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

1 Accenture, Securing the Supply Chain, 2020

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.

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

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.

Why supply chain security?

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:

- **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.
- **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 on Intel® standards that authenticates each key step in the boot and test system integrity.

Prior to release

Furthermore, our vulnerabilities, malware scans, and security validations data can be transmitted and reviewed securely.

Development

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

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

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 industry standards, such as PCI/DSS, NERC-CIP, HIPAA, and ISO.

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

40% of cyberattacks are aimed at the supply chain.

Copyright © 2022 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell and other trademarks are trademarks of Dell Inc. or its subsidiaries. VMware® is a registered trademark or trademark of VMware, Inc. in the United States and/or other countries and is used herein with permission. All other marks and names mentioned herein may be trademarks of their respective companies. Copyright © 2022 VMware, Inc. All rights reserved.