dtuc.

How to help secure your fleet from first boot

Dell SafeSupply Chain

Dell Technologies User Community

DELL Technologies

dtuc.

DELL TECHNOLOGIES USER COMMUNITY

Zoom Reminders

- Please note this webinar is being recorded
- If you have a question, please use the chat or put it in the Q&A Section
- Have fun!

dtuc.

DELL TECHNOLOGIES USER COMMUNITY

We want to hear from you!

Don’t forget to participate in
our post-event survey!

2 lucky survey participants will be randomly selected to a $25 Amazon Gift Card!

Upcoming Webinars

SupportAssist for Business PCs Demonstration and Deep Dive

October 24th from 11:00am – 12:30pm CT

TechDirect: IT Admin Onboarding and Self-Dispatch

October 28th from 11:00am – 12:00pm CT

Meet our speaker!

DELL TECHNOLOGIES USER COMMUNITY

Tom Bentz

Product Marketing Manager

Dell Endpoint Security

Agenda

- Cybersecurity State of the Union
- How Dell Approaches Supply Chain Security
- Dell SafeSupply Chain solutions for supply chain assurance
  - Platform Certificates and SCV
  - Other Supply Chain Offers for North America
- Summary and resources

Cybersecurity State of the Union

Endpoints are an Expanding Attack Surface

69%

of organizations report at least one hardware or firmware level attack[1]

Unsafe Hardware

62%

of network breaches in 2021 attributed to supply chain vulnerabilities[2]

Supply Chain Compromise

82%

of breaches were driven by individual error, e.g., phishing attack[2]

Social Engineering

Replication Through Removable Media

External Remote Services

Valid Accounts

[1]Futurum Group Survey, 2023 [2]Verizon DBIR Report, 2022

The Threat Landscape

What's keeping IT & security up at night?

Detection of BIOS firmware events

High-risk configurations

Validating device integrity configuration from the factory

Source: TechTarget's Enterprise Strategy Group, research sponsored by Dell Technologies, "Assessing Organizations' Security Journeys," November 2023.

Cyber Complexities

Increase in disruptive technology & behaviors on the horizon

Hardware Threats

Counterfeit, taint, & component insertion threats

Supply Chain IT Globalization

Increased IT global dependence & interconnectivity

Software Threats

Intended & unintended vulnerabilities are evolving & dynamic

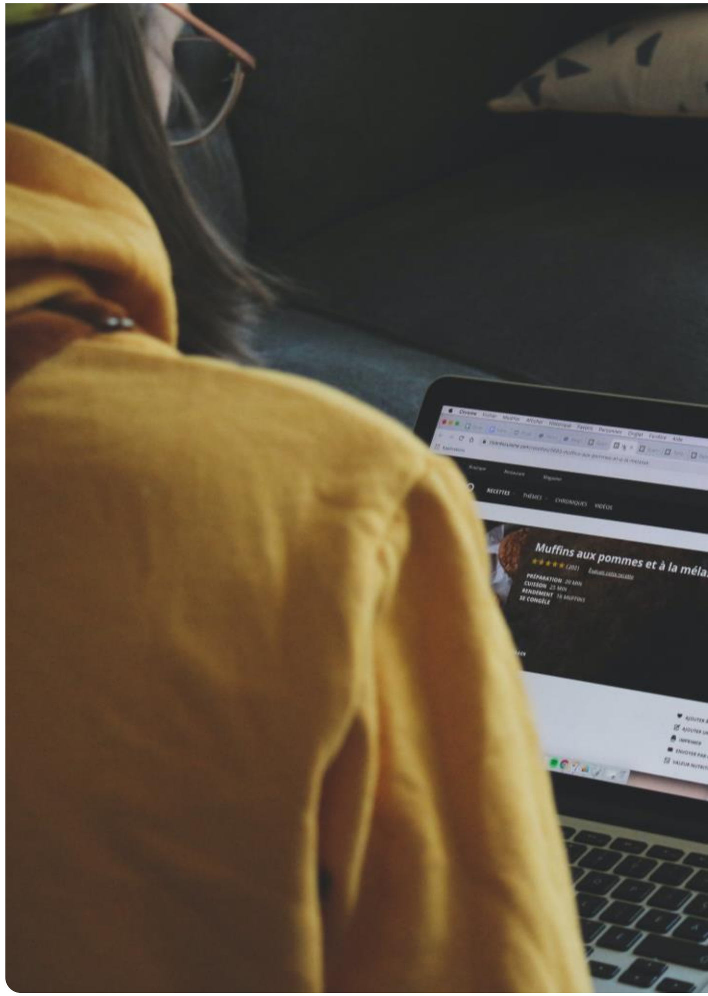
Regulation Risks

Rise in government regulation & industry controls

DELLTechnologies

What else is impacting cybersecurity?

- COVID, cyberattacks and Global Government Security Orders
- May 2021 Executive Order
- IDC validated security tenants
- High profile successful attacks
- Newer Targets: SLED and SMB
- 2022 Global Events



DELL Technologies

How Dell Approaches Supply Chain Security

Supply Chain Security

Strict supply chain standards are foundational to device security

Innovation

Supply Chain

Manageability

Ongoing Support

Dell’s Supply Chain Security initiative takes a comprehensive approach to protect its supply chain and deliver solutions customers can trust

Security

Provides confidentiality, and availability of information

Integrity

Ensures products or services are genuine, unaltered and will perform properly

Quality

Reduces vulnerabilities that may limit function and lead to failure or exploitation

Resilience

Ensures that IT supply chain provides required products and services

62% of supply chain attacks investigated by the European Union Agency for Cybersecurity were **the result of misplaced trust in a supplier**[1]

[1] *ENISA, 2021*

Supply Chain

- Innovation
- **Supply Chain**
- Manageability
- Ongoing Support

Manufacturing

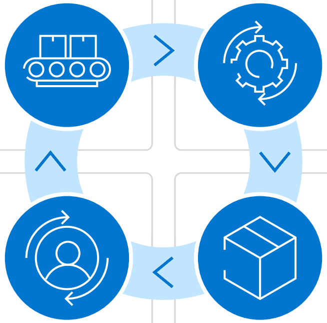
ID of device components (**PPID**)

Source parts & products through Dell-authorized channels

Assembly & Customization

Hard drive sanitization and reimaging

BIOS image verification



End User Lifecycle

Licensing, entitlements, updates, transfer of ownership, sustainable and secure end of life

Shipping & Delivery

Tamper evident seals and tape for endpoints and ports

Tamper evident pallet seals and secure chain of custody

Hardware Integrity

Ensure devices are not tampered with or counterfeit components are not inserted before shipping

Software Integrity

Ensure no malware is inserted in firmware or device drivers before shipping to help prevent coding vulnerabilities

Physical Security

Ensure high level of physical security in factories, robust screening and hiring practices, annual compliance training and certification

Supply Chain Security

Hardware Integrity

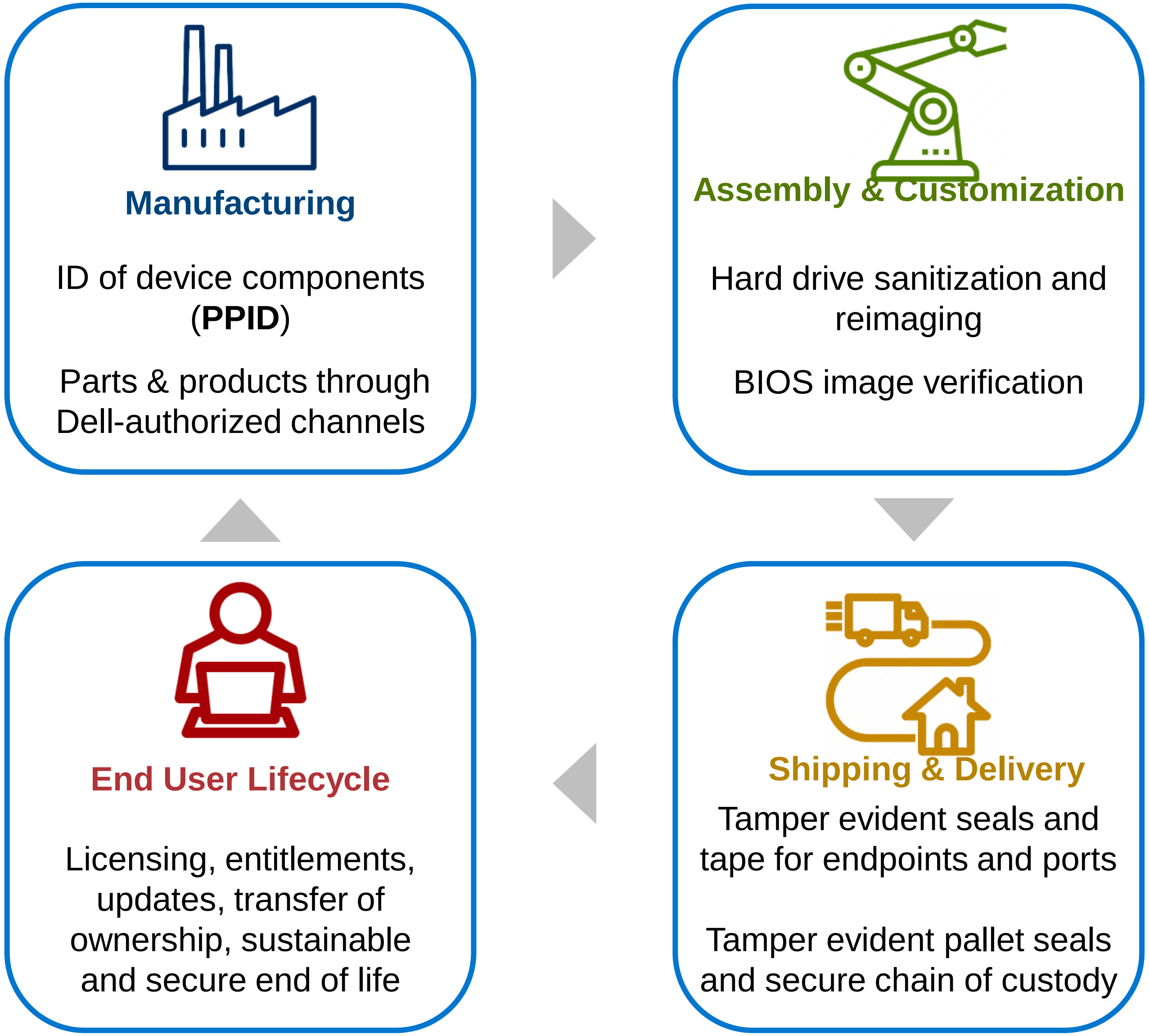
Ensure devices are not tampered or counterfeit components are not inserted before shipping

Software Integrity

Ensure no malware is inserted in firmware or device drivers before shipping and prevents coding vulnerabilities

Physical Security

High level of physical security in factories, robust screening and hiring practices, annual compliance training and certification



Manufacturing

ID of device components (**PPID**)

Parts & products through Dell-authorized channels

Assembly & Customization

Hard drive sanitization and reimaging

BIOS image verification

Shipping & Delivery

Tamper evident seals and tape for endpoints and ports

Tamper evident pallet seals and secure chain of custody

End User Lifecycle

Licensing, entitlements, updates, transfer of ownership, sustainable and secure end of life

Dell SafeSupply Chain solutions for supply chain assurance

Dell Trusted Workspace

Built-on Software Security

Strengthen the security of any fleet with advanced protection via an ecosystem of best-of-breed partners curated by Dell.

SafeGuard and Response • SafeData

Built-in Hardware & Firmware Security

Prevent and detect foundational attacks with deep defenses at the BIOS/firmware and hardware levels.

SafeBIOS • SafeID

Built-with Supply Chain Security

Trust hardware is tamper-free on delivery with optional paid add-ons for extra supply chain assurance.

SafeSupply Chain

Key Dell SafeSupply Chain Offers

Secured Component Verification

(SCV)

Tamper-evident packaging

Hard drive wipes

Platform Certificates and Dell Secured Component Verification

What are Platform Certificates?

A supply chain security measure to ensure that high-risk PC components are not compromised or hacked on the way from the manufacturer to the customer

Why All the Talk of Platform Certificates?

- 2021 US Executive Order on Supply Chain Security: platform certificates will become mandatory for some segments
- Last year, NSA published a hardware procurement guide last year that calls for adding platform certificate solutions.
- In fact, it is becoming a requirement for upcoming US Federal purchases

National Security Agency | Cybersecurity Information Sheet

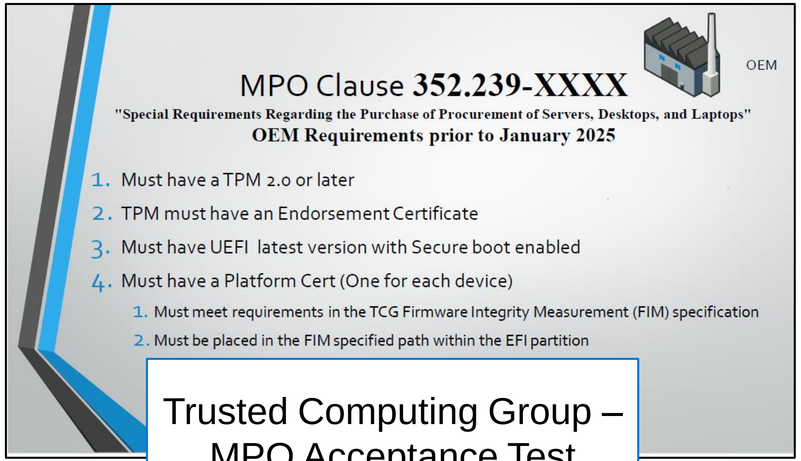
Procurement and Acceptance Testing Guide for Servers, Laptops, and Desktop Computers

Executive summary

Enterprise-grade servers, laptops, and desktops should be procured with a robust set of security artifacts, configurations, and capabilities. The security artifacts enable several risk mitigation techniques that should be used with an automated Acceptance Test process. This guidance is intended to:

- Encourage the implementation of enterprise Acceptance Testing.
- Inform procurement professionals what provisions will be needed to support Acceptance Testing.
- Inform original equipment manufacturers (OEMs) on what artifacts and capabilities will be needed to support an Acceptance Test.

NSA Procurement and Acceptance Testing Guide, Sept 2023



MPO Clause **352.239-XXXX**

"Special Requirements Regarding the Purchase of Procurement of Servers, Desktops, and Laptops"

OEM Requirements prior to January 2025

1. Must have a TPM 2.0 or later
2. TPM must have an Endorsement Certificate
3. Must have UEFI latest version with Secure boot enabled
4. Must have a Platform Cert (One for each device)
   1. Must meet requirements in the TCG Firmware Integrity Measurement (FIM) specification
   2. Must be placed in the FIM specified path within the EFI partition

Trusted Computing Group – MPO Acceptance Test Technical Overview (April 2024)

SCV Use Cases

Who is SCV designed for?

- Federal, State and Local Governments who will be required to have additional security measures
- Large companies who will align with similar measures based on US Executive Orders
- Companies that have greater need of IP security protection
- Companies that have more stringent security needs to due to increased compliance requirements (financial, pharmas, for example)

SCV Benefits

- Verify devices are secure through setup
- Enhance IT security
- Improve IT security operations

Secured Component Verification Versions

SCV (on Cloud)

Worldwide; commercial PCs

SCV (on Device)

North America; select SKUs

Availability

	SCV (on Cloud)	SCV (on Device)
Available	Worldwide	North America
IT Environment	Cloud-based	Air gapped
Certificate Creation	At factory	At 2nd touch facility
Verification Certification Storage	Off-host (secure location in cloud via Dell online portal)	On-host (secure location in EFI partition of local hard drive)
Certificate Retrieval	Dell attestation tool with root cert pre-loaded; retrieves platform certificate from Dell cloud. Uses the Dell Trusted Device app and SupportAssist for Business	Customer retrieves root certificate from support.dell.com and platform certificate from EFI partition on local hard drive
Attestation/ Authenticity	Use TechDirect to validate authenticity of PC hardware	Use 3rd party tool, loads Dell-provided root and platform certificates, validates authenticity on PC hardware
Supported Products	Wide range of devices across Dell commercial lineup, including most recent products.	Select, existing models across Latitude, OptiPlex and Precision

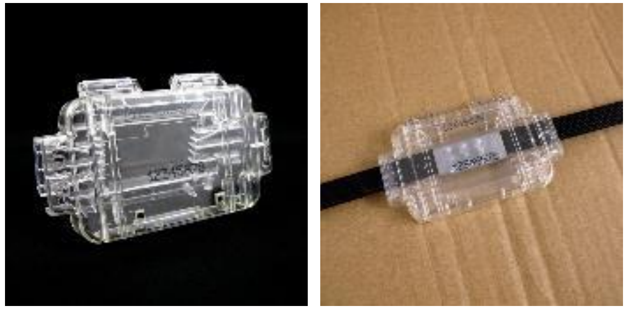
Other Supply Chain Offerings (North America)

Safe SupplyChain – Tamper-Evident Services

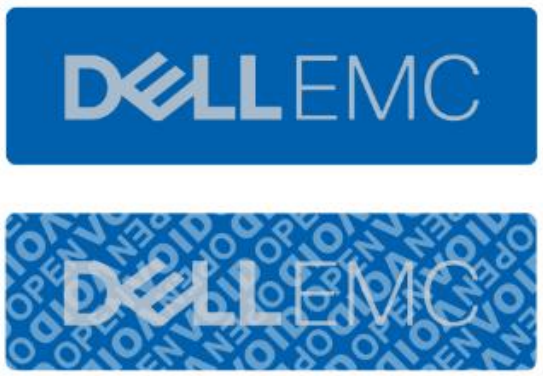
Tamper-Evident pallet and product seals available in North America

- Dell **tamper-evident seals** added to seal the system before shipping to final destination
- Dell **tamper-evident tape** added to seal the system box
- Dell **tamper-evident pallet seals** added before shipping to final destination
- Added separately to full pallet orders

Pallet seals



Tamper Evident Seals



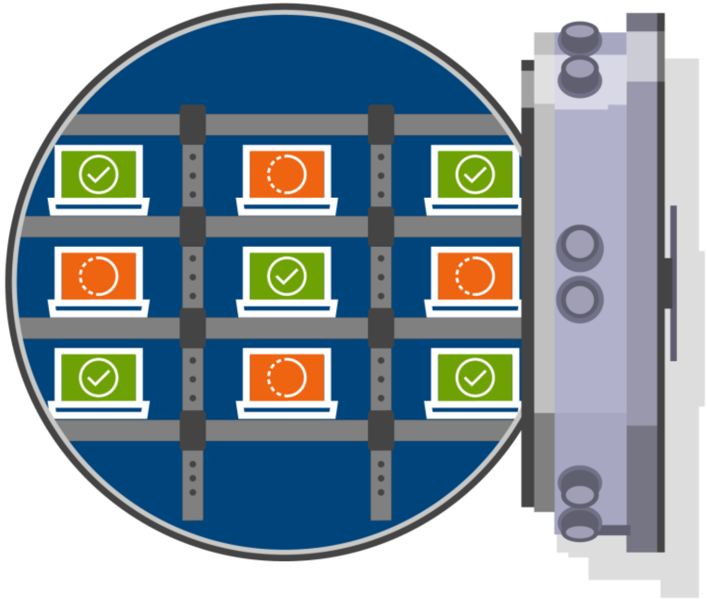
SSG155-48BL

Example of tampered label

Safe SupplyChain Data Sanitization Services

Device Sanitization and Reimaging

- **NIST 800-88 secure hard drive wipe** mitigates the risk of compromised hard drive firmware prior to imaging
  - **NIST 800-88 Clear** wipe & sanitization for SSD drives
  - **NIST 800-88 Purge** wipe & sanitization for HDD drives
- **Hard drive reimaging** according to customer contract specifications



Closing

Summary

How to access solutions

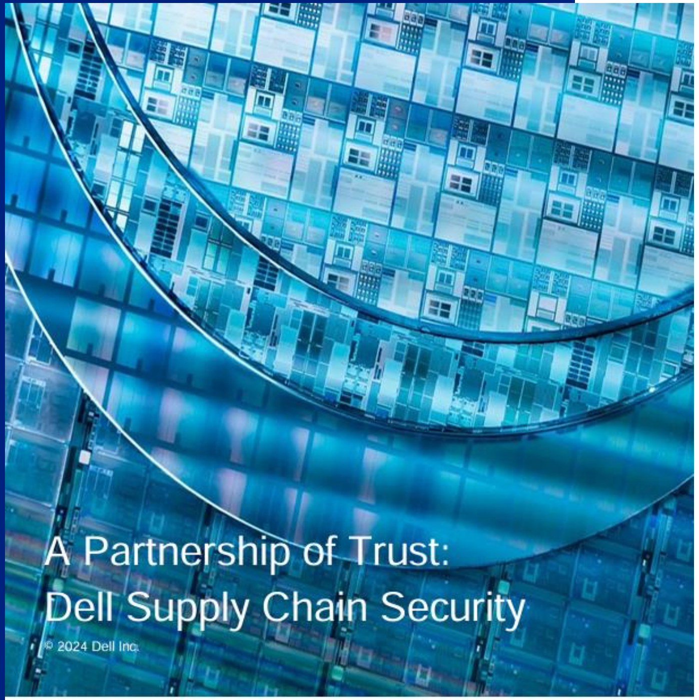
Learn more

Summary

- Supply chain attacks are on the rise
- Dell has market-leading supply chain security and optional supply chain assurance offers
- Secured Component Verification is our platform certificate offer that provides even greater security from factory to setup
- North American customers can gain additional security with tamper-evident seals and tapes shipped from our 2nd touch facility along with SCV (on Device)

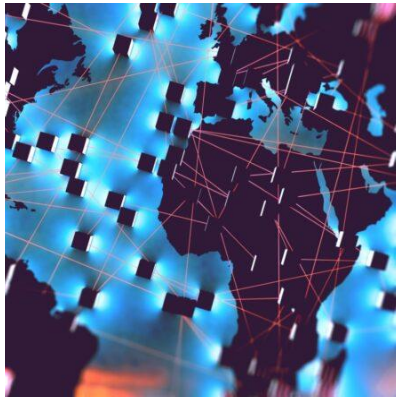
Learn More

dell.com/endpoint-security



[Dell Supply Chain Security White Paper]

[Blog; Keep Device Trust Close to the Vest]



[Blog: Shore up Your Defenses]

DELL Technologies
Data Sheet

Secured

With Secured Com
knowing that critic

Key benefits

- Verify devices are se
setup: SCV ensures
commercial devices
and ready for deploy
exactly as they were
Dell manufacturing.
- Enhance IT security
your security standa
Zero Trust principles
emerging industry g
to meet the most de
requirements for se
infrastructure.
- Improve IT security
Add SCV to your sta
operating procedure
deployment for a lo
risk enhancement th
secures your overall
operations.
- Accelerate IT innova
added peace of min
devices are built and
intended, IT teams c
other areas such as
related innovations.
- Secured Component
provides digital pro
chain security by en
that the Dell system
components ordered
the components tha
manufactured and a
the factory.

DELL Technologies
Data Sheet

Dell SafeSupply Chain

Commercial

Optimize Endpoint Security

Security-sensitive organizations are becoming increasingly aware of the potential threats to Information and Communication Technology (ICT) supply chains. Threats continue to evolve as nefarious actors try to take advantage of any weak link in the supply chain that will allow them to gain access to protected information or to disrupt a corporations day to day activities. Threats include malware, coding vulnerabilities, and counterfeit electronic components that are inserted into products within the supply chain - any time between the initial design and development of the product through actual delivery to customers. Recognizing this potential risk to the business, Dell continues the development of stronger ICT supply chain security solutions.

Dell Technologies is committed to being the preferred supplier of end-to-end, cutting-edge technology solutions to customers to provide added security straight out of the box. Dell leverages a robust Supply Chain Risk Management (SCRM) Program to ensure foundational controls for all product supply chains meet or exceed customer expectations and industry standards. The program focuses on giving customers the confidence that the products acquired from Dell Technologies are exactly what they expect them to be, nothing more and nothing less, and that they will operate as intended. This is accomplished through an evolving strategy that relies on multiple layers of supply chain security and integrity controls throughout the entire supply chain lifecycle.

Delivering Trustworthy Products Straight Out of the Box

Dell Technologies Supply Chain Standard Practices

Dell's intent is to fulfill customer requirements with authentic, Dell-branded systems and accessories. As the OEM, Dell can ensure that the customer receives products that come through Dell-authorized channels. Preventative and detective control measures that protect physical assets, inventory, information, intellectual property and people include the following:

- Customer Information Security (CIS) controls and requires annual employee compliance training.
- All employees submit to appropriate background checks in accordance with local laws and regulations and all employees working in the Dell U.S. are U.S. citizens.
- Certified C-TPAT partner working with U.S. Customs and Border Protection (CBP) and other principle stakeholders of the international supply chain community to identify potential security gaps, and implement specific security measures and best practices to advance protection of the global supply chain. All Dell Client Products (desktops, laptops, and All-in-Ones) and PowerEdge Servers have been certified at Tier 3 while products other than Dell Clients and PowerEdge Servers have been certified at Tier 2.
- Accredited member of Transported Asset Protection Association (TAPA) and follows TAPA FSR (Freight Security Requirements) standards for the purpose of addressing cargo security threats that are common to the high tech industry. Dell logistics and transportation providers are required to be TAPA "A" compliant.
- Product design incorporates Secure Development lifecycle (SDL) based on industry standards (ISO/IEC 27034) and best practices (SAFECode).
- Product designs include BIOS protections in accordance with NIST 800-147 guidelines. All Dell BIOS development and coding is performed or managed by Dell employees.

Dell SafeSupply Chain
© 2024 Dell Inc. or its subsidiaries.

Datasheets:

- [SafeSupply Chain]
- [SCV]

DELL Technologies

Questions?