DELL Technologies

Solution Brief

Dell Technologies Secured Component Verification for PowerEdge

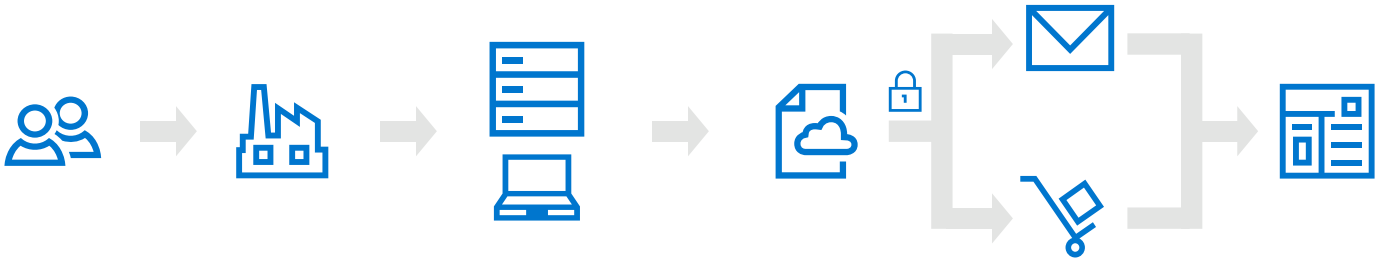
Defending against cybersecurity attacks continues to challenge IT Operations and Security teams at every level of their infrastructure. While application and operating system compromises are the more common attack vector, utilizing malware and ransomware, hardware attacks are also on the rise. Because of this growing threat, more and more attention is being paid to servers and the assurance that nothing in the server hardware configuration has been altered between the time the system is built and the time the system is deployed. It is no wonder that 84% of respondents to a Forrester Research survey[1] considered hardware/supply chain security to be critically or very important to their business.

Dell Technologies Secured Component Verification provides verification of the as-built hardware configuration for your PowerEdge servers. The verification enables you to confidently deploy new servers in your datacenter knowing the hardware configuration will provide you with a solid foundation for your mission critical applications. Secured Component Verification is aligned with emerging U.S. Government guidelines for technology supply chain security.

Deploy Servers with Confidence

The Dell Technologies Secured Component Verification, now an integral part of the Dell EMC PowerEdge Server line, enables IT administrators to securely validate their delivered systems prior to deployment. Organizations can ensure that their new servers are delivered with the same components installed at Dell Technologies' manufacturing facility.

When the system is ready for shipment, the server components and their unique ID's are assessed, and the resulting data is cryptographically secured using a signed certificate. The encrypted inventory is embedded in the server and shipped with the system to the datacenter. After the system is received, the IT administrator will conduct an inventory of the delivered system using the SCV tool provided and authenticate that inventory with the certificate stored on the system. Once authenticated, and components are verified to match, the system is ready to be provisioned and deployed.



Order
Customer places order for Server Product

Build
Order is sent to Factory to Build

No Change to Existing Order → Build Process

Collect
System's Component Data is Collected, Encrypted and a Platform Certificate is Created and Signed by an HSM (High Security Module)

Store
Platform Certificate is Stored in a central location (DL for Services) and on the Server (iDRAC)

Deliver
Dell Signed Certificate is Delivered to Customer on the Server (iDRAC)

Validate
Customer Validates Authenticity of componenets via local system management tool

[1] Source: Forrester Research, Inc., The Next Frontier for Endpoint Protection

The Need for a Secure Technology Supply Chain Comes into Focus

The U.S. Government, in collaboration with its global trade partners, has continued to refine its guidance for cybersecurity. With respect to server infrastructure, they have recently focused greater attention on the validation of server components and the authenticity of firmware on those servers. In their most recent draft paper, the National Cybersecurity Center of Excellence (NCCOE), part of the National Institute of Standards and Technology clearly illustrated the challenge - all server OEMs are working with numerous component and subsystem vendors. While all have instituted supply chain assurance programs to guarantee the quality and security of their suppliers' components, there hasn't been an easy way for the end-user to validate that what was installed at the factory is exactly what they received. Dell Technologies is collaborating with the NCCoE in the Supply Chain Assurance Building Block Consortium to develop practical, interoperable cybersecurity approaches that address the real-world needs of complex Information Technology (IT) systems.[2]

Dell Technologies Secured Component Verification - A Secure Foundation for Trusted Applications

In today's evolving cybersecurity environment, where software and hardware are potential penetration targets, there is clearly a need for increased assurance and confidence in the server infrastructure. To keep pace with the increasing demand for faster application development, test, and deployment, new features like Secure Component Validation need to be incorporated into the infrastructure lifecycle. With SCV, IT Operations and Security teams can be assured that their as-delivered systems are aligned with their server specifications and their security framework, eliminating a potential attack vector so they focus their energy on business outcomes.

Features and benefits of Secured Component Verification:

- Cryptographically signed inventory certificates available across the PowerEdge server portfolio
- Factory to rack assurance - secure self-verification assures full hardware integrity during transit to your datacenter
- Integration with existing scripts to facilitate the validation process, making trusted deployment an automatable process
- Aligns with emerging standards for supply chain security, important to industries where cybersecurity is the top priority

[2] NIST does not evaluate commercial products under this consortium and does not endorse any product or service used. Additional information on this consortium can be found at: https://www.nccoe.nist.gov/projects/building-blocks/supply-chain-assurance

Discover more about PowerEdge servers

Learn more about Dell Technologies Secured Component Verification

Learn more about our systems management solutions

Search our Resource Library

Follow PowerEdge servers on Twitter

Contact a Dell Technologies Expert for Sales or Support

DELL Technologies