Dell Technologies Expands Cybersecurity and Resilience for the AI Era and Emerging Quantum Risks

March 23, 2026

New enhancements help organizations strengthen device trust, improve cyber resilience and detect threats in AI data platforms

- Security by design approach hardens the world's most secure commercial PCs [i] with quantum-ready protections
- AI-powered cyber resilience helps organizations spot ransomware signals earlier and simplify recovery at scale
- Managed detection and response extends into AI data platforms to close visibility gaps attackers exploit

SAN FRANCISCO--(BUSINESS WIRE)--Mar. 23, 2026-- Dell Technologies (NYSE: DELL) introduces new security by design and cyber resilience capabilities to help organizations secure, detect and recover from next-generation threats. The enhancements address emerging risks from quantum computing and AI by hardening device foundations, strengthening cyber resilience when incidents occur and extending threat detection into AI data platforms.

Why it matters

AI is creating more valuable data and giving attackers new ways to move faster. Quantum computing will accelerate that shift by weakening the encryption technology that organizations use today to protect data and verify software integrity.

These converging threats are driving demand for devices built to resist future attacks, cyber resilience to minimize incident impact, and stronger detection across environments where AI data lives. Dell is addressing these security challenges through a layered defense approach across the technology stack, from the PC to the data center.

Hardening the PC foundation with quantum-ready protections

Quantum computing threatens the security foundations that protect devices today, driving a need for security by design at the deepest firmware layers. Dell is introducing quantum-ready security features to its commercial PCs to protect against attacks that can evade traditional security tools and remain hidden even after a restart or system reinstall.

The upgraded security features harden the PC's embedded controller (EC), a core hardware security component, to verify firmware updates using signatures designed to resist future quantum-enabled attacks. This helps prevent the controller from accepting malicious or tampered firmware and reduces supply chain risk by validating updates with stronger encryption and digital signatures.

Dell's enhanced BIOS Verification capability, aligned to post-quantum standards, detects tampering by checking the BIOS against a trusted reference stored securely in Dell's cloud. If something does not match, this Dell-unique verification[ii] flags the device and triggers an alert so teams can investigate and respond.

Strengthening cyber resilience with AI-powered recovery

Hardened devices are essential for helping reduce successful attacks, and so is cyber resilience to minimize impact when incidents occur. According to Dell's Cyber Resilience Insights research, only 40% of global organizations successfully contained and recovered from a cyberattack or incident drill with minimal impact. Dell is strengthening its PowerProtect cyber resilience portfolio to help organizations detect threats like ransomware sooner and recover faster from incidents.

Enhancements to **PowerProtect Data Manager** help organizations resolve recovery issues faster with an AI-powered assistant that provides contextual guidance during time-sensitive tasks, spot ransomware risk earlier with enhanced anomaly detection that scans Dell PowerStore snapshots and simplify management at scale with a unified dashboard across distributed systems.

PowerProtect Data Domain, the world's most secure foundation for cyber resilience [iii], extends protection to smaller sites and strengthens data security in transit. The PowerProtect Data Domain DD3410 appliance delivers up to 2x faster backups and 46% faster data restores,[iv] empowering organizations to resume operations quickly after an incident. The updated Data Domain Operating System, now including support for Transport Layer Security (TLS) 1.3, helps protect data while it moves between systems and aligns with NIST requirements for encrypted connections.

Extending threat detection from endpoints to AI data platforms

Fast recovery requires early threat detection. AI workloads concentrate valuable data in platforms that traditional endpoint security can miss, creating visibility gaps that attackers exploit. Dell is extending its **Managed Detection and Response (MDR) service** into environments where unstructured data and AI workloads live.

Building upon the MDR expansion to Dell PowerProtect, Dell MDR now extends to Dell PowerScale, providing organizations with enhanced visibility into threats targeting their AI data storage platforms. Supported by Dell's expert cybersecurity analysts, this service enables earlier detection of suspicious activity and automates response actions, streamlining security operations and safeguarding critical data.

Additionally, Dell is introducing a new **Endpoint Detection and Response (EDR)-only** option. This service monitors, investigates and responds to endpoint threats using advanced threat detection and next-generation antivirus capabilities. When used with Dell PCs, the service offers unique visibility into BIOS verification results. If a PC's BIOS drifts from its trusted baseline due to a potential compromise, an alert is sent to Dell's MDR team to investigate.

Perspectives:

John Roese, global CTO and chief AI officer, Dell Technologies: “Quantum computing will break the encryption and digital signatures protecting data today, while agentic AI raises the stakes by increasing the value of data and autonomously shares it across teams and organizations. We've been preparing for both shifts for almost a decade through our investments in post-quantum cryptography and our approach to cyber resilience and security by design. We are continuing to bring these protections across our portfolio to help organizations navigate emerging technologies and stay ahead of tomorrow’s threats.”

Javier González Belinchón, director, Corporate Infrastructure & Operations, Palladium Hotel Group: “In luxury hospitality, even a brief IT disruption during peak operations can have a major impact. We work with heavy workloads, and PowerProtect Data Manager’s Transparent Snapshots make a real difference. We get no business disruption, lower risk of data loss and the VM backup times are cut in half. Coupled with our PowerProtect Data Domain appliance, deduplication and compression optimize bandwidth, remote backups are seamless and storage requirements are drastically reduced.”

Fernando Montenegro, vice president & practice lead, Cybersecurity & Resilience, Futurum: “As AI adoption expands, security teams need to protect more high-value data in areas where traditional controls may not provide adequate visibility into how threats move across AI workloads and data platforms. Dell’s approach reflects this broader cyber resilience strategy aimed at reducing risk, deepening security visibility and helping organizations recover more effectively when incidents occur.”

Availability:

- Quantum-ready security features will be available on new Dell commercial PCs launching in 2026.
- Dell PowerProtect Data Manager enhancements are now available.
- Dell PowerProtect Data Domain Operating System updates are now available.
- Dell PowerProtect Data Domain DD3410 appliance will be available April 15, 2026.
- Dell Managed Detection and Response (MDR) expansion to Dell PowerScale is now available.
- Dell Endpoint Detection and Response (EDR)-only option is available April 16, 2026.

Additional Resources:

- Quantum Resilience, Built In
- PowerProtect: Accelerate Innovation. Trust Your Resilience.
- How Palladium Hotel Group Built Cyber Resilience to Power AI Innovation
- Follow and stay connected with us on Instagram, Facebook, YouTube, X and LinkedIn.

About Dell Technologies

Dell Technologies (NYSE: DELL) helps organizations and individuals build their digital future and transform how they work, live and play. The company provides customers with the industry’s broadest and most innovative technology and services portfolio for the AI era.

---

[i] Based on Dell internal analysis, October 2025 (Intel) and March 2026 (AMD). Applicable to PCs on Intel and AMD processors. Not all features available with all PCs. Additional purchase required for some features. Intel-based PCs validated by Principled Technologies, July 2025.

[ii] Based on Dell internal analysis, October 2025 (Intel) and March 2026 (AMD). Applicable to PCs on Intel and AMD processors. Not all features available with all PCs. Additional purchase required for some features. Intel-based PCs validated by Principled Technologies, July 2025.

[iii] Based on internal analysis. October 2025. The foundation for cyber resilience is offered by a family of Dell PowerProtect Data Domain appliances that deliver a comprehensive, trusted and unique collection of capabilities, including: secure supply chain, Zero Trust maturity, immutability, managed detection and response, durability, chain of trust, secure remote access card, secure period.

[iv] Based on Dell internal testing comparing a PowerProtect Data Domain DD3410 appliance vs a PowerProtect Data Domain DD3300 appliance, both configured at similar capacity. January 2026. Actual results may vary.

View source version on businesswire.com: https://www.businesswire.com/news/home/20260323998903/en/

Dell Technologies Media Relations: Media.Relations@Dell.com

Source: Dell Technologies