INSIGHTS | TECH BRIEF

PowerEdge Servers: Engineered for AI, Resilient to Cyber Threats

At one time, buying a server was about selecting a box to run workloads. That is no longer the case today. Server selection is complicated. Besides a workload host, servers are prime targets for cyber criminals who want to carry out ransomware, nation state attacks and AI-powered threats.

Speaking of AI, general-purpose servers are not suitable for the AI-driven workloads of today. Instead, they demand specialized servers that are designed to handle the scale, speed, and complexity of modern artificial intelligence. Dedicated AI servers ensure that your business has the required computational power, memory and networking capabilities to ensure that your AI objectives are achieved.

Why Cyber Resilience is Critical

Organizations have learned the harsh reality that protecting against every type of cyberattack is simply unrealistic for multiple reasons:

- **Shifting Tactics:** Attackers adapt their methods faster than defenses can be updated.
- **Emerging Technologies:** New tools and platforms introduce unforeseen vulnerabilities.
- **Zero-Day Exploits:** Previously unknown vulnerabilities are discovered and weaponized daily.

What this means is that you want servers that are designed with the assumption that they will be breached. This isn't about surrender. It's about strategic resilience. Businesses must have the modern server architecture that can:

- **Contain Damage:** Limit an attacker's ability to move laterally or access critical assets.
- **Enable Rapid Recovery:** Restore operations quickly to minimize business disruption.
- **Maintain Continuity:** Keep essential services running even during active incidents.

These and other factors have brought cyber resilience to the forefront, defined as the ability of a system to withstand attacks, recover quickly when compromised, and continue operating with minimal disruption.

77%

of organizations are either exploring potential use cases or investing significantly in GenAI technologies.[1]

DELL Technologies
PLATINUM PARTNER

PowerEdge Servers & Cyber Resiliency

Dell PowerEdge servers are designed with cyber resiliency as a core principle. At the core of this philosophy is Dell's Secure Development Lifecycle (SDL) model, which ensures that security is intrinsically built into every stage of design, development, and deployment. This intrinsic approach demands that security is built-in from the start, not an added feature.

- PowerEdge Server design starts with applying threat modeling and penetration testing during the design process itself.
- Secure coding standards are enforced throughout firmware development, ensuring that the underlying software can actively resist, detect, and counter attempts to inject malicious code.
- Continuous validation and monitoring are enforced to ensure PowerEdge servers are resilient against evolving cyber threats.

Dell's unwavering commitment to total security guarantees that PowerEdge firmware or BIOS aren't tampered with in the supply chain or at runtime, ensuring trusted integrity across every operational stage.

Zero Trust Architecture

Dell PowerEdge servers are built under the presumption that the network they reside in is always vulnerable to compromise. Thus, the only way to safeguard access to critical data and resources is by enforcing a Zero Trust architecture throughout, built on the principle of least privilege. This principle is applied not only to users, but to applications, communication paths, network devices, and the data itself.

To ensure a Zero Trust product, Dell must apply the same security principle across its entire supply chain. Dell enforces supply chain controls that cover all aspects of supplier selection, sourcing, production process and governance. All the parts that go into a Dell PowerEdge are verified against the approved vendor list and bill of materials and then further inspected using multiple checkpoints.

Securing the IDRAQ

Any compromise of the iDRAC can open the door to attackers taking control over server operations, manipulating underlying server infrastructure or obtaining access to sensitive data. That is why securing the remote management interface from attacks is imperative for cyber resilience. Dell achieves this using multiple features including:

- **Hardware Root of Trust:** A built-in silicon chip validates firmware authenticity at startup, preventing attackers from tampering with BIOS or core system files.
- **Encrypted Remote Access:** All management connections use strong encryption (TLS 1.2/1.3) to prevent attackers from intercepting credentials or sensitive data.
- **User Authentication & RBAC:** iDRAC integrates with Active Directory/LDAP and supports multi-factor authentication for granular role-based access control.
- **Network Isolation:** iDRAC operates on separate management networks and supports 802.1X port-based network access control with certificate authentication for greater isolation.
- **Automatic Security Updates:** Dell regularly releases firmware patches to fix newly discovered vulnerabilities, ensuring iDRAC stays protected against evolving threats.
- **Zero Trust Architecture:** PowerEdge servers assume the network that hosts them is vulnerable, so it implements zero trust principles. Every user, device, and application must be continuously authenticated and explicitly authorized. The principle of least privilege is enforced, minimizing access to only what is necessary.

Dell iDRAC's multilayered security architecture provides organizations with a trusted foundation that embeds protections at every layer, ensuring that PowerEdge infrastructure can withstand evolving cyber risks while maintaining operational continuity.

AI-Driven Resiliency

People are using AI to enhance their performance in a growing number of ways. Unfortunately, that includes hackers. Cyber criminals are using advanced AI systems to carry out nefarious activities at an unprecedented scale and manipulate systems in innovative and harmful ways beyond human capabilities. To even the playing field, you need servers with AI integration to thwart these automated attacks.

Dell PowerEdge servers leverage AI and machine learning to enhance cyber resilience by embedding intelligent, automated security and recovery functions directly into server operations. Through platforms like Dell OpenManage and iDRAC, PowerEdge continuously monitors for anomalies, detects threats in real-time, and uses AI-driven analytics to predict and remediate potential issues before they disrupt workloads.

Built for the Era of AI

The Dell PowerEdge server family includes models that are built to deliver the power necessary to accelerate AI workloads. Some of the workloads it is designed for include generative AI, natural language processing (NLP), digital twins, recommendation learning, financial modeling and simulation. To meet these demands, PowerEdge servers support leading AI accelerators from NVIDIA, Intel, and AMD that speed up machine learning training, AI processing, and complex computations.

Advanced GPUs alone aren't enough to handle demanding AI workloads. In addition to dense acceleration, Dell servers offer advanced thermal design, and optional liquid cooling to efficiently manage the high computational and heat demands of modern AI workloads. These features deliver consistent performance, energy efficiency, and reliability, ensuring mission critical environments can safely run large scale AI training or real time inference without compromise. If your business wants to put AI to work, then consider server models like the XE9680, XE9640, XE8640, and R760xa that can handle the work because they are purpose-built for AI, ML, and deep learning applications.

Talk to WEI Today

The technology is advanced, but the premise of Dell PowerEdge servers is straightforward. They are engineered for cyber resiliency while also having the computational muscle to handle today's most demanding AI workloads. Whether you're deploying AI now or planning future implementations, PowerEdge provides the security foundation and performance capabilities your organization needs. Before your next infrastructure refresh, explore how Dell PowerEdge can strengthen both your security posture and AI readiness.

Sources:

1. IDC Future Enterprise Resiliency and Spending Survey, Wave 6, July 2023.

About WEI

WEI is an innovative, full service, customer centric IT solutions provider.

Why WEI? Because we care. We go further.

WEI is an expert in business technology improvement, helping clients optimize their technology environments and work efficiently. WEI works with clients to understand goals, integrate strategy with technology solutions, and leverage their current IT environment into one company-wide model to increase utilization and efficiencies around their unique business processes.