DELL Technologies

Dell EMC PowerEdge Cyber Resilient Architecture 2.0

As cyber threats and attacks become more nefarious and widespread, businesses must change the way they approach security to be more comprehensive. **Dell EMC PowerEdge servers take cyber resilience to the next level**, serving as the bedrock for organizations to secure invaluable data and their critical infrastructure.

What is the Dell Cyber Resilient Architecture 2.0?

Safeguarding your data and intellectual property requires a more robust, layered approach. Cyber Resilient Architecture 2.0 builds on Dell's security legacy with enhanced capabilities that effectively protect your infrastructure, reliably detect threats and rapidly recover from cyberattacks.

Confidently deploy servers with built-in cyber-security controls and a protected supply chain, including cryptographic component verification for factory-to-site hardware integrity assurance.

PowerEdge layered security solutions are pervasive to protect your business against today's ubiquitous and sophisticated threats.

Through design, manufacturing, production and retirement, Dell's **Security Development Lifecycle (SDL)** and **Cyber Resilient Architecture** provide continual security to protect, detect and recover from threats.

End-to-end boot resilience, anchored with **Root of Trust**, ensures a trusted and protected boot cycle. Cryptographically attest to the integrity of BIOS and iDRAC firmware.

Cyberattacks are everywhere, coming at your organization from outside of the business and within.

Safeguard sensitive information at all times using strong encryption with Secure Enterprise Key Management (SEKM) and protect data in use using new confidential compute technologies.

Why choose Dell Technologies?

"It is **NCC Group's** opinion that **Dell has a mature product security program**. They have a long history of engaging with external security partners like NCC Group to perform security reviews of their systems and new features as they are developed. **Their SDL continues to consider security throughout the product development process**, where security can be built into the product from the earliest stages."*

"**The SCV framework leverages well-established cryptographic constructions throughout the implementation**. iDRAC provides a separate security domain, which helps put large portions of the security guarantees provided by SCV out of harm's way from potential exploits that affect the x86 host portion of the system."*

Dell Technologies use of "Intel BootGuard and AMD Platform Secure Boot are host processor features that provide **strong firmware integrity guarantees**, preventing firmware other than that authorized by the OEM from executing on the system. By enabling these as additional defense-in-depth measures, certain classes of physical attacks are mitigated, such as flash memory replacement or reprogramming, and Time-of-Check-Time-of-Use (TOCTOU) race conditions. All combined, the Root of Trust features in the system make compromise of the TCB difficult."*

*Based on a NCC Group paper commissioned by Dell Technologies, Secured Component Verification, April 30, 2021. Actual results may vary.

Visit the following resources to learn more.

Technical White Paper

Cyber Resilient Security in Dell EMC PowerEdge Servers

Supply Chain Security Video

Secured Component Verification

Technical White Paper

iDRAC9 Security Configuration Guide