ESG SHOWCASE

Cyber-resilience Is Essential for Mission-critical Storage

Date: October 2022 **Authors:** Scott Sinclair, Practice Director; and Monya Keane, Senior Research Analyst

ABSTRACT: The IT landscape has changed. Because data is such a high-value asset now, cyber-threats have also become pervasive. Cyber-resilience must, therefore, be a core tenet when choosing mission-critical storage. With PowerMax, Dell Technologies has further established itself as a leader in mission-critical storage by building and integrating essential cyber-resiliency capabilities directly into these systems.

Overview

Data is a vital, highly valuable business asset. ESG research shows that 59% of surveyed organizations identify data as essentially being their business, and that percentage is expected to increase to 81% in two years.[1] The role of a mission-critical storage infrastructure is to preserve, protect, and deliver data that underpins workloads and apps that simply cannot go down, ever.

For decades, deploying "mission-critical storage" was synonymous with providing requisite performance and scale, while also ensuring always-on availability to protect against component failures, site failures, user errors, and natural disasters. Now, malicious attacks are increasing in prevalence. The core tenets of mission-critical storage, thus, must evolve beyond those traditional capabilities to include improving an organization's cyber-resiliency posture as well.

Dell Technologies, a leader in enterprise storage, continues to evolve its flagship storage platform—PowerMax—to meet the mission-critical needs of the most demanding IT environments. Dell's recent innovation efforts have centered on imbuing the PowerMax line with a series of robust features to improve the cyber-resiliency posture of any organization that is interested in better protecting its data and vital applications, preserving its brand reputation, and achieving long-term success.

The Era of Ever-present Cyber-threats to Data

Along with the increase in cyber-threats, IT complexity has also increased. Nearly half (46%) of ESG survey respondents say IT is more complex today than it was two years ago. The rapid evolution of the cybersecurity landscape (cited by 37%) and efforts to adhere to new data security and privacy regulations (cited by 32%) were two of the most commonly identified drivers of that IT complexity.[2]

Unfortunately, organizations are currently struggling to hire enough skilled cybersecurity talent to prevail over that complexity head on. Forty-eight percent of surveyed organizations report that they don't have enough cybersecurity specialists on staff—it is the most-often-cited skills shortage area in enterprise IT right now.[3]

[1] Source: ESG Research Report, *Data Infrastructure Trends*, November 2021.
[2] Source: ESG Complete Survey Results, *2022 Technology Spending Intentions Survey*, November 2021.
[3] Ibid.

Ransomware and Malware Are Prevalent

Among the multiple threats businesses face, external ransomware and malware attacks have become practically inescapable. In a recent ESG research survey of IT and cybersecurity professionals overseeing technologies and processes associated with protecting their companies against ransomware, 79% reported experiencing an attempted ransomware attack within the last 12 months. And 30% of those respondents said those attacks are occurring weekly or even more frequently.[4]

Among organizations that have experienced an attempted attack, 73% experienced at least one that succeeded. However, in these circumstances, payment of a ransom is not an optimal or even somewhat smart strategy. 56% of organizations victimized by a successful attack paid. However, of those who paid the demanded ransom:

- **87%** of them then experienced additional extortion attempts for more money. In fact, 61% of those who paid initially ultimately ended up paying even more money later.[5]
- Only **14%** got 100% of their data back, even after sending the ransom money.
- And **61%** got only 75% or less of their data back after paying.

Clearly, full-fledged ransomware protection requires a more multi-faceted strategy—one that incorporates multiple technologies and tools focused on detection, prevention, and recovery.

Many organizations are now modeling their cyber-resilience strategies after guidance provided by the NIST Cybersecurity Framework, which recommends that organizations identify critical resources, protect those resources, detect failures and breaches, and plan for response and recovery from cyber-incidents. Another component of the NIST framework that organizations are embracing widely is the zero trust architecture, which dismisses the concept of a protective network edge in favor of a "never trust; always verify" philosophy. In this model, the security configuration of users (even people working inside the organization) must be repeatedly and routinely validated before those users can access applications/data.

Storage systems absolutely must be a part of this cybersecurity approach. After all, the most common infrastructure component targeted by ransomware attacks is storage hardware, according to ESG research. It was the top response—cited by 40% of respondents.

How Mission-critical Storage Improves Ransomware Resiliency

Ransomware attacks center on accessing, and then encrypting, important business data. Many cyber-resiliency strategies are built upon tools and technologies that focus on the **prevention** of threats by keeping them out and the early **detection** of any attacks that do make it through. But with ransomware, it is important to focus on **accelerated recovery**, too.

Mission-critical storage systems reside in a spot in the data path that is prime for assisting in rapid recovery of data after an attack occurs. For example, as successful ransomware attacks have increased, some storage systems have been able to leverage capabilities engineered into them to assist in rapid recovery by safekeeping and then serving up secure and immutable data volume copies.

[4] Source: ESG Research Report, *The Long Road Ahead to Ransomware Preparedness*, June 2022. All ESG research references in this showcase have been taken from this research report unless otherwise noted.
[5] Source: ESG Complete Survey Results, *The Long Road Ahead to Ransomware Preparedness*, June 2022.

That kind of support is incredibly valuable in accelerating recovery. Snapshots can quickly be identified as "known good" volumes and be recovered quickly by IT to restore data sets to their prior pristine condition. However, for mission-critical application environments, *storage technology must do even more*.

Dell PowerMax Can Improve an Organization's Cyber-resiliency Posture

Product names have changed and capabilities have grown over the decades, but Dell Technologies' mission-critical infrastructure storage systems have led this space since enterprise storage was established as a separate category of IT by EMC in the late 1980s. Today, Dell PowerMax offers multiple capabilities designed to meet mission-critical workloads' intensive requirements, including:

- An all-NVMe, multi-controller scale-out architecture for extreme, consistent performance at scale.
- Massive workload consolidation, with support for diverse block and file application environments encompassing mainframe workloads, bare-metal systems, VMs, containers, and more.
- The highest levels of security, availability, and resiliency. PowerMax provides 99.9999% availability with end-to-end data encryption from hosts to PowerMax, data-at-rest encryption, and secure snapshots—specifically, it supports up to *64 million snapshots per array*, according to Dell. Additionally, Dell's Symmetrix Remote Data Facility (SRDF) disaster recovery software uses advanced topologies and automation features to provide a strong foundation for resiliency. With SRDF, organizations can even create an air-gapped vault. Within that vault, data is isolated, and the connection to the vault is intermittent and highly restricted.

Dell Has Architected PowerMax for Resilience

Recently, Dell has concentrated on building and incorporating even more security features into PowerMax. For example, PowerMax is now designed for zero trust security environments based on Dell's seven pillars of zero trust, including intrinsically securing/protecting the system itself from attacks through:

- Immutable hardware root of trust capabilities—These capabilities authenticate hardware and software changes across nodes, media enclosures, and the control station. Embedded, immutable, component-level cryptographic keys are physically fused into the memory by Dell Manufacturing.
- Secure boot chain of trust capabilities—These capabilities establish and extend a firmware "chain of trust" against malicious boot, kernel, and driver rootkits. Secure boot chain of trust uses cryptographic authentication for subsequent firmware loads/boot loaders based on Dell signatures.
- Digitally signed firmware updates—PowerMax also leverages Dell's digital signature authentication to protect against unauthorized firmware updates. It performs node, media, and control station component scans using cryptographic authentication keys.

On top of this trustworthy design, PowerMax offers additional capabilities to improve the prevention, detection, and recovery from ransomware attacks and other cybersecurity threats.

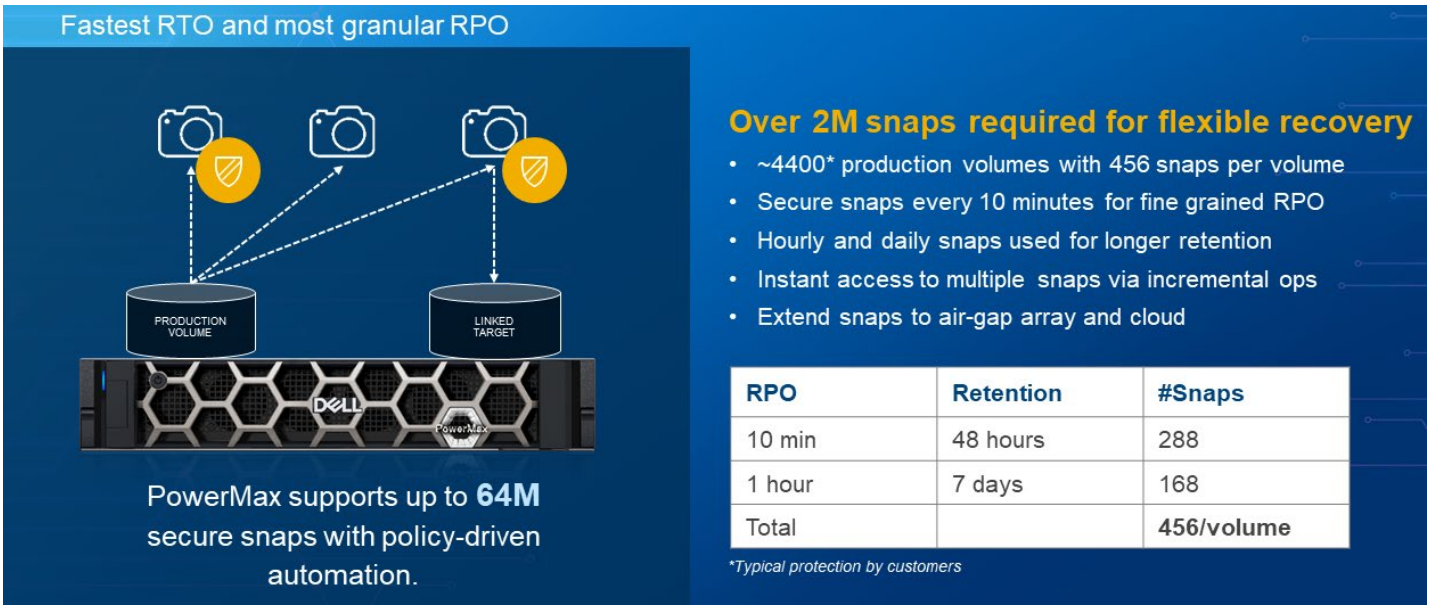
For prevention, in addition to possessing built-in hardware security, PowerMax helps prevent attacks with its advanced security for preventing unauthorized user access—featuring Common Criteria, STIG Hardening/APL, FIPS 140 certified security certifications, and support for trusted admin access control mechanisms, such as:

- SecurID multi-factor authentication to verify an administrator's identity.
- CAC/PIV smartcard support containing a certificate/private key to gain access to online resources within the U.S. federal government.
- Role-based access controls (RBAC), LDAP support, and zDP 2 Actor (requiring two people to execute certain zDP commands), allowing only authorized users to perform designated operations such as provisioning storage.

For detection, both PowerMax hardware and Dell CloudIQ AI software offer malware anomaly detection. This is compliance alerting based on cybersecurity alerting protocols, along with secure syslog alerts and exports. Specifically, CloudIQ quickly detects cyber-attacks by monitoring unusual PowerMax storage utilization and suspicious activity metrics. It then alerts admins to any drastic changes due to possible encryption. It can also continuously monitor storage infrastructure to automatically identify cybersecurity risks from misconfigured system settings and then provide detailed recommendations to correct those issues.

And for recovery, PowerMax secure snapshots technology has brought data security and protection to the next level. Depending on the business's service level objectives, IT can configure up to 64 million snapshot copies on each PowerMax (see Figure 1).

Figure 1. How PowerMax Supports Fast Cyber Recovery



Source: Dell Technologies

This capability allows PowerMax to support recovery point objectives (RPOs) of as little as a few minutes before an attack succeeded. And with support for that many snapshots, IT will have sufficient copies to protect even large, consolidated mission-critical storage environments practically to the minute, thereby, achieving almost instant recovery of mission-critical applications. This level of protection flexibility is game changing for production environments at scale. According to Dell, PowerMax offers the most granular cyber recovery at scale to optimize RPO.

Dell can also add a PowerMax cyber recovery vault option for organizations requiring a remote-vault air-gap recovery option (SRDF), with orchestrated vaulting/recovery for open systems and mainframe storage alike. The PowerMax cyber recovery vault offering will be generally available later this month and uses SRDF remote replication to create an air gap. This solution is designed for customers that require a copy of data outside of their production network with fast recovery

(RTO). While PowerMax customers have been deploying this configuration manually for a while, this month's announcement incorporates deployment orchestration automation and Dell professional services to streamline installation.

The Bigger Truth

Dell isn't usually the first name that comes to mind when people think about security vendors. That perception needs to change. Malicious attackers are becoming more organized, and their threats are more sophisticated. Dell has made and is continuing to make significant investments to help counter these threats, protect data, and make the entire management of security and resilience simpler.

Data is an organization's most critical asset. It's got to be protected. It's got to be always available. The latest threat to that availability is ransomware, malware, and other cyber-attacks. Yes, PowerMax has a strong lineage in supporting high-end, mission-critical workloads. Dell's been doing it for years, but the new features of PowerMax are particularly applicable to just about every storage buyer today. Everyone is worried about ransomware, malware, and being the next news headline.

And it's not about combatting thieves who are trying to get rich. Those hackers just may work for a foreign government, stealing intellectual property to bolster their own national security or military strength. If they can encrypt your data, beyond taking away your access to it—there's no telling what else they can do with it then.

If you have business information that you absolutely cannot let the bad guys get their hands on, you'll want to have a conversation with Dell about the proper way to protect a storage infrastructure.

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com contact@esg-global.com 508.482.0188