4 QUESTIONS IT LEADERS NEED TO ASK ABOUT SERVER SECURITY

Read the full server security report

Successful IT Transformation begins with embedded end-to-end server security. Ask these 4 essential questions to ensure that you partner with a security leader to protect your servers from malicious attack.

1 How do you ensure server security at the firmware/hardware level?

Focusing only on network, data, OS, and applications protection may leave your IT vulnerable to malicious attacks at the hardware and firmware levels. Dell EMC uses silicon-based security and cryptographic root of trust to authenticate BIOS and firmware during the server boot process, logging hardware intrusion detection even without AC power.

2 How are my servers protected throughout the security lifecycle?

IT security depends on comprehensive protection, from server deployment to retirement. PowerEdge servers feature an enhanced cyber-resilient architecture to protect, detect, and recover from cyberattacks – through each phase of the lifecycle. It's important that your server vendor be well-versed in this end-to-end security approach.

3 How does your product development process integrate security?

Delivering cyber-resilient architecture requires security awareness and discipline at each stage of server development. At Dell EMC, security is built in from the ground up as an integral part of the overall hardware and firmware design.

4 How do you price key security features?

Some vendors charge a licensing fee for security features, and your data center will not be fully protected without the additional purchase. PowerEdge servers include hardware and firmware security as a fundamental component in every server, not as an optional set of features to be licensed over time.

Full-lifecycle security embedded in every server

Dell EMC PowerEdge servers – powered by Intel® Xeon® Scalable processors – form the foundation of your modern IT infrastructure. See how to secure your business and prevent malicious cyberattacks with embedded, end-to-end protection at the firmware and hardware level.

Read the full server security report