DELL Technologies

SOLUTION BRIEF

Embracing Multilayer Security With AMD and Dell EMC PowerEdge Servers

The Three Tenets of PowerEdge Ensure Complete Cyber Resilience

AMD

When it comes to keeping your data infrastructure secure, hardware-based security matters just as much as more commonplace software-based measures. Threat actors know that a company's firmware, BIOS, or other hardware-based entry points are often more vulnerable than their software-based applications or OS, especially if the proper firewalls are in place. Dell Technologies and AMD have developed hardware-level solutions to ensure maximum protection without compromising performance.

This solution brief explores how Dell EMC PowerEdge servers work in tandem with AMD EPYC™ processors to build multilayer hardware protection infrastructure that's adaptive, proactive, and fully autonomous, making it the most effective method for combating modern cyberthreats.

Countering Hardware Threats With Solutions From Dell Technologies

Most enterprise companies anticipate that threat actors will target vulnerabilities in their software or network infrastructure but given the global shift toward remote work and the more widespread adoption of IoT, the importance of addressing hardware-based vulnerabilities cannot be overstated.

Potential hardware attack vectors that cybercriminals are primed to exploit include:

- Component/server tampering
- Firmware corruption
- Malware injection
- Server identity spoofing
- Unauthorized open-port attacks
- Counterfeit components
- Manufacturing site security
- Theft and/or tampering during transport

Dell Technologies has anticipated these and other potential attack vectors and has developed technologies to keep your hardware secure. These technologies are an inherent part of Dell EMC PowerEdge servers, giving you peace of mind from the start.

Across the server platform security layer, Dell EMC PowerEdge servers incorporate technologies like Secure Component Verification (SCV), Silicon-Based Root of Trust, and iDRAC9 server management to ensure hardware components cannot be physically or remotely tampered with. For the server environment security layer, Self-Encrypting Drives, Secure User and Component Verification, and existing partnerships with the Transported Asset Protection Association (TAPA) guarantee full physical and data security.

Building a Complete Hardware Protection Framework

For Dell, the emphasis on hardware-based security coverage is best summarized in the three tenets of Dell EMC PowerEdge protection:

- Adaptive compute solutions
- Autonomous compute infrastructure
- Proactive cyber-resilient architecture

Dell EMC PowerEdge servers embrace these tenets most clearly by prioritizing protection-based functionality. Specific capabilities of the cyber-resilient architecture that lies at the heart of Dell EMC PowerEdge servers include:

- User access security which ensures proper authentication and authorization
- Encrypted data storage which deters physical data theft
- Physical security which actively protects the Dell Technologies' product supply chain

- Signed firmware updates to ensure only authentic firmware is running on the server platform
- Cryptographically-verified trusted booting for monitoring, securing, and verifying the boot process
- BIOS live scanning for verifying the integrity and authenticity of system BIOS images

These and other key Dell EMC PowerEdge protection features work together to give prospective adopters peace of mind throughout every step of the PowerEdge server adoption process, from initial procurement to deployment, setup and configuration, and ongoing use and maintenance.

AMD EPYC: Improving Security Without Impacting Performance

Dell Technologies recognizes that one major barrier of adoption for hardware-level security is the performance impact it can have on specific hardware components, particularly CPUs. That's why it works closely with AMD to pair Dell EMC PowerEdge servers with AMD EPYC processors which are built specifically to prioritize hardware-level security without impacting performance. AMD EPYC processors take a proactive approach to system security through their built-in AMD Infinity Guard security suite. However, when paired with Dell EMC PowerEdge servers, they also leverage Secure Memory Encryption (SME) and Secure Encrypted Virtualization-Encrypted State (SEV-ES) to create work environments with comparable performance metrics to environments with no extra security features enabled.[1]

Along with their inherent SME and SEV-ES security functionality, AMD EPYC processors also further support Dell Technologies' focus on layered cyber-resilient architecture by adopting similar physical security principles such as Silicon Root of Trust and boot verification.

Fostering Trusted Dell EMC PowerEdge Partnerships With Precision Computer Services (PCS)

Dell Technologies knows that no matter which part of a company's infrastructure it's targeting, security is important, which is why it only works with trusted supplies and vendors like AMD and PCS to offer its proven security-focused Dell EMC PowerEdge server solutions. PCS is a Dell Technologies Gold partner, so you can rest assured that when you work with them, you'll get the same high level of quality that you'd get from working with Dell Technologies directly.

About PCS

Precision Computer Services (PCS) was founded in 1989. From the get-go, we knew we wanted to be different. We ditched the corporate bureaucracy and the complicated sales process. As a Dell Technologies Gold Partner, we focus on one thing: tackling complexity for our customers. At PCS, we encourage individual creativity and promote working in a team environment with the simple mission of putting our clients first.

PCS | 175 Constitution Blvd South | Shelton, CT 06484 | 203.929.0000 |
contactus@precisiongroup.com | precisiongroup.com

Contact us at 203.929.0000 to learn what PCS can do for you.

[1]Principled Technologies, "Enabling two security features on 3rd Gen AMD EPYC processors minimally affected OLTP performance on a Dell EMC PowerEdge R6525 system," March, 2021.