Enterprise Strategy Group by TechTarget

SHOWCASE

APRIL 2024

Building the Foundation for Cyber Resilience with Dell PowerProtect Data Domain Appliances

Christophe Bertrand, Practice Director

Abstract: Amidst frequent ransomware attacks that often lead to significant data and financial losses, modern digital organizations must reevaluate their data protection and disaster recovery strategies to mitigate risk. It is crucial to recognize that we are now in the era of cyber resilience. To meet new challenges, businesses must establish or upgrade their data recovery infrastructure to support strict security and recovery service levels. This should be done while also providing comprehensive and integrated capabilities at scale. The PowerProtect Data Domain family of protection storage appliances from Dell Technologies can help achieve these objectives efficiently.

Market Landscape

In today's age of accelerating digital transformation and IT complexity, ransomware has become an alarming and prevalent issue that most organizations have encountered within the last 12 months.[1] Whether the attack was successful or not, the reality is that it's not a matter of if an attack will occur but rather when it will occur.

The situation is bleak, as ransomware is reported to be an existential threat to organizations, with 65% of respondents to a research survey by TechTarget's Enterprise Strategy Group identifying it as one of the top three most critical risks to their organization's viability (see Figure 1).

When a ransomware attack occurs and is successful, the primary objective is to recover the data and minimize the losses. Unfortunately, only 16% of respondents reported being able to fully restore their data after experiencing a successful ransomware attack, with most organizations believing they can fully recover their data and resume operations within a week. This is in sharp contrast with traditional recovery SLAs of a few hours, despite organizations' best efforts at practices like proactive recovery testing.

Adding to the complexity and risk of the situation, 29% of IT leaders are very concerned that their organization's data protection copies could also become infected or corrupted by ransomware attacks. If there are no backups, there can be no recoveries!

This is driving investments in both cybersecurity and data protection: 68% of organizations reported that they are planning to increase their spending on cybersecurity in 2024, and 49% reported that they plan on increasing their spending on data protection.[2]

Not surprisingly, cybersecurity and disaster recovery rank amongst the top 10 most common broad technology initiatives that have become significantly more important to an organization's future over the past two years. In

[1] Source: Source: Enterprise Strategy Group Research Report, *Ransomware Preparedness: Lighting the Way to Readiness and Mitigation*, December 2023. All Enterprise Strategy Group research references and charts in this showcase are from this report unless otherwise noted.

[2] Source: Enterprise Strategy Group Research Report, *2024 Technology Spending Intentions Survey*, February 2024.

This Enterprise Strategy Group Showcase was commissioned by Dell Technologies and is distributed under license from TechTarget, Inc.

addition, 40% of respondents plan to make the most significant data protection investments in 2024 in disaster recovery, followed by 35% in cyber-resilience solutions and 34% in ransomware protection.[3]

Figure 1. Ransomware Is a Top Threat to Organizations' Viability

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Advancing Cyber Resilience Maturity

Disaster Recovery or Cyber Resilience?

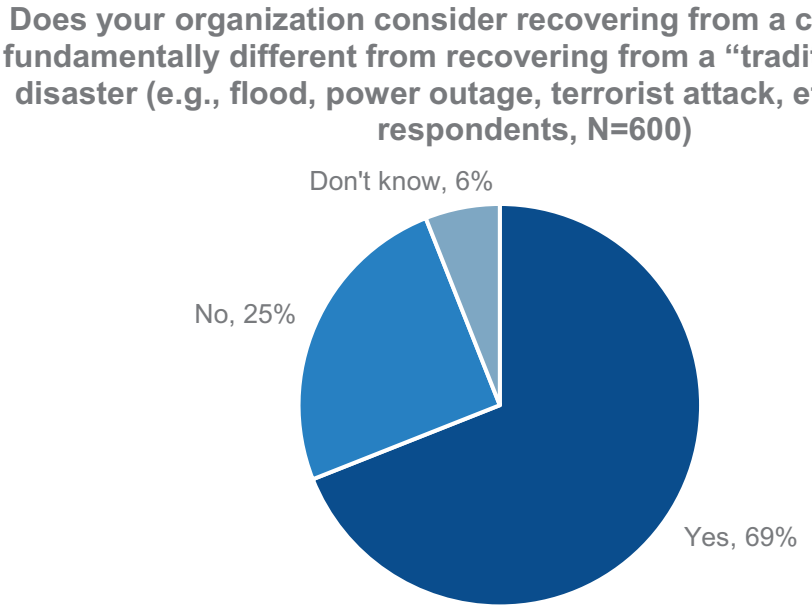
While ransomware is considered a crisis, as are other types of cyber disasters, it exhibits different characteristics for many, affecting multiple processes, KPIs, and teams (see Figure 2). IT leaders have identified that recovering from a cyber event is different from a "traditional" outage or disaster because it:

- Involves different technologies/features (cited by 56% of respondents).
- Involves different processes/workflows (53%).
- Is more complex (53%).
- Involves different personnel/skill sets (50%).
- Involves different SLAs (45%).
- Takes more time (41%).

As cyberthreats continue to evolve, Enterprise Strategy Group research shows that it has become increasingly important to recognize the fundamental differences in IT strategies to secure critical data assets. Employing updated and innovative approaches and revisiting current platforms, teams, and processes to safeguard against these ever-changing threats is key.

[3] Ibid.

Figure 2. Recovering From Ransomware Is Fundamentally Different



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Key Capabilities

When considering the technology and features currently needed in the market, it is essential to consider the wide range of capabilities required across multiple disciplines. The most desired ransomware recovery capabilities among IT professionals are closely related to backup and recovery infrastructure. The focus is mainly on protection and recovery features that can help mitigate the damage caused by ransomware attacks. Such solutions should provide comprehensive protection and recovery capabilities across all systems, applications, and data types.

Key considerations include:

- Protected/Immutable data copies/backups.
- Data encryption (at rest and/or in flight).
- AI-based[4] ability to detect ransomware in data copies/backups.
- Ability to recover from air-gapped/isolated protection storage.
- Integrated data protection mechanisms within the platform.
- Integration with ransomware detection or resolution capability.
- Integrated cloud services capabilities.
- Ability to recover to any point or location.
- Ability to protect virtual machines.
- Integrated storage capabilities.

[4] Source: Enterprise Strategy Group Complete Survey Results, *Reinventing Backup and Recovery With AI and Machine Learning*, April 2024.

In addition to backup and recovery infrastructure, IT professionals also seek solutions that can help them identify vulnerabilities and security gaps in their systems. These solutions should provide real-time monitoring capabilities and alerts to help organizations respond quickly to potential threats. Other critical capabilities include secure data storage and secure access controls to prevent unauthorized access to sensitive information.

The PowerProtect Data Domain Difference

Data Domain has a longstanding reputation as a reliable backup appliance that safeguards data in on-premises and multi-cloud environments. The appliances help advance cyber resilience maturity with multiple layers of Zero Trust security.

Data Domain target storage appliances are specifically designed and optimized for data protection—with performance, efficiency, and security advantages that simplify operations, reduce risk, and lower costs. The appliances also benefit from a broad partner and backup software ecosystem, which means that they can easily integrate into existing data protection environments.

According to Dell, the latest iteration of Data Domain is characterized by faster backups and restores, significant data reduction, and increased efficiency, requiring less power, floor, and rack space. These benefits translate into a lower cost of data protection.

Key Capabilities for Cyber Resiliency

Data Domain customers can get end-to-end resilience wherever their data lives for traditional and modern workloads, whether on premises or in multi-cloud environments. Cybersecurity is built into the Data Domain framework by completely controlling the hardware and software supply chain.

- The appliances deliver multiple layers of Zero Trust security, helping ensure the integrity and recoverability of data with capabilities like Hardware Root of Trust and Secure Boot, encryption, retention lock, role-based access control, and multifactor authentication. In addition, Data Domain can be deployed in an isolated cyber recovery vault with independent management controls for tighter security. The vault is not an additional data center but rather a secure storage environment located at the production or corporate data center, in the public cloud, or with a third-party solution provider.
- The appliances are also designed to scale for performance and efficiency by leveraging advanced deduplication to deliver a cost advantage.[5] Dell highlights that Data Domain appliances typically result in significant data reduction, improved backup and restore performance, and a better environmental and data center footprint requiring less power and floor space. In addition, DD Boost is a patented technology that enables deduplication to happen at the source, minimizing the amount of data that needs to be backed up. Deduplication is done at the micro level, delivering a more fine-tuned result.
- In support of a strong cyber-resiliency approach, Data Domain appliances are built with a CPU-centric architecture, with Intel® Xeon® scalable processors. CPU and memory access is orders of magnitude faster than primary storage, including flash.
- Data Domain is backup software agnostic. It integrates easily with existing infrastructures, enabling ease-of-use with leading backup applications, and offers significant performance in conjunction with Dell PowerProtect Data Manager.
- DD Replicator provides automated, policy-based, network-efficient, and encrypted replication for disaster recovery and multi-site backup and archive consolidation.
- Through unique integration and development work with VMware by Broadcom, Transparent Snapshots offers significant benefits to backup performance and costs, simplified management, reduced risk of data loss, and

[5] Source: Enterprise Strategy Group, Economic Validation commissioned by Dell, *Analyzing the Economic and Operational Benefits of the Dell Data Protection Portfolio*, November 2022

improved recovery performance, which is vital in ransomware recovery. Storage Direct Protection also delivers performance and simplified management via integration with Dell storage including PowerStore and PowerMax.

- IT leaders face increasing complexity in their management responsibilities, making effective management a priority, especially in the face of cyberthreats. Solutions such as Data Domain Management Center and CloudIQ are available to simplify the process.
- Data Domain is also available as software-defined protection storage on premises using PowerProtect DD Virtual Edition (DDVE) and in the cloud with Dell APEX Protection Storage. These solutions are designed with operational efficiency and ease of deployment in mind, can be deployed on premises on any standard hardware (converged or hyperconverged), and run in VMware vSphere, Microsoft Hyper-V, and KVM
- APEX Protection Storage is a virtual appliance with Data Domain DNA. It increases transactional and operational efficiencies and provides significant cost savings by providing the ability to write data or backup into the cloud object storage directly.

Conclusion

Organizations must acknowledge that relying solely on traditional disaster recovery methods is inadequate for safeguarding critical assets against cyberthreats like ransomware. The intricacies of these attacks demand a more robust and proactive approach to security.

It is also essential to note that there is no “one-size-fits-all” solution for ransomware recovery. Instead, a combination of platforms, services, and an ecosystem of technologies and vendors must be pulled together to create integrated solutions that meet organizations' diverse needs.

This era of cyber-recoverability presents a significant opportunity for vendors in the cybersecurity and data protection space to differentiate their products and services. Vendors can help businesses feel more secure and confident in handling cyberthreats by offering innovative solutions that prioritize data recovery and protection.

That’s where the PowerProtect Data Domain protection storage appliance from Dell can make a difference and become a foundational component of modern cyber resilience because of its breadth and depth of capabilities, inherent security-focused design for hardware and software, and cyber vault solution. It also meets modern online consumption expectations, such as subscription licensing, and offers a future-proof guarantee program.

IT and cybersecurity professionals should evaluate the Data Domain protection storage appliance to better prepare for the inevitable onslaught of ransomware.

[6] Source: Enterprise Strategy Group Showcase, *Protecting VM Backup at Scale With Dell Technologies*, February 2024.

About Enterprise Strategy Group
TechTarget’s Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com