Zero Trust. Verified Trust.

Meet the challenge of ever-changing threats with the new standard in cybersecurity.

The complexity of today’s IT environments along with the sophistication of today’s threat landscape requires a shift in thinking that cannot be solved with point-by-point security solutions.

Device trust
A silicon-based hardware root of trust — the foundation of device trust — is embedded in every phase of the server lifecycle — from design to manufacturing through use and end of life. We continue to innovate to meet the ever-growing threat landscape.

Data trust
Storage data and cache so that no confidential information is compromised. Customers can also take advantage of secure server lifecycle: multifactor authentication, system lockdown, and recovery. Systems need to be taken out of production securely to avoid data compromise and misuse. System erase eliminates nonvolatile stores.

Software trust
The default state of every server is verified trust. By design, zero-trust deployments using robust layers of security across hardware and software must be achieved. If the server is compromised, it should perform verifications before it trusts a user, or device, and grants access.

Transport and session trust
Network and session trust must also be achieved. Data in transit must be encrypted and data in use must be protected. Data-in-use protection, key management, and confidentiality are necessary to the fundamentals of information security. Unlike trust-then-verify frameworks, the zero-trust approach performs verification before it trusts a user, or device, and grants access.

visibility and analytics
Threats can come from anywhere, and it is critical to secure all aspects of the enterprise network from the edge to the endpoint, data to applications to help protect data access to sensitive, managed data and resources. In some way — and sets out to do so within a framework that presumes the network is not trusted.

Tenets of zero trust
Zero trust is integral to the Dell Technologies infrastructure and end-to-end lifecycle. Dell Technologies believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

Manufacture and deliver
With the newly released Secured Component Verification program, customers augment zero trust with cryptographic verification of devices throughout the delivery process. The Dell Technologies supply chain assurance program implements cyber resilience and zero trust from the time features are conceived and designed through production and maintenance. This provides assurance to the customer that servers are resilient at their foundation.

Visibility and analytics
Software root of trust is embedded into every phase of the server lifecycle — from design to manufacturing through use and end of life. The complexity of the modern IT infrastructure along with the sophistication of today’s threat landscape requires a shift in thinking that cannot be solved with point-by-point security solutions.

Dell EMC OpenManage Enterprise
Dell EMC OpenManage Enterprise modules and capabilities, and drift detection plus secure E2E boot and UEFI boot capabilitie, and drift detection plus secure E2E boot and UEFI boot

In the wake of a rash of bold cyberattacks and ever-evolving risks that have targeted everything from the national energy grid to the food supply chain, organizations are going back to the fundamentals of information security. Unlike trust-then-verify frameworks, the zero-trust approach performs verification before it trusts a user, or device, and grants access.

Zero Trust: The new standard in cybersecurity

The Dell Technologies zero-trust approach is a security orientation that is a critical component of infrastructure. In the context of today’s IT infrastructure, the zero-trust approach redefined to align with the U.S. Department of Defense.

Learn more about cyber-resilient Dell PowerEdge servers. Visit DellTechnologies.com/Servers or our Infobar.