Dell cybersecurity resonates above the competition

By Andrew Glinka, Vice President of Competitive Intelligence, Dell Technologies | Oct. 2022

Expanding digital footprints and evolving digital priorities such as remote work and business processes running in the cloud have made companies and governments vulnerable to cyber-attacks. Technology providers have been stepping up their efforts to advance cybersecurity capabilities to address escalating threats. Messaging has become a cacophony of cybersecurity terms and references with loose understandings and much confusion, all while cyber-criminals continue to penetrate networks, applications, and data.

Those tasked with protecting their organization's digital assets simply want to trust that their technology is going the extra mile to help them keep their company safer. That's where Dell Technologies resonates above the prevailing clamor. When it comes to cybersecurity, Dell goes above and beyond the competition.

Dell has the world's most cyber-secure scale-out NAS[1] and object storage.[2]

Some of the fastest-growing and most vulnerable digital assets exist in the form of unstructured data, which is stored as files, objects, and streams. Most unstructured data competitors focus their cybersecurity capabilities on snapshot-based recovery strategies that assume some level of data loss. More advanced competitors may provide capabilities for early cyber-attack detection using filesystem auditing and API integration with more robust cyber-security solutions to help minimize data loss. With Dell PowerScale scale-out NAS and ECS object storage platforms, organizations can trust Dell to help them keep their unstructured data safer than competitors in three ways:

- More expansive and vigorous multi-vector analytics, which include network, storage, IDS, perimeter, and endpoint analytics to help detect attacks more quickly and successfully
- More intelligent automated responses to early-warning anomalies, which include locking out malicious actors, triggering immutable snapshot copies, and turning on/off replication to a remote cyber-vault to help thwart attacks faster and protect data more effectively
- More advanced recovery mechanisms, including smart operational airgap technology, to help speed up recovery and prevent data loss

Organizations that rely on less resilient unstructured data solutions may not have the ability to thwart an attack as effectively or recover as quickly, leading to greater data loss and longer system outages.

Dell has the world's most cyber-secure mission-critical storage.[3]

While storage array competitors may have some pieces of the puzzle when it comes to cybersecurity, Dell's more comprehensive approach to protection, detection, and recovery with PowerMax can help organizations have greater confidence in deploying highly resilient mission-critical storage that is less susceptible to cyber-attacks. Based on the National Institute of Standards and Technology (NIST) framework, PowerMax's Zero Trust architecture is differentiated in important ways:

- PowerMax's silicon-based Hardware Root of Trust and multi-factor authentication help to ensure that the array and users can be trusted.
- PowerMax and CloudIQ Cybersecurity software enable storage administrators to define compliance-based configurations, monitor the system, and receive alerts if the array is out of compliance. CloudIQ Cybersecurity can also detect anomalies, including changes to data reduction rates, to alert administrators to a cyber-attack to take quick action.
- PowerMax's massive snapshot scalability of up to 65 million snapshots helps to speed recovery and minimize data loss with the most granular cyber-recovery at scale.[4]

Organizations relying on storage arrays with less robust hardware security are more vulnerable to malicious access. Arrays with less capable monitoring and analytics software can be more vulnerable to malicious intrusion. Arrays with less granular snapshot capabilities can lead to recoveries with significant data loss.

Dell has the world's most cyber-secure commercial PCs.[5]

Dell employs software-based protection above the operating system (OS) and hardware-based defenses below the OS to help harden Latitude, OptiPlex, and Precision client systems against cyber-attacks. With these PCs, organizations can trust Dell to help them protect BIOS and firmware layers, user access, and authentication integrity with a richer set of hardware-based protection features than competitors offer, for example:

- Dell's Off-host BIOS Verification function uses a secure cloud environment to conduct a point-in-time check for the integrity of the BIOS. Dell's BIOS Image Capture automation captures the BIOS image for forensic analysis if the BIOS appears compromised. Dell's BIOS Indicators of Attack (IoA) analytics help to identify attacks and alert IT administrators of any issues.

- Dell SafeID with ControlVault firmware mechanisms provide user authentication integrity by securely storing and processing advanced user authentication credentials in a dedicated security chip.
- Dell Secured Component Verification allows customers to verify that Dell commercial PCs and key components have arrived as they were ordered and built.[6]
- To enable cybersecurity hardening around the Intel Management Engine, Dell provides a unique off-host firmware check against a golden copy to verify that malicious actors have not compromised the firmware.

Without these advanced layers of protection, end users are more vulnerable to hidden attacks and less equipped to recover quickly.

World's most cyber-secure vSAN HCI system with inclusive and available data protection services from a single vendor.[7]

Proper management of software updates is vital to secure infrastructure operations. VxRail Manager, which is natively integrated into vCenter, notifies administrators when updates are available and offers a streamlined and automated approach to upgrading without disrupting operations. In addition, joint engineering with VMware enables a seamless Hyper-Converged Infrastructure (HCI) experience, consistent management, and committed 30-day synchronous releases of new VMware updates. With more than 100 staff dedicated to system and ecosystem testing of over 6,000 unique tests, and up to 800,000 test hours per release utilizing automated, unique test frameworks for VxRail, Dell minimizes the need for IT staff to do their own research and testing.[8]

Organizations using hyper-converged systems with less optimized software lifecycle management can face challenges in piecing together firmware, drivers, and software packages, which can complicate patching security vulnerabilities.

Dell has the world's first turnkey cyber-vault solution endorsed to meet Sheltered Harbor's data vaulting standards.[9]

Sheltered Harbor, the standard-bearer for data protection and cyber-resilience in the U.S. financial sector, awarded Dell PowerProtect Cyber Recovery their very first endorsement for meeting all Sheltered Harbor cyber resilience and recovery requirements by a turnkey data vaulting solution vendor. That's a powerful validation of Dell's ability to deliver cyber-resiliency solutions you can trust. In fact, more than 1,100 cyber-recovery customers trust PowerProtect

Cyber Recovery software to deliver the utmost in cyber resilience and fast recovery with on-premises, hybrid-, and multi-cloud mission-critical backup data.[10]

What makes Dell PowerProtect Cyber Recovery so secure, reliable, and effective?

- Data copies written to an isolated, highly secure vault are write-lock protected (i.e., immutable) and secured by strict authorized access mechanisms.
- Independent vault data copy and recovery transfer operations are managed by a secure, isolated vault partition.
- CyberSense intelligent AI/ML cybersecurity pattern analysis and malware/ransomware detection software learn from uninfected data and get smarter over time.

Solutions that are less proven and less capable can burden organizations with greater risk of data loss and increased potential for extended outages when cyber-attacks occur.

Secured Component Verification (SCV) for PowerEdge servers made Dell the first vendor with a cross-portfolio solution for cryptographically verified hardware integrity.[11]

Dell's SCV enables you to verify that the hardware components of the PowerEdge server you have received matches what was manufactured in the factory. This assurance enables organizations to confidently deploy new servers, knowing the hardware configuration has arrived as ordered and built.

PowerEdge SCV is just one of many features of PowerEdge's enhanced cyber-resilient architecture. Other cyber-resiliency features include silicon root of trust, secure boot, dynamic system lockdown, automatic SSL certificate enrollment, two-factor authentication, real-time BIOS scanning for malicious code, and more.

Servers that do not have comprehensive cyber-resiliency layers baked in at the architecture level and throughout the supply chain and full product lifecycle can pose a serious risk to organizations' business-critical operations.

Epilogue: Dell goes above and beyond to help keep you safer

As organizations grapple with the cacophony of cybersecurity messages echoing across the industry, one message resonates loud and clear: Dell goes above and beyond the competition when it comes to cybersecurity. For unstructured data storage, mission-critical storage, hyper-converged storage, backup/recovery, and client and server platforms, Dell addresses a wide array of cybersecurity vulnerabilities that competitors don't. In summary, organizations relying on Dell can enjoy the following cybersecurity advantages:

- With Dell PowerScale and ECS scale-out storage systems, organizations get more robust analytics, automation, and recovery mechanisms for their unstructured data to help them thwart cyber-attacks, minimize data impact, and speed recovery.
- With Dell PowerMax storage arrays, organizations get more robust hardware security for their mission-critical application data, and they get more granular snapshot capabilities at scale to help minimize data loss in the event of a cyber-attack.
- With Dell Precision, Optiplex, and Latitude client systems, organizations get more advanced layers of hardware security in their end-user environment to heighten awareness of cyber threats and speed up recovery in the event of an attack.
- With Dell VxRAIL hyper-converged systems, organizations can reduce cyber risks more effectively as they modernize infrastructure with more streamlined software lifecycle management.
- With Dell PowerProtect Cyber Recovery software, organizations get a cyber-proven data protection solution, with impressive recovery success, which helps reduce risk of data loss.
- With Dell PowerEdge servers, organizations can deploy and expand workloads with greater confidence that the hardware configuration has arrived as ordered and built.

#TrustDell

About the author: Andrew Glinka is Vice President, Competitive Intelligence at Dell Technologies. Andrew is an 11-year Dell Technologies veteran and brings over 23 years of experience in technology sales, management, and operations. Prior to assuming his current role, Andrew served as Global Director of Sales Strategy for the Data Protection Solutions Division. He has also managed the Global Software Sales team as well as other sales teams in the Data Protection Solutions Division. Prior to joining Dell through the EMC acquisition, Andrew owned and operated an IT Managed Services business in Virginia for over 8 years before successfully selling the company.

[1] Based on Dell analysis comparing cyber-security software capabilities offered for Dell PowerScale vs. competitive products, September 2022.

[2] Based on Dell analysis comparing cybersecurity software capabilities offered for Dell ECS vs. competitive products, September 2022.

[3] Based on Dell internal analysis of cybersecurity capabilities of Dell PowerMax vs. cyber security capabilities of competitive mainstream arrays supporting open systems and mainframe storage, February 2022.

[4] Based on Dell's analysis of PowerMax cyber recovery scalability vs competitive enterprise arrays, April 2022. Assuming an RPO of 10-minutes for 2 days and 60-minutes for 7 days, more than 2 million snaps are required, based on average number of 5000 volumes configured in PowerMax.

[5] Based on Dell internal analysis, September 2022. Not all features available with all PCs. Additional purchase required for some features.

[6] For U.S. Federal customers only.

[7] Based on Dell analysis comparing Data Protection services for vSAN systems from a single vendor. VxRail comes with Dell RecoverPoint for VMs. Data Protection Suite for VMware and Data Domain Virtual Edition (DD VE) are available for larger environments.

[8] Based on Dell analysis, August 2022.

[9] Based on Dell Technologies analysis, August 2022.

[10] Based on Dell Technologies analysis, August 2022.

[11] Based on Dell Technologies analysis, August 2022.