Protect Your Device, Data and Business

Dell VxRail — Security built into every stage of the supply chain

How do you know your hyperconverged system hasn't been maliciously tampered with before it arrives at your data center? Dell Technologies and VMware® enact digital and component security measures that drive supply chain assurance and confidence that you're receiving a product without backdoor vulnerabilities.

40% of cyberattacks are aimed at the supply chain.[1]

Why supply chain security?

Supply chain security is the process of applying preventive and detective control measures to protect your physical and digital assets, inventory, information, intellectual property and people. It typically applies to outsourced components and software. With our comprehensive product security programs, however, Dell Technologies works to minimize the injection of malware and counterfeits into the supply chain at any stage of the process.

Dell Secure Development Lifecycle

VxRail product development includes security integrated throughout the product lifecycle. Particular measures address malicious tampering before you even receive your system. Here's some of what you can expect from Dell Technologies:

Development

Threat modeling, code reviews, scanning of third-party components

Trusted Execution Technology (TXT)

built into the Intel® processor, uses cryptography to verify that the firmware BIOS and the hypervisor haven't been tampered with.

Trusted Platform Management (TPM)

is a secondary, optional layer of security (an international standard) that stores cryptograpic keys to verify secure boot and test system integrity.

Secured Component Verification (SCV)

is a Dell initiative that provides last-leg assurance on the integrity of your product from the time an order is fulfilled at the Dell factory to when it's delivered to your data center.

Software bill of materials (SBOM)

is soon to be a federal requirement that Dell Technologies already offers. An SBOM identifies all software used in your system, including its dependencies on other subcomponents.

Prior to release

Software scan, no open vulnerabilities, malware screen, validate data can be transmitted and received securely

Compatible standards and certifications

VxRail security lifecycle is intrinsically hardened in accordance with NIST 800-53 standards. This enables us to help your organization comply with most industry standards, such as PCI/DSS, NERC-CIP, HIPAA, and ISO.

Just better

Dell Technologies, VMware and Intel have spent years innovating to serve you — even before you receive your system.

Dell VxRail — delivering the assurance you need to move forward and thrive.

- ✓ Read the Dell VxRail Secure Supply Chain brief.
- ✓ Download the Dell Technologies supply chain white paper.

1st

Dell Technologies is the first vendor to provide an SBOM to customers, for the VxRail system.

[1] Accenture, Securing the Supply Chain, 2020