeline can have reverberating impacts across businesses, communities, and the economy.

Dell Technologies' portfolio of data protection and cyber-recovery solutions integrate well with the entire smart manufacturing ecosystem from VMware to core storage to encrypted backups. Dell EMC recommends an integrated solution that uses PowerProtect Data Manager to back up smart industry applications to PowerProtect DD series backup appliances spanning low- to high-capacity storage requirements.

4.4 Protecting business intelligence databases

Databases containing vast repositories of business intelligence are vital to operations in telecommunications, healthcare, and other industries with high-volume, high-capacity data storage requirements. These databases run operation support systems/business support systems (OSS/BSS), electronic medical records, and radiology applications, among other workloads.

In these environments, Dell Technologies OEM Solutions recommends backing up databases to PowerProtect DD series with PowerProtect Data Manager. The Dell EMC PowerProtect solution is easy to deploy and manage and offers automated management of backup policies. When integrated with the PowerProtect DD series appliances, the solution assures highly efficient transfer of data from production to backup systems with automated data deduplication. In addition, PowerProtect Data Manager performs backups of databases in VMware environments without interfering with the operation of virtual machines.

5 Differentiate your solutions by adding modern data protection

Acceleration of cyberattacks, increasing automation of workloads, and growing value of data all point toward an urgent requirement to adopt a stronger, comprehensive data protection and cyber-resilient strategy.

Dell Technologies OEM Solutions, with our extensive engineering resources and portfolio of data protection and cyber-recovery products, are here to partner with you to create your optimal solutions. We can even rebrand our solutions to align with your branding or your customer's branding.

We have the expertise, resources, and technologies to help you achieve high-impact business outcomes and we encourage you to reach out to your Dell Technologies OEM Solutions representative to discuss how a modern data protection and cyber-recovery solution can provide you with competitive advantage. Or visit us at https://www.DellTechnologies.com/OEMstorage.htm to learn more.

6 Reference list

[1] 2021 SonicWall Cyber Threat Report, Cyber threat intelligence for navigating the new business reality

[2] Dell Technologies Global Data Protection Index 2021, findings from Vanson Bourne's Global Data Protection 2021 study commissioned by Dell Technologies of 1,000 IT decision makers (ITDMs) globally

[3] A Dell Technologies commissioned paper ESG Economic Validation 2020: Analyzing the Economic and Operational Benefits of the Dell EMC PowerProtect Data Protection Portfolio

[4] NIST Cybersecurity Framework