Dell EMC PowerEdge Cyber Resilient Architecture 2.0

As cyber threats and attacks become more numerous 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 Dell Cyber security solutions powered by Dell’s secure supply chain, including built-in cyber-security features and component verification for increased business integrity by design.

PowerEdge learned security solutions are purpose-designed to protect your business infrastructure and improve system resilience.

Through design, manufacturing, and operations, Dell’s Secure Supply Chain leverages high-integrity standards to detect and recover from threats.

Why choose Dell Technologies?

"The NCC Group’s opinion that Dell has a mature product security program. Dell has a long history of engaging external security partners to perform independent security reviews and remain proactive and up-to-date. Additionally, Dell has mature processes to continuously monitor and test the changing threat landscape to ensure that they are always prepared to protect against emerging threats. Their SDL continues to consider security throughout the product development process, resulting in secure products that are trusted by customers around the world."

"The SCV framework leverages well-established cryptographic constructions throughout the implementation to ensure a trusted and protected endpoint. From the moment the system is booted, Cryptographic Root of Trust features in the system make compromise of the TCB difficult.*

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 provides strong firmware integrity guarantees, preventing firmware other than that authorized by the OEM from executing on the system.

"The DTS Technology uses of Intel BootGuard and AMD Platform Secure Boot are host processor features that provide firmware integrity guarantees, allowing you to trust the starting point of your system.*"

Cyberattacks are everywhere. Ensure that your infrastructure is battle-hardened, detect threats and recovery from attacks.

Safeguard sensitive information of all types using encryption technologies and SSL certificates. Protect your management plane with multi-factor authentication and single sign-on.

Visit the following resources to learn more.

Technical White Paper
Cyber Resilient Security in Dell EMC PowerEdge Servers

Supply Chain Security Video
Secondary Component Verification

Technical White Paper
iDRAC Security Configuration Guide

Copyright © 2019 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC and other marks are trademarks of Dell Inc. or its subsidiaries. Intel, the Intel logo, Intel BootGuard, and other trademarks are the property of Intel Corporation.

Dell Technologies makes no representations or warranties with respect to the accuracy or completeness of the content contained in this document, and disclaims all liability for damages resulting from the use of this document. Dell Technologies reserves the right to make changes to this document without further notice.

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

Dell Technologies believes the information in this document is accurate as of its publication date. The information is subject to change without notice.