ECONOMIC VALIDATION

The Economic and Operational Benefits of the Dell PowerProtect Portfolio

Organizations Can Strengthen Cyber Resilience and Reduce Total Cost of Ownership Up to 61% Through More Efficient Recovery Operations

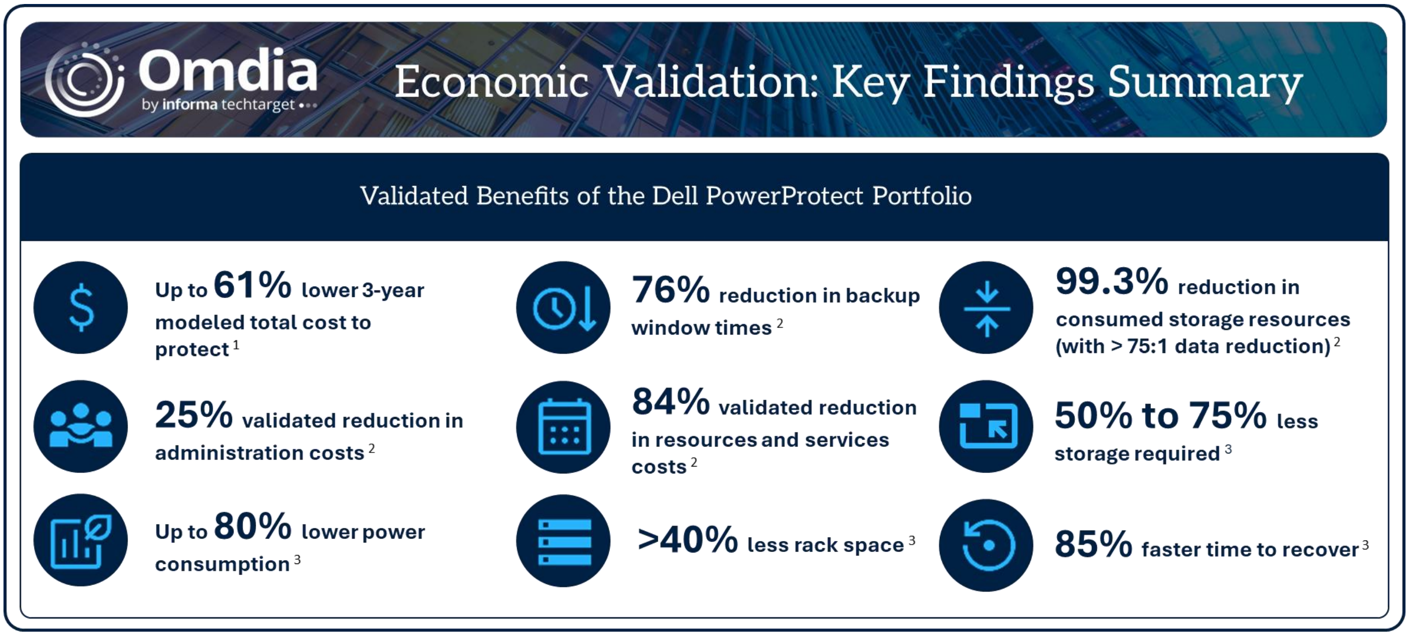
By Aviv Kaufmann, Practice Director; Jennifer Duey, Senior Economic Analyst; and Nathan McAfee, Senior Economic Analyst

Omdia

February 2026

This Economic Validation from Omdia was commissioned by Dell and is distributed under license from TechTarget, Inc.

Contents



Omdia by informa techtarget

Economic Validation: Key Findings Summary

Validated Benefits of the Dell PowerProtect Portfolio

Up to **61%** lower 3-year modeled total cost to protect[1]

76% reduction in backup window times[2]

99.3% reduction in consumed storage resources (with > 75:1 data reduction)[2]

25% validated reduction in administration costs[2]

84% validated reduction in resources and services costs[2]

50% to 75% less storage required[3]

Up to **80%** lower power consumption[3]

>40% less rack space[3]

85% faster time to recover[3]

[1] Modeled by Omdia vs. alternative solutions.

[2] Reported by customers vs. previous solutions.

[3] Based on Dell analysis vs. previous generation Dell solutions.

Introduction

This Economic Validation examines the economic and operational benefits organizations can achieve by adopting the Dell PowerProtect Portfolio, powered by Intel Xeon Scalable processors. The portfolio helps enterprises withstand, respond to, and recover from cyber incidents by combining a purpose-designed backup foundation with advanced data reduction and an integrated, scalable, and cloud-extendable cyber resilience architecture. Rather than focusing solely on backup, the platform integrates secure data storage, threat detection, recovery orchestration, and data integrity validation across hybrid, multicloud, and SaaS environments.

Omdia developed a modeled scenario to evaluate how organizations realize cost efficiencies by consolidating cyber resilience capabilities on a single, integrated platform. The analysis shows that organizations improve infrastructure and storage efficiency, reduce operational overhead, and accelerate backup and recovery performance, while optionally enabling automated cloud-based disaster recovery and long-term data retention. Together, these outcomes deliver faster, more predictable recovery and lower the total cost of maintaining enterprise-grade cyber resilience.

Challenges

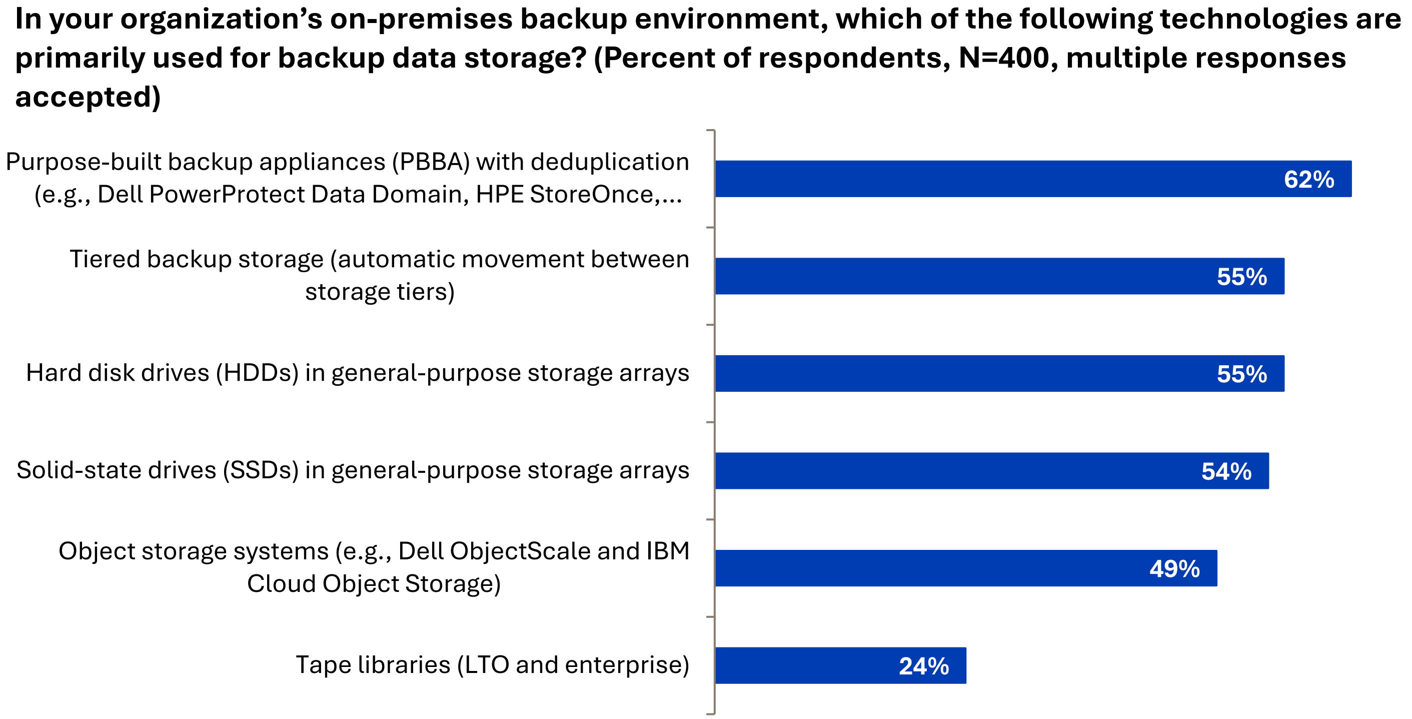
Organizations face increasing difficulty achieving cyber resilience as attack techniques evolve and IT environments become more complex. Modern ransomware and cyberattacks frequently rely on credential abuse, lateral movement, and trusted administrative tools rather than traditional malware, allowing adversaries to persist undetected while deliberately targeting recovery systems. As a result, many organizations only discover the full extent of compromise during recovery, when backups are unavailable, incomplete, or no longer trustworthy.

At the same time, data sprawl across hybrid, multicloud, and increasingly distributed on-premises environments introduces operational complexity and inconsistent controls. Organizations must also contend with an expanding regulatory and compliance landscape, including retention, immutability, and audit requirements, while meeting tighter recovery objectives. As data volumes grow and recovery expectations tighten, backup infrastructure must balance security, performance, and operational efficiency. Without immutability, isolation, and data integrity controls built directly into the backup platform, recovery operations become manual and resource-intensive, extending downtime, increasing operational costs, and amplifying financial and reputational risk.

These challenges are reflected in how organizations architect their on-premises and hybrid backup environments today. According to Omdia research, purpose-built backup appliances with deduplication are the most widely used backup storage technology (62%), followed by tiered backup storage and general-purpose storage arrays, including hard disk drives (55%).[1]

[1] Source: Omdia Research Report, *The Ransomware Reality: Cyber Resilience, Data Resilience, and Data Protection*, November 2025.

Figure 1. Purpose-built Appliances Are Commonly Targeted for Backup



Source: Omdia

As organizations continue to modernize their backup and recovery environments, the widespread reliance on purpose-built backup appliances reflects a broader shift toward platforms that prioritize efficiency, predictability, and resilience at scale. Enterprises are increasingly seeking architectures that integrate storage efficiency, secure data foundations, and offer reliable recovery capabilities without introducing additional operational complexity or unforeseen infrastructure requirements.

This shift focuses on the growing importance of integrated cyber resilience platforms built on purpose-designed backup foundations. Rather than relying on fragmented tools or general-purpose infrastructure, organizations are evaluating approaches that can support secure, efficient data protection and recovery across evolving enterprise environments.

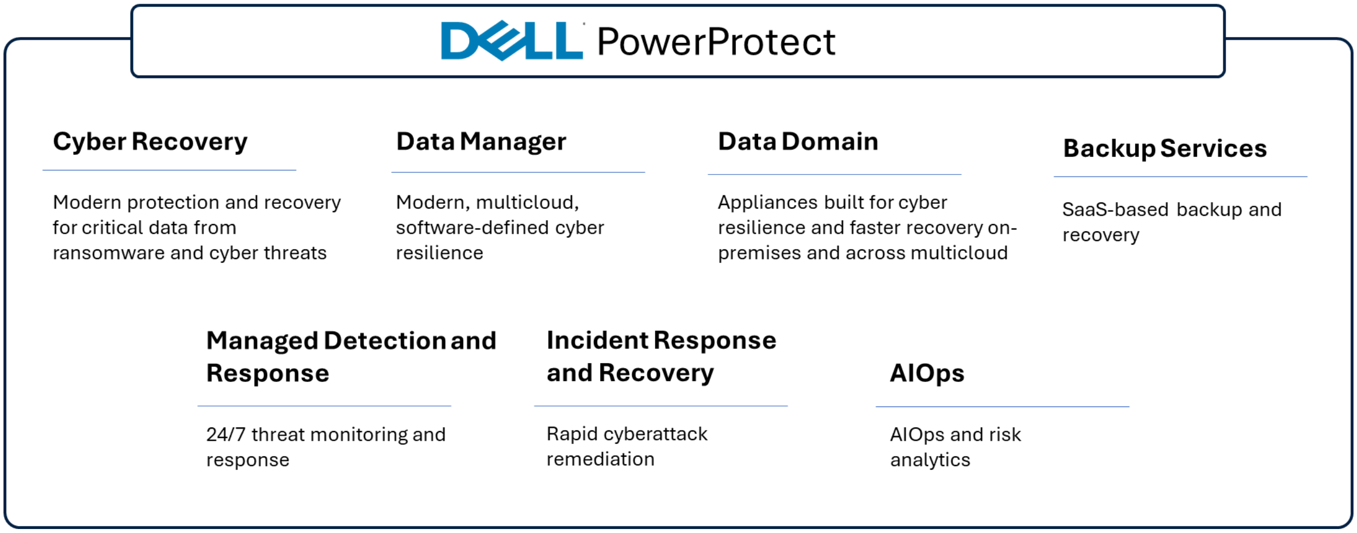
The Solution: Dell PowerProtect Portfolio for Cyber Resilience

Dell offers a highly secure and reliable platform for cyber resilience, designed to meet the needs of organizations of all sizes and safeguard critical data and applications deployed across on-premises, edge, ROBO, hybrid, and multicloud environments. The platform supports organizations in anticipating, withstanding, recovering from, and adapting to cyber incidents by integrating secure data foundations, threat detection, and recovery capabilities into a unified architecture.

As shown in Figure 2, the Dell Intel-powered platform for cyber resilience comprises software, purpose-built backup appliances, cyber recovery solutions, and as-a-service offerings. Core components include PowerProtect Data Manager for software-defined cyber resilience and orchestration; PowerProtect Data Domain purpose-built backup appliances with advanced data reduction; PowerProtect Cyber Recovery that provides an isolated recovery vault; and as-a-service delivery. Together, these components deliver cyber-resilient backup and recovery, application-consistent protection with governance, cloud disaster recovery, and support for both proven and modern workloads.

Strong interoperability across platform components enables advanced capabilities such as on-demand scaling, non-disruptive upgrades, centralized management, and consistent policy enforcement. PowerProtect Data Manager provides a single control plane across systems and sites, streamlining operations while enabling global visibility into protection status, compliance, and recovery readiness aligned with business objectives.

Figure 2. Dell PowerProtect Portfolio



DELL PowerProtect

Cyber Recovery
Modern protection and recovery for critical data from ransomware and cyber threats

Data Manager
Modern, multicloud, software-defined cyber resilience

Data Domain
Appliances built for cyber resilience and faster recovery on-premises and across multicloud

Backup Services
SaaS-based backup and recovery

Managed Detection and Response
24/7 threat monitoring and response

Incident Response and Recovery
Rapid cyberattack remediation

AIOps
AIOps and risk analytics

Source: Omdia

The Dell cyber resilience portfolio includes:

- PowerProtect Data Manager. PowerProtect Data Manager is a software-defined cyber resilience platform designed for modern, multicloud workloads. It automates discovery and policy-based protection across virtual machines, Kubernetes environments, NAS, and cloud-native applications while providing centralized visibility and control. The platform incorporates Anomaly Detection, Dynamic NAS Protection, and Transparent Snapshots to support application-consistent backups with minimal performance impact. These capabilities enable improved service-level objectives, simplified operations, and accelerated recovery, delivering up to 5x faster backups and up to 6x faster restores compared to traditional approaches.
- PowerProtect Data Domain. PowerProtect Data Domain is an Intel-powered, purpose-built backup appliance that provides a secure, efficient storage foundation for cyber resilience. It supports both traditional and modern workloads while delivering high-performance recovery and data reduction capabilities that are not achievable with alternative offerings. Data Domain delivers data reduction, typically 75:1, helping organizations control storage growth and infrastructure costs. They lead the industry as one of the most secure platforms for cyber resilience, featuring a secure supply chain, hardware security with a chain of trust, and tamperproof data immutability to support a zero-trust architecture. Ideal for recovering from hardware failures or ransomware attacks, they simplify operations and reduce risks for organizations of all sizes.

The latest addition to the Data Domain family, an all-flash appliance based on Intel Xeon processors, extends the platform for environments with demanding recovery and analytics requirements. By leveraging flash storage, the system delivers up to 4x faster restores and up to 2.8x faster analytics performance, while reducing rack space requirements by up to 40% and consuming up to 80% less power than traditional disk-based systems.[2]

- **PowerProtect Cyber Recovery.** PowerProtect Cyber Recovery secures critical data in a hardened recovery vault, isolated from production and backup environments. It uses CyberSense analytics to detect corruption with 99.99% accuracy, validate backups, and identify clean recovery points. Automated workflows enable recovery in days, not weeks, while ensuring data integrity. The vault enforces immutability, strict access controls, and multifactor authentication, integrating threat detection to mitigate risks. This ensures data remains secure, intact, and recoverable, even during active cyber incidents.
- **Dell AIOps.** Dell AIOps is a cloud-based, AI-driven observability and management solution designed to optimize Dell infrastructure. It delivers near-real-time insights to maximize infrastructure performance, strengthen cybersecurity, enhance sustainability, and support proactive planning. Featuring an intuitive platform and a generative AI assistant, Dell AIOps helps customers minimize risks, boost efficiency, and simplify IT operations, all within a seamless experience.
- **PowerProtect Backup Services.** PowerProtect Backup Services deliver SaaS-based cyber resilience for hybrid workloads, endpoints, and SaaS applications. These services provide centralized monitoring, automated updates, and ransomware recovery without requiring customers to deploy or manage backup infrastructure. Rapid deployment and on-demand scalability enable organizations to protect distributed environments efficiently, while guaranteed point-in-time recovery supports Microsoft 365 applications, including SharePoint, Exchange, OneDrive, and Teams.
- **Incident Response and Recovery Services.** These services help organizations minimize downtime and restore normal operations after a cyberattack. They provide comprehensive assistance to rebuild and redeploy infrastructure, data, and applications while containing threats and preventing the reintroduction of malware. Delivered by global teams of certified cybersecurity professionals at Dell, the services provide Dell with real insight and expertise to build cyber resilient solutions by enabling structured, safe recovery aligned to organizational risk and compliance requirements. Many alternatives sell recovery solutions but cannot help customers beyond clicking the restore button.
- **Managed Detection and Response (MDR).** Managed Detection and Response provides continuous, 24/7 monitoring and rapid response to cyberthreats. The service combines infrastructure telemetry, proprietary threat intelligence, and next-generation SIEM capabilities to detect anomalous behavior early. In the event of an incident, MDR delivers forensic investigation, threat containment, and eradication services, supported by industry-certified professionals who help organizations maintain business continuity.

Omdia Economic Validation

Omdia conducted a quantitative economic analysis of customer deployments of the Dell PowerProtect Portfolio to evaluate the full economic impact of improving data and cyber resilience across the enterprise. While storage efficiency and data reduction remain important contributors to value, the analysis deliberately extends beyond those metrics to capture total cost considerations that are often overlooked in solution

[2] Based on Dell analysis vs. previous-generation Dell solutions.

evaluations. These include the impact on supporting infrastructure, operational overhead, system performance, maintenance requirements, and long-term scalability.

Importantly, many alternative solutions and vendor-provided TCO models focus narrowly on front-end storage efficiency or acquisition costs and/or only one aspect of the total cyber resiliency solution, thereby underrepresenting the true long-term cost of ownership. By excluding downstream operational, infrastructure, and performance-related cost drivers, these approaches may present an incomplete view of TCO that does not reflect how costs accumulate in real-world enterprise environments. Omdia's methodology is designed to address this gap by incorporating the broader set of cost and operational factors that organizations consistently encounter over time. We explore many of the factors that can impact TCO in the "Beyond Data Reduction" chapter of this report, starting on page 10.

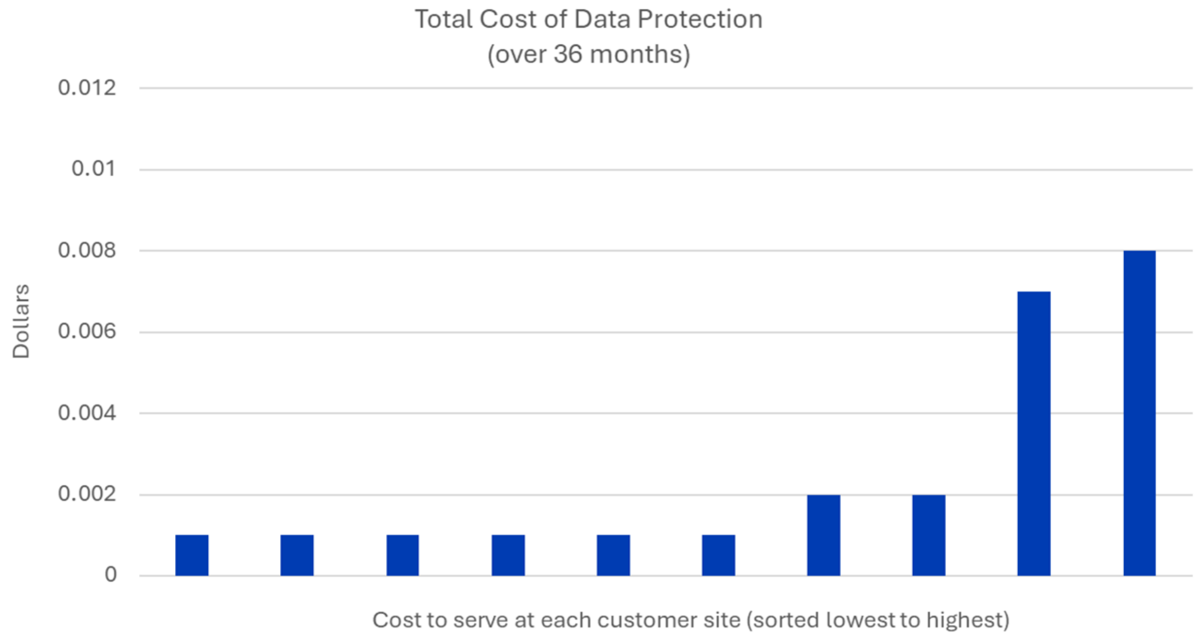
The Economic Validation process leverages Omdia's core competencies in market and industry analysis, forward-looking research, and technical and economic validation. Omdia analyzed system field data and conducted in-depth interviews with end users to understand how Dell's Intel-powered cyber resilience architecture delivers predictable, enterprise-grade efficiency without introducing hidden downstream costs. This approach reflects how organizations experience value in practice, through consistent performance, reduced operational burden, and minimized infrastructure surprises over time, rather than through data reduction metrics alone.

Validated Cost to Protect

To start the analysis process of determining the cost to protect the production data assets of an organization, we audited performance, capacity, and utilization metrics from more than ten field-deployed environments that are leveraging Dell cyber resilience solutions. The results of the analysis are shown in Figure 3, which details how Dell PowerProtect solutions translate into economic benefits for business stakeholders. This part of the analysis measures solution efficiency against hardware, software, support, and Dell Technologies/Partner professional services costs. It should be noted that the cost to protect ranges between 0.001 dollars per gigabyte for six out of the ten customers and .002 dollars to .008 dollars per gigabyte for the remaining four customers.

> **"For us, standardizing on the Dell cyber resilience portfolio was a big win on overall data protection cost savings."**
>
> - Senior Tech Architect, Government Sector

Figure 3. Total Cost to Protect



Source: Omdia

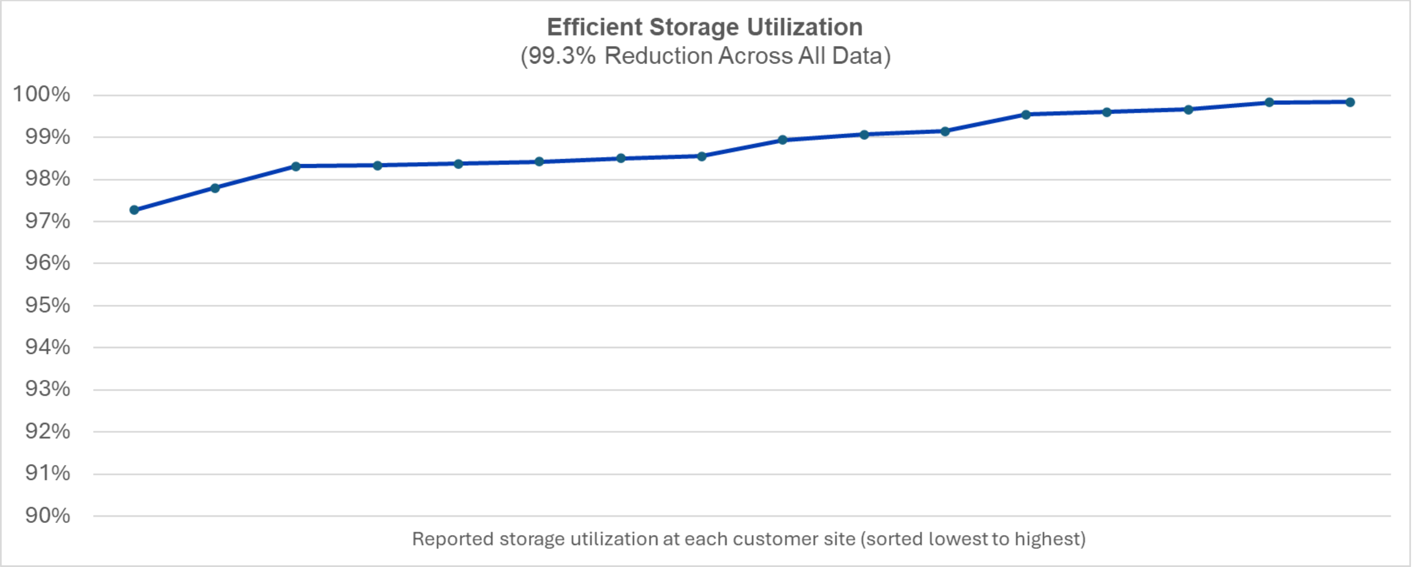
Our analysis of real-world data demonstrates that the Intel-based cyber resilience solutions from Dell are easily capable of serving data resources and services for fractions of a penny per GB per month.

Validated Storage Efficiency

> **"We were expecting good storage efficiency with our new solution, but the results we actually achieved were quite amazing."**
>
> - IT Director, Healthcare Sector

Storage efficiency is a critical part of operating an efficient environment for cyber resilience and represents significant cost savings. Omdia began its exploration of storage efficiency by analyzing 16 backup and recovery environments (across 14 companies) with either Dell backup and recovery software or third-party backup applications, plus Data Domain appliances with advanced hardware-assisted data reduction and compression. This range of data environments needing protection—from 7.6PB up to 758PB of logical data protected—allowed for a regression analysis to determine if data volume is a factor on data reduction. As shown in Figure 4, the data reduction rates are extremely high and range from a low of 97.3% (37:1 data reduction ratio) to a high of 99.84% (637:1 data reduction ratio), with a total across all data of 99.3% (136:1 data reduction ratio). This was calculated by comparing the sum of all physical storage consumed by the sum of all logical data protected rather than averaging each individual result (which results in an average of 98.8%). The customers spanned multiple industries, including technology, manufacturing, insurance, and healthcare. The selection of customers in different industries was designed to capture data reduction results across different types of datasets. Even the customer with the smallest observed data reduction rate of approximately 11:1 could protect almost 1.2 PB of data using just 112 TB of capacity. Figure 4 shows the storage reduction at each of the 16 environments we validated.

Figure 4. Validated Storage Efficiency



Source: Omdia

There is also no pattern to suggest that high or low volumes of data have any effect on data reduction rates. Some organizations with large production environments performed better than others with lower volumes, and, in some cases, small environments outperformed larger ones, suggesting that the type of data is more of a driving factor than the amount of data. Additional efficiencies are also seen over time. Typically, the longer the Dell PowerProtect solution has been receiving data in the environment, the higher the data reduction rate.

Validated Environmental Metrics

We also analyzed the total number of rack units required of the Data Domain systems and the total kW used by Data Domain systems in each customer environment to calculate an average amount of logical protected data per rack unit and the average amount of logical protected data per kW of electricity consumed. Because the system rack space and power consumption are constant regardless of the protected data's capacity, we provided a range. The systems we analyzed were operating between 54% to 78% of total available physical capacity, so we validated both the active logical data currently protected, as well as modeled the maximum amount of logical data that could potentially be protected at 100% capacity. Figure 5 shows that, on average, the deployments were protecting 3.1 to 4.9PB of logical data per rack unit (RU) and 27PB to 43PB of logical data per kW consumed. It should be noted that, based on Dell analysis vs. previous-generation Dell solutions, the highest performing deployments were protecting as much as 10PB/RU and 109PB/kW, and that an Intel-based, all flash Data Domain solution could be capable of using up to 40% less rack space and 80% less power than the HDD-based solutions that we reviewed.

Figure 5. Analysis of Data Domain Footprint and Power Consumption Across Active Deployments

3.1PB to 4.9PB

of protected data per RU

27PB to 43PB

of protected data per kW

Up to an additional 40% less rack space with PowerProtect Data Domain All-Flash[1]

Up to an additional 80% less power with PowerProtect Data Domain All-Flash[1]

Note: Ranges show average of all validated sites at current capacity utilization (typically 54% to 78%) and modeled at 100% capacity utilization. Maximum deployments were as high at 10PB/RU and 109PB/kW.

[1] Based on Dell analysis vs. previous-generation Dell solutions.

Source: Omdia

Beyond Data Reduction: Considerations When Choosing a Cyber Resilience Solution

Our validation shows that the Dell PowerProtect solutions provide significant space efficiency and cost savings, both of which many point solutions claim that their products provide as well. It can be difficult to compare solutions based on vendor claims alone, especially if they are point solutions that only provide one part of the cyber resilience strategy. There are a number of additional factors that customers should consider when comparing cyber resilience solutions between alternatives:

- **Raw storage requirement:** It is important to understand how much raw storage will actually be required to protect an organization's logical data. This is not as simple as the maximum reported compression and data reduction ratio of logical data. Different solutions may require more storage based on technology used for backup data, protection levels, system reserve, replication overhead, block granularity, and determining how much data must be kept to maintain consistency when snaps or backups are moved or deleted. Data Domain has been proven to require at least 2x to 4x less physical storage to protect the same data using the same retention policies.

> **"We get a very good data reduction rate with Dell PowerProtect, which is key for storage of any kind, but especially for backups."**
>
> - Senior Systems Engineer, Healthcare Sector

  - **What happens when increasing retention?** An organization should understand what happens when it chooses to increase its retention of protected data. Data Domain's data reduction technologies make it possible to maintain more copies of data on primary protection storage, increasing cyber resilience by enabling faster recovery from more points in time without greatly increasing storage footprint. In one example assuming a 70%/30% mix of VM file system and SQL database data, less than 14% additional storage is required to double the retention on primary storage from two weeks to four weeks. Using the same assumptions, a competing scale-out solution might require 25% more storage (on top of the 2x-4x more data to begin with) than Data Domain to handle the same increase in retention due to Data Domain's ability to only store small blocks of incremental data and more efficient metadata management.

  - **What happens when protecting backups with immutability?** Data Domain can improve cyber resilience by making all data associated with existing backups immutable (unchangeable) without requiring additional storage capacity, thanks to the native data reduction and immutability built into its architecture. Some alternative offerings that have "bolted-on" immutability can require an additional 2x to 3x more storage when making data immutable since multiple copies must be maintained.

- **Efficient movement of data:** When creating backups and recovering data, information must be moved across the network to and from the backup appliance. Data Domain's DD Boost technology leverages metadata intelligence and source-side data reduction and compression to only send unique and modified data blocks to the appliance to greatly reduce the amount of data that must be sent over the network. This results in significant reduction in network traffic and faster backup and restores.

> **"By using PowerProtect Data Manager, we were able to reduce our exchange backups from four hours to 20 minutes and overall reduce our backup windows significantly."**
>
> - Network Engineering and Operations Supervisor, Utilities Sector

  - **How much data traverses the network during backup and replication?** Data Domain can help reduce bandwidth used by backups and replication by 98% or more. This means that less compute and network resources are required to move data and that backups and replication can complete in up to 98% less time.

  - **How many networking ports are required?** Because far less data must be moved across the network, Data Domain does not require a dedicated backup network and requires fewer dedicated networking connections to effectively move data, as well as reduces or eliminates the need for internal and external networking ports for scale-out nodes, media agents, and management hosts.

  - **How many servers are needed to move data?** Some traditional backup solutions require dedicated media servers that handle data movement, perform software-based data reduction, and index backup data. This not only requires investment in expensive servers or IaaS instances with substantial CPU, memory, and storage capabilities, but each server also requires operational expense to handle deployment, management, and maintenance of the servers. This cost continues to increase over time, especially in scale-out deployments, as server costs rise and servers need to be refreshed.

  - **How fast can you back up and restore data?** The speed at which data can be backed up, replicated, and restored is paramount to an effective cyber resilience strategy. Our validations revealed that Dell customers' backup and restore windows were reduced by 76% (and up to 4x faster restores with an all-flash solution[2]), which can have a major impact on business resiliency and the reliability of the backed-up data. The ability to quickly and safely recover from ransomware attacks is also greatly increased, which can reduce any financial or reputational damage to the company.

  - **How long do disaster recovery operations take?** Cloud Disaster Recovery (CDR) enables enterprises to copy backed-up VMs from their on-prem environments to the public cloud for the orchestration and automation of DR testing. Analysis of CDR revealed up to 85% faster DR recovery times over previous customer DR procedures. Customers also reported up to an 84% reduction in resources and service costs over their previous solutions. A big factor in the reduction was the deduplication of data from the primary data store to the offsite location.

- **Protection and consistency of data?** An effective cyber resilience strategy requires that backup data is consistent and recoverable and remains separated and safe from malicious activities that have breached the network and/or platform.
  - **How do you protect backups against data corruption?** Data Domain's patented Data Invulnerability Architecture provides continuous data validation and self-healing of all backups and data to validate and ensure consistency of 100% of all protected data. Alternative backup solutions can offer some level of data validation, but do not validate 100% of all protected data. Software-only solutions also do not provide nor ensure data consistency once written to a storage target or service. This introduces the possibility of cascading issues, where one piece of corrupt data can unknowingly lead to many backup copies being unrecoverable.

> **"The right technology is critical because our reputation is on the line. Customer data is our key asset. The Dell PowerProtect portfolio ensures it's protected."**
>
> - Finance Sector

  - **How do you protect backups from ransomware and breaches?** Data Domain offers a security hardened 2-copy resilient solution that combines AIOps, Anomaly Detection, Managed Detection and Response for Backup for security configuration and monitoring, ML/AI-enabled anomaly detection, and real-time attack identification across the PowerProtect Portfolio with 24x7 monitoring and response. For mission-critical workloads, protection can be further enhanced with a Cyber Recovery Vault and CyberSense analytics, ensuring robust defense and recovery from evolving cyber threats.

> **"We had a cyber incident two years ago. We had a big virtual environment where we backed up a lot of central files to the virtual environment, which we lost. [With Dell PowerProtect Backup Services], I don't lose sleep anymore about whether [we have] people's data backed up."**
>
> - IT Director, Automotive Sector

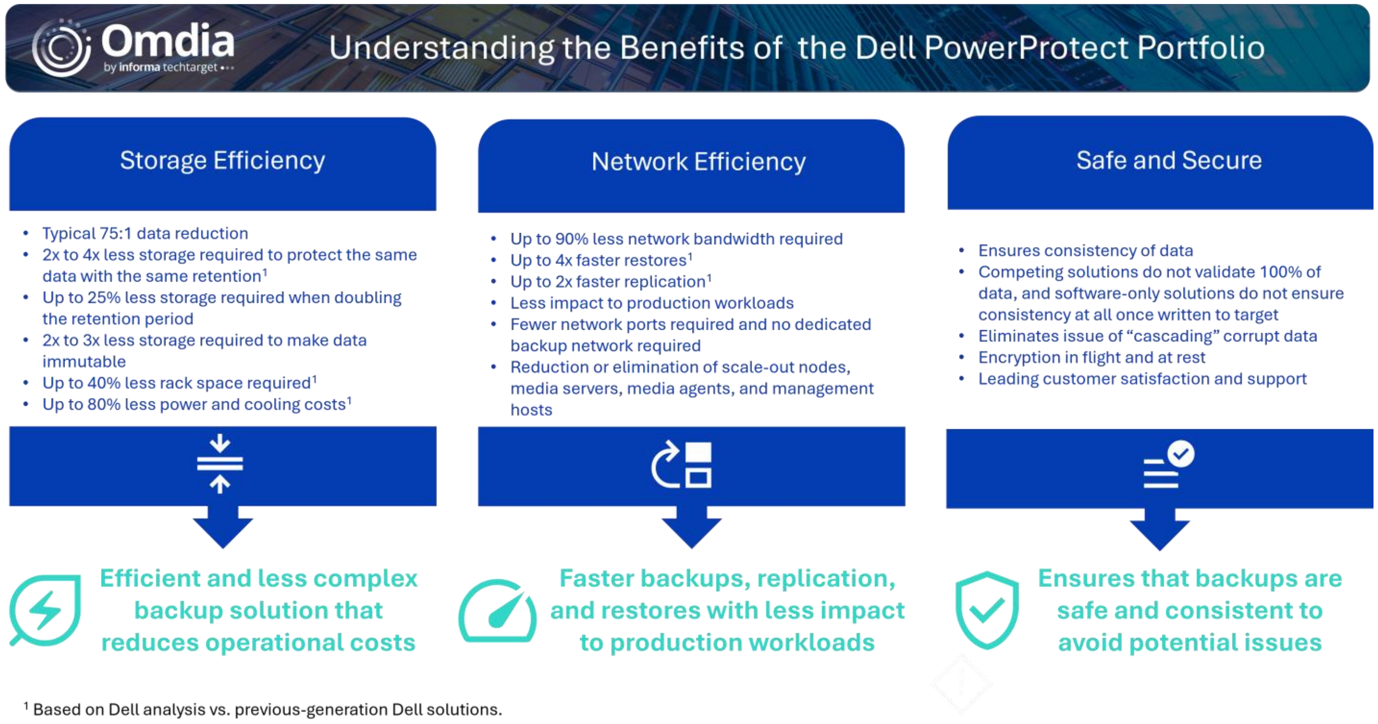
- **What are the ongoing operational costs associated with operating the solution?** Organizations must consider the total cost to operate the solution beyond the investment in hardware and licenses. This includes the cost of time and effort spent by IT teams as well as the environmental costs of operating the physical hardware.

> **"Dell PowerProtect has been rock solid, it is cost efficient and cost effective."**
>
> - Senior Systems Engineer, Healthcare Sector

  - **What are the environmental costs and impact?** Deploying less physical storage to protect data, as well as fewer additional compute, memory, storage, and networking resources to scale out and move data results in a smaller physical footprint and a more energy-efficient solution. The cost of power, cooling, and floorspace is generally thought of as a shared expense and not considered in the overall cost of backup solutions, but one alternative solution's customer claimed that up to 60% of the power consumed in their data center was consumed by their backup infrastructure. Data Domain solutions can reduce footprint by 40% to 80% and can require up to 80% less power and cooling costs when compared with previous-generation Dell models. With rising backup capacity requirements and energy costs, this becomes a very important consideration.

- **How much effort is required to manage the solution?** The time and effort required to deploy, manage, and maintain all hardware (servers, network, and storage), as well as ensure data consistency, security, and governance, is an important consideration. With less hardware and software to maintain, integration with other backup solutions, and AI-powered visibility into the backup environment, Dell PowerProtect solutions require less time and effort from IT infrastructure teams and backup administrators. We validated that the Dell solution can reduce operational costs by 25% to 33% through automation, integration, reduced complexity, and improved efficiency. Dell managed services like MDR and Incident Response and Recovery help organizations improve detection and response capabilities while offloading the burden from security and backup teams.
- **How much more operational overhead and expense are required if tiering is necessary?** Many alternative solutions represent only one tier or aspect of the overall backup solution and, thus, do not focus on costs outside of their core solution. It is important to consider all costs associated with cyber resilience across all tiers of the backup strategy, especially cloud costs. This goes beyond simple $/GB/month and can include costs such as cloud connectivity, storage transactions, and restore egress costs.

Figure 6. Summary Of Validated Benefits Provided by Dell PowerProtect



Omdia by informa techtarget

Understanding the Benefits of the Dell PowerProtect Portfolio

Storage Efficiency

- Typical 75:1 data reduction
- 2x to 4x less storage required to protect the same data with the same retention[1]
- Up to 25% less storage required when doubling the retention period
- 2x to 3x less storage required to make data immutable
- Up to 40% less rack space required[1]
- Up to 80% less power and cooling costs[1]

Efficient and less complex backup solution that reduces operational costs

Network Efficiency

- Up to 90% less network bandwidth required
- Up to 4x faster restores[1]
- Up to 2x faster replication[1]
- Less impact to production workloads
- Fewer network ports required and no dedicated backup network required
- Reduction or elimination of scale-out nodes, media servers, media agents, and management hosts

Faster backups, replication, and restores with less impact to production workloads

Safe and Secure

- Ensures consistency of data
- Competing solutions do not validate 100% of data, and software-only solutions do not ensure consistency at all once written to target
- Eliminates issue of "cascading" corrupt data
- Encryption in flight and at rest
- Leading customer satisfaction and support

Ensures that backups are safe and consistent to avoid potential issues

[1] Based on Dell analysis vs. previous-generation Dell solutions.

Source: Omdia

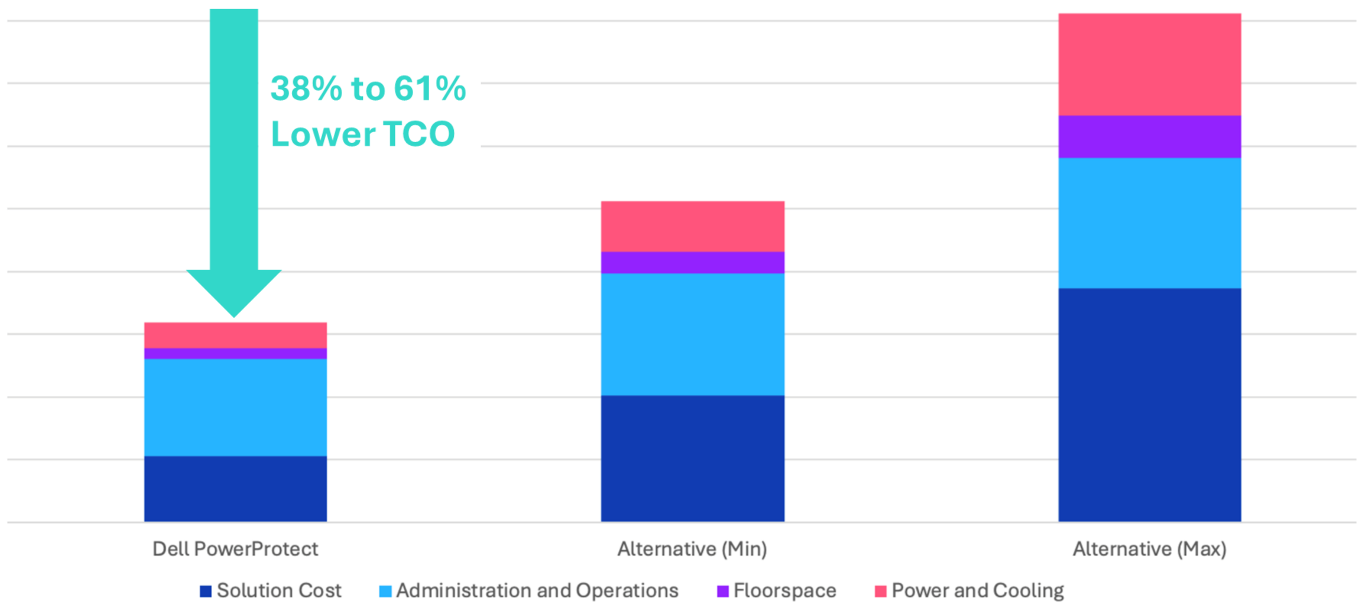
3-year Total Cost of Ownership Model

Omdia leveraged the information collected through vendor-provided material, public and industry knowledge of economics and technologies, and customer case studies to create a simple three-year total-cost-to-protect model. The model compared the costs and benefits of protecting the same environment with the

Intel-powered Dell PowerProtect solution instead of alternative backup solutions. Omdia's analysis of the 15 real customer environments protected with Data Domain, combined with experience and expertise in economic modeling and technical validation of Dell and alternative technologies, helped to form the basis for our modeled scenario.

Our model assumed that an organization protected a total of 200PB of logical capacity with an initial retention period of two weeks, which was then increased to four weeks, as well as 20% of the most important backups made immutable for added protection. For simplicity, we estimated an equal acquisition cost per physical GB required. We leveraged the known ranges of data efficiency, power consumption and rack space, and administration effort validated in the real-world scenarios to estimate the required Dell capacity and costs. We then applied the known ranges of Dell advantages versus alternative solutions described in the earlier sections of this report and summarized in Figure 7 to model a minimum and maximum range of costs associated with alternative solutions. This included a conservative 2x-4x more physical storage required per protected PB, 25% more storage required when doubling the retention period, and 2x-3x more storage required to enable immutability. We assumed equivalent density and power consumption per physical PB required (conservative) and an additional 25% to 33% effort for hardware, software, and backup administration. **Our models predicted that the Dell PowerProtect solution could protect the organization for a 38% to 61% lower total cost over the three-year timeframe.**

Figure 7. Omdia's Modeled 3-year Total Cost to Protect 200PB of Logical Data With PowerProtect



Source: Omdia

Considerations

Omdia's models are built in good faith upon conservative, credible, and validated assumptions; however, no single modeled scenario will ever represent every potential environment. Each organization has a unique set of challenges that they must overcome and opportunities that can be achieved through their own cyber resilience environment. The benefits received by an organization depend on the size of the organization, the nature of the business, and the current capabilities, characteristics, and composition of their IT organization, along with many more variables. Omdia recommends that you perform your own analysis of available products and consult with your Dell representative to understand and discuss the differences between the solutions through your own proof-of-concept testing.

Conclusion

The top cyber resilience priorities for IT and security leaders increasingly focus on strengthening data security, improving operational readiness, and enabling consistent recovery across complex enterprise environments. At the same time, organizations face rising ransomware risk, expanding regulatory and compliance requirements, and growing infrastructure and cloud costs that consume a larger share of annual IT budgets. The central challenge lies in enabling organizations to extract value from rapidly expanding data estates while protecting critical data and recovery systems that continue to grow in scale and complexity. These challenges are closely interconnected and, as demonstrated by customer experience, can be addressed through an integrated cyber resilience approach built on secure data foundations, efficient backup infrastructure, and orchestrated recovery capabilities.

Omdia reviewed and validated the benefits of Dell PowerProtect cyber resilience solutions using existing customer interviews, documented case studies, and updated performance and operational metrics reported across customer deployments. The evidence shows a shift from reactive recovery practices to more proactive, predictable operations, enabled by improved visibility, automation, and consistency across backup and recovery environments. Updated metrics demonstrate substantial gains in storage efficiency driven by advanced data reduction (**99.3% reduction across all validated deployments, with 2x to 4x less storage required**), reductions in administrative effort through simplified management (**25% reduction**), and measurable improvements in backup and restore performance that translate into shorter recovery windows and improved operational agility (**76% faster backup windows**, up to **4x faster restores, 2x faster replication**, and **85% faster DR recovery**). Additional benefits include the ability to extend cyber resilience capabilities across on-premises, hybrid, and cloud environments, including cloud-based disaster recovery and long-term retention, resulting in reduced recovery-related resource requirements, faster recovery times, lower infrastructure overhead, reduced operational complexity, and decreased exposure to downtime and data loss over time. Our 3-year model based on the results of our validation predicted that a Dell

Quantified Impact Across Cyber Resilience:

Storage & Infrastructure

- 99.3% data reduction[3]
- 2x-4x less storage required[2]

Operational Efficiency

- 25% reduction in admin effort[3]

Performance & Recovery

- 75% faster backups[2]
- Up to 4x faster restores[2]
- 2x faster replication[2]
- 85% faster DR recovery[2]

Financial Impact

- 38%-61% lower 3-year total cost to protect[4]

[3] Validated by Omdia across Dell customer deployments.
[4] Modeled by Omdia vs. alternative solutions.

PowerProtect solution using Intel Xeon processors can **lower the 3-year expected total cost to protect by 38% to 61%.**

Organizations seeking to modernize their cyber resilience capabilities may benefit from evaluating a comprehensive platform that integrates secure data foundations, threat detection, and recovery across modern environments. The Dell PowerProtect portfolio provides a broad set of capabilities to support these objectives and warrants consideration as organizations assess options to strengthen recovery readiness and operational resilience.

Get in touch: www.omdia.com askananalyst@omdia.com