A Partnership of Trust: Dell Supply Chain Security

© 2024 Dell Inc.

Table of Contents

Why Does Supply Chain Security Matter?

Dell's approach to security runs deep in our DNA. We provide security through every stage of the supply chain: from designing a product, through sourcing the components and making the product, to delivering it to the customer. At Dell, our aim is to deliver trustworthy products straight out of the box and into the hands of our valued customers.

Supply chain security is pivotal to protecting critical data and information from hackers and other cyber security threats, as well as complying with legal and regulatory guidelines. As cyber threats grow exponentially each year, they expose vulnerabilities within information technology (IT), hardware and software systems through malware attacks, piracy, and unauthorized access. Taking steps to improve security protocols to mitigate against these threats remains the most effective method to maintaining a secure and resilient supply chain.

A single ransomware incident can lead to operational disruptions, lost revenue, compromised data, diminished productivity, and a tarnished brand or corporate reputation. Given the uptick in these crimes, customers are actively seeking assurance from technology companies that they are taking appropriate actions to protect the privacy of their data and that their products are authentic, namely that they are free from malicious modification.

In *Four Keys to Navigating the Hardware Security Journey* by Futurum, the author stated that 44% of organizations faced at least one Hardware-Level or Basic Input Output System (BIOS) attack during the last 12 months, making securing IT hardware a priority.

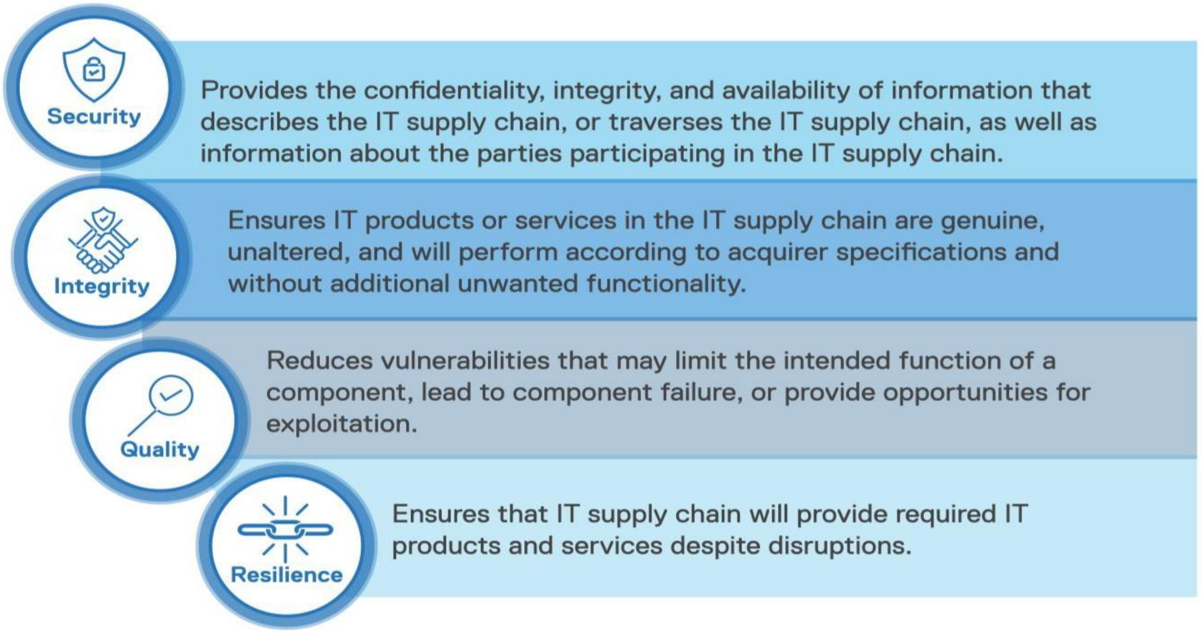
Dell constructed its business model with a partnership of trust among its people, customers, and suppliers.

Dell Technologies understands the importance of providing a safe and secure digital environment and has taken the necessary steps to increase the security of its supply chain ecosystem. With a safe supply chain in place, Dell believes that creating a partnership of trust and collaboration with key stakeholders – both upstream and downstream – is essential to delivering the best value of innovative technologies to customers.

The Dell Supply Chain

Dell takes a holistic approach to protecting its supply chain and delivering solutions that customers can trust. The strategy of "defense-in-depth" and "defense-in-breadth" involves multiple layers of controls to mitigate threats that could be introduced into the supply chain. These controls, along with effective risk management, help establish supply chain security.

Dell values the capabilities of security, integrity, quality, and resilience when determining the implementation of controls throughout each phase of the supply chain.



Security

Provides the confidentiality, integrity, and availability of information that describes the IT supply chain, or traverses the IT supply chain, as well as information about the parties participating in the IT supply chain.

Integrity

Ensures IT products or services in the IT supply chain are genuine, unaltered, and will perform according to acquirer specifications and without additional unwanted functionality.

Quality

Reduces vulnerabilities that may limit the intended function of a component, lead to component failure, or provide opportunities for exploitation.

Resilience

Ensures that IT supply chain will provide required IT products and services despite disruptions.

Security in the Dell Supply Chain

Supply chain security is the practice and application of preventing and detecting control measures that protect physical assets, inventory, information, intellectual property and people. Addressing information, personnel, and physical security helps secure the supply chain by reducing opportunities for the malicious introduction of malware and counterfeit components into the supply chain.

Supply chain security is Dell’s top priority. It employs a multifaceted approach to protecting its products at every stage of the production lifecycle, from conception, design prototype implementation, set into production, deployment, maintenance, to validation.

Securing Data

Securing data in the supply chain involves practices, policies, and principles that protect digital data against unauthorized access or use that could result in exposure, exploitation, deletion, or corruption of the data. It involves information, personnel, and physical security.

Dell incorporates overlapping practices to secure digital data, including establishing robust administrative and physical controls and maintaining multi-layered access protocols to protect sensitive customer data. Dell data governance efforts focus on optimizing relationships and security postures to proactively identify vulnerabilities and mitigate risk. To protect the confidentiality, integrity and availability of customer data, Dell extends trust and assurance throughout our end-to-end value chain. Dell takes multiple steps to protect digital data and other customer-sensitive information, in a manner that minimizes the impact on end-user functionality.

Information Security

Through the normal course of business, Dell collects and uses information about products, solutions, suppliers, and partners throughout the supply chain lifecycle. Robust security measures guard sensitive information against exposure and exploitation. For example, Dell and its partners use a combination of encryption methods and private communication channels to transfer data. This includes secure protocols and encapsulation technologies, which align with industry best practices.

Dell secures its internal network environment and associated assets through controls such as virus detection, strong password enforcement, email attachment scanning, system and application patch compliance, intrusion prevention, and firewalls. Dell has added more enhanced controls to help protect against malware and misuse of assets.

Dell also employs the principles of “separation of duties” and “least privilege” to guide key controls throughout the supply chain, which help prevent misuse of data access across the business. These principles help ensure that access to sensitive information is granted only to individuals that have a need to perform their assigned duties.

Personnel Security

Dell’s internal security efforts involve screening employees and restricting their access to company data and resources. Dell policy requires employees throughout the supply chain, including those at contract suppliers, to go through a pre-employment suitability screening process. This process includes security background checks, drug screening, identity verification, and application information verification as applicable and permissible by law.

Dell employees maintain a culture of security and must undergo annual security awareness and compliance training designed to mitigate the risk of behavior that may put products at risk throughout the supply chain. This training conforms to government standards and industry protocols for supply chain security. In addition, employees receive security developments throughout the year in the form of corporate newsletters, internal and external security websites, customer whitepapers, seminars, participating in corporate security awareness campaigns, and taking additional online courses and video training. Additionally, employees and contractors must sign and agree to confidentiality provisions that protect intellectual property, customer information and other sensitive data not only during their employment but also once they leave.

Physical Security

Facilities used to design, build, customize, or fulfill Dell’s product orders must demonstrate compliance with several internationally recognized physical security standards, to include the Transported Asset Protection Association (TAPA), American Society for Industrial Security (ASIS), International Standards Organization (ISO) and the Business Alliance for Secure Commerce (BASC).

Dell physical and cybersecurity audits of suppliers and facilities include the inspection of digital closed-circuit TV cameras, access control systems, intrusion detection and guard service protocols. Other controls are applied to protect Dell cargo during the shipping and logistics process, including tamper-evident packaging, cargo locks and seals, and threat intelligence monitoring of key freight lanes. Internet of things (IoT) tracking devices are also deployed on select shipments to enable real-time telemetry data monitoring to escalate any security non-compliance events observed during transit.

Dell also maintains certifications in multiple secure trade and commerce programs such as Tier 3 status with the United States Customs and Border Protection's Customs Trade Partnership Against Terrorism (C-TPAT), Canada's Partners in Protection (PIP), Singapore's Secure Trade Partnership and Authorized Economic Operator (AEO) status in several other nations. These programs are recognized by international member states of the World Customs Organization and demonstrate "best in class" supply chain security standards within the private sector. They also focus on supplier accountability, security management policies, counter-smuggling, trafficking controls, and tamper prevention – all intended to secure trade across international borders.

Integrity in the Dell Supply Chain

Supply chain integrity helps ensure that customers' products are delivered safely and once received, operate as intended. An important feature of supply chain integrity is the development of baseline specifications of hardware and software, which is used to verify a product's authenticity.

Hardware Integrity

Dell has implemented robust quality control processes to help minimize the risk of counterfeit components infiltrating our supply chain. Dell's new product introduction process verifies the sourcing of materials from Dell's approved vendor list and match the bill of materials (BOM). Dell procures parts directly from the Original Design Manufacturer (ODM) or Original Component Manufacturer (OCM).

Dell's Quality Management System verifies ongoing compliance to engineering specifications and processes, including sourcing from approved vendors. Material inspections during production help identify components that are mismarked, deviate from normal performance parameters or contain an incorrect electronic identifier.

To enable appropriate traceability, Dell identifies all key components by a serial number label or marking, a Dell-prescribed Piece-Part Identification (PPID) label or an electronic identifier that can be captured during the manufacturing process. PPID provides a foundation for downstream component verification capabilities offered by Dell, like Secured Component Verification (SCV). Additionally, Dell maintains ISO 9001 certification for quality control practices at all global manufacturing sites. Dell's adherence to these processes and controls helps minimize the risk of counterfeit components being embedded within Dell products.

Software Integrity

Dell ascribes to software engineering best practices by integrating security throughout the development process for any code, including operating systems, applications, firmware and device drivers. Third-party components integrated into Dell's software are purchased from trusted suppliers, plus Dell verifies the integrity of these components prior to integration. Dell reduces opportunities for the exploitation of product security flaws by incorporating Secure Development Lifecycle (SDL) measures throughout the Design and Development process. These measures are tightly aligned with Software Assurance Forum for Excellence in Code (SAFECode) guidelines[1], ISO 27034[2] and the National Institute of Standards and Technology (NIST) SSDF.

Dell's proactive verification, validation, and security testing activities throughout the software component's lifecycle help to ensure integrity and reduces the likelihood of the introduction of malware or malicious coding. A robust cybersecurity program can improve software integrity by preventing unauthorized access to source code and minimizing the potential for malware to be introduced into a product before it is shipped to the customer.

As part of Dell's software supply chain security controls, and in alignment with U.S. Executive Order 14028 and NIST standards, a Software Bill of Materials (SBOM) data is available for select products across our portfolio. Dell SBOM data adheres to the Software Package Data Exchange (SPDX) standard and is provided in JSON format. SBOM data enables robust software supply chain transparency and rapid vulnerability scanning and response and is a critical component of Zero Trust Architecture.

Design and Develop

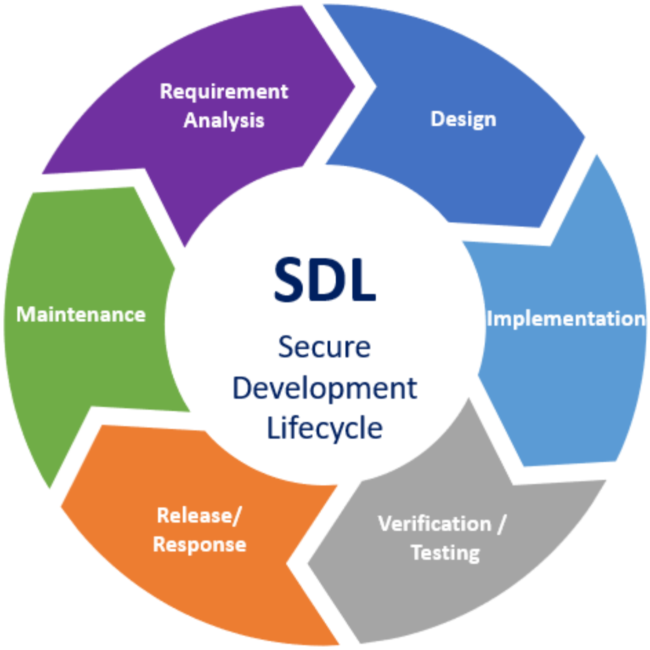
Dell uses a mature and proven SDL program for security when it designs its hardware products and develops its software/firmware code. This program includes processes and policies that help ensure that secure code has been implemented at the time of product hardware and software inception and continue throughout the development cycle. Basically, security is built in from the start. For Dell to effectively execute this program, its engineers are required to take mandatory security training before handling any code. In addition, Dell assigns security champions to each product development team to drive a security culture within the organization.

Secure Development Lifecycle

Dell's SDL program is based on regulatory guidance, industry standards, and best practices. It includes a comprehensive catalogue of security controls that Dell product teams implement throughout the product development lifecycle to produce secure code. In addition to the SDL program, which is aligned with both the NIST SP.800-218 (Secure Software Development Framework (SSDF) and the ISO/IEC 27034 standard for Application Security, Dell collaborates with many industry standards organizations such as SAFECode[3], Building Security in Maturity Model (BSIMM) and the Institute of Electrical and Electronics Engineers (IEEE) Center for Secure Design to ensure that SDL controls are tightly aligned with industry best practices.

Dell's SDL includes both analysis activities and prescriptive proactive controls around all risk areas. Dell integrates analytic activities, threat modelling, static code analysis, vulnerability scanning, and security testing to holistically identify and remediate potential security weaknesses and vulnerabilities throughout the development lifecycle. SDL helps mitigate many common design weaknesses in the software and firmware, including but not limited to: unauthenticated code updates, exposed or enabled debug interfaces, insecure default settings and hard-coded passwords. Dell's SDL leverages tools that have been developed by industry and public-private partnerships to identify and address new and existing weaknesses and vulnerabilities discovered over time in code, to include the CVE (Common Vulnerabilities and Exposures)[4] and CWE (Common Weaknesses Enumeration)[5] published by MITRE, the OWASP (Open Web Application Security Project) Top 10[6] and the SANS Top 25 Most Dangerous Software Errors[7].

Dell's SDL program governs the design and testing of software and firmware. Engineers are required to follow a set of strict protocols defined by the SDL when it begins to design new product features and functionality. This process helps to prevent vulnerabilities, in both proprietary code and third party components. During product design, the engineering team creates threat assessments and a model to determine the threat surface and focus of testing following code development. For the engineers developing software or firmware, they begin with static code analysis—an automated process which uses special tools for finding and fixing weaknesses and vulnerabilities. They then test the process features by conducting a line-by-line reading of the source code. It is a rigorous method that usually points to previously unknown mistakes in the code rather than malicious activity. However, these protocols provide additional assurances that the source code is safe and secure.



[1] https://safecode.org/ Last reviewed January 9, 2023.
[2] https://www.iso.org/standard/44378.html Last reviewed January 9, 2023.
[3] https://safecode.org/ Last reviewed January 9, 2023.
[4] https://cve.mitre.org/ Last reviewed January 9, 2023.
[5] https://cwe.mitre.org/ Last reviewed January 9, 2023.
[6] https://owasp.org/www-project-top-ten/ Last reviewed January 9, 2023.
[7] https://www.sans.org/top25-software-errors Last reviewed January 9, 2023.

Towards the end of the design stage, engineering teams provide risk assessments by using special tools to scan for known security vulnerabilities and verify that the threat model is accurate. Software in the combined integration and delivery pipeline leverages the SDL automation in building, testing and deployment of applications, ensuring that security is integrated at each phase of the lifecycle. Finally, a team of expert hackers are at times directed to undertake penetration testing—depending on the outcome of the threat assessment and model. This team may find potential vulnerabilities that were missed in the earlier phases. These findings are mitigated based on risk, and any additional identified exposure is documented and corrected.

Additional information on Dell's Secure Development Lifecycle can be found on the Dell Security and Trust Center.

Firmware Digital Signing

One potential threat to any supply chain is the risk of unauthorized code or data modifications. Dell engineers add a cryptographic digital signature to software, application and firmware to enable confirmation of authenticity and integrity—a process known as code signing.

Digital signing follows these basic steps:

- Dell's Core BIOS is architected and developed mostly in the U.S. for Dell commercial client products (OptiPlex, Latitude, Precision and XPS Notebooks) and Dell servers and storage.
- PC and data center infrastructure Original Equipment Manufacturers (OEMs), including Dell, incorporate chipset and BIOS firmware components provided by technology partners.
- Dells firmware development team select platform-specific features and integrated technology partner firmware into Dell's Core BIOS.
- Final production BIOS builds and digital signing are performed on all commercial systems physically located within Dell facilities in the U.S.

Penetration Testing

Penetration testing, or "pen testing," has become synonymous with mature security practices across the industry. Dell leverages in-house teams and external vendors to pen test its PCs, servers, and storage devices while these products are still in the engineering phases of development. These tests focus on physical access and Dell prioritizes them based on risk assessments of individual components integrated into the device.

BIOS Protections

BIOS is firmware that facilitates the hardware initialization process and transition control to the operating system. It controls the hardware device. If an attacker manages to corrupt the BIOS, he would gain control of the device because of the BIOS's unique and privileged position within the device architecture.

Dell has implemented procedures across our servers, storage products, and PCs in accordance with the NIST SP 800-147, BIOS Protection Guidelines. These policies specify that only signed and authorized BIOS should run on the system and include security guidelines and management best practices which prevent the BIOS from attack.

Dell deploys silicon-based security and cryptographic hardware root of trust (HwROT) to authenticate server and storage booting and firmware updates. Read-only cryptographic keys are burned into the silicon microchips of processors used in Dell designs so that they cannot be altered or erased. At power on, the chip verifies that the BIOS code is legitimate. This technology significantly mitigates the risk of undetected BIOS modification and reduces the risk of pre-boot malware or unwanted functionality.

Additionally, Dell created BIOS safeguards that comply with SP 800-193 NIST Platform Firmware Resilience standards. These ensure that unauthorized BIOS and firmware code simply cannot run. If the code is somehow replaced with malware, the device will not function. This resilience is intended to last for the device’s lifespan, from deployment to decommissioning.

Chassis Intrusion

Chassis within Dell PowerEdge products are registered with the Integrated Dell Remote Access Controller (iDRAC)—a specialized microcontroller that sits on the motherboard and allows administrators to update and manage the system, even when the server is turned off. This configuration makes it possible to track the source of an intrusion.

Similarly, many Dell commercial client devices include a chassis intrusion capability that can be monitored via management tools, including Microsoft Configuration Endpoint Manager and Dell Command Suite.

Additional Built-In Security Measures: Dell Servers and Storage

Dell prides itself on the security protocols for its PowerEdge servers. The 15th and 16th Generation PowerEdge server capabilities provide cyber resilience features to protect, detect, and recover from attacks, as well as a locked-down posture for a Zero Trust approach. By working together, these PowerEdge security controls provide a comprehensive security solution.

PowerEdge provides multiple tools and security features to enable strong controls of system maintenance and data integrity:

- Platform silicon root of trust anchors other security controls including UEFI secure boot.
- Component attestation through Security Protocol and Data Model (SPDM).
- Firmware integrity through cryptographically signed updates.
- Protect data integrity and confidentiality through strong flexible encryption controls.
    - Protect data-at-rest against unauthorized access with self-encrypting drives and local and external key management.

    - Data-in-use encryption with confidential compute.

- Establish a secure, encrypted connection using SSH SSL/TLS 1,3 and update with Automatic Certificate Renewal.
- Dedicated iDRAC network module.
- Enforce least privilege access with strong identity using multifactor authentication (MFA), single sign-on, and role and scope-based access control.
- Dynamic System lockdown.

For more information, please refer to the Cyber Resilient Security in Dell PowerEdge Servers 2023 whitepaper.

Like servers, Dell's storage platforms employ equally robust security measures required to protect customer data.

- Dell PowerStore and PowerScale have followed applicable security standards such as NIST SP800-193 Platform Firmware Resiliency Guidelines and NIST 800-147 BIOS Protection Guideline specifications. These specifications are integrated into our Trusted Platform Module (TPM), digitally signed firmware updates, Unified Extensible Firmware Interface (UEFI) secure boot, Intel bootguard and HwROT product capabilities.
- Additionally, PowerScale and PowerProtect products built on PowerEdge hardware benefit from PowerEdge security resilience features directly.
- Next generation PowerStore, PowerScale and PowerMax build on top of the existing features to include HwROT at the disk array and fabric levels, setting Dell apart from its competitors. In addition, we have upgraded the BMC HwROT to support National Security Agency (NSA) Top Secret grade algorithms and longer service requirements. Similarly, with the enablement of secure UEFI boot features and cryptographic signing, HwROT ensures that malicious or unauthorized BIOS, firmware, drivers or application code simply cannot be installed or run within the storage platforms.
- Additionally, the new generation of Dell data storage devices—PowerMax and PowerStore—are fitted with additional lines of defense in the shape of TPM-by-default, data-at-rest and data-in-flight encryption and configuration locking. Typically, data is stored and protected by passwords, firewalls, basic encryption, and anti-virus software, but PowerMax and PowerStore have data-at-rest encryption that is validated to Federal Information Processing Standard (FIPS) 140-2. Our solutions encrypt the data and delivers integration with external key managers, enabling customers to simplify security through a centralized key management platform.

Additional Built-In Security Measures: Dell PCs

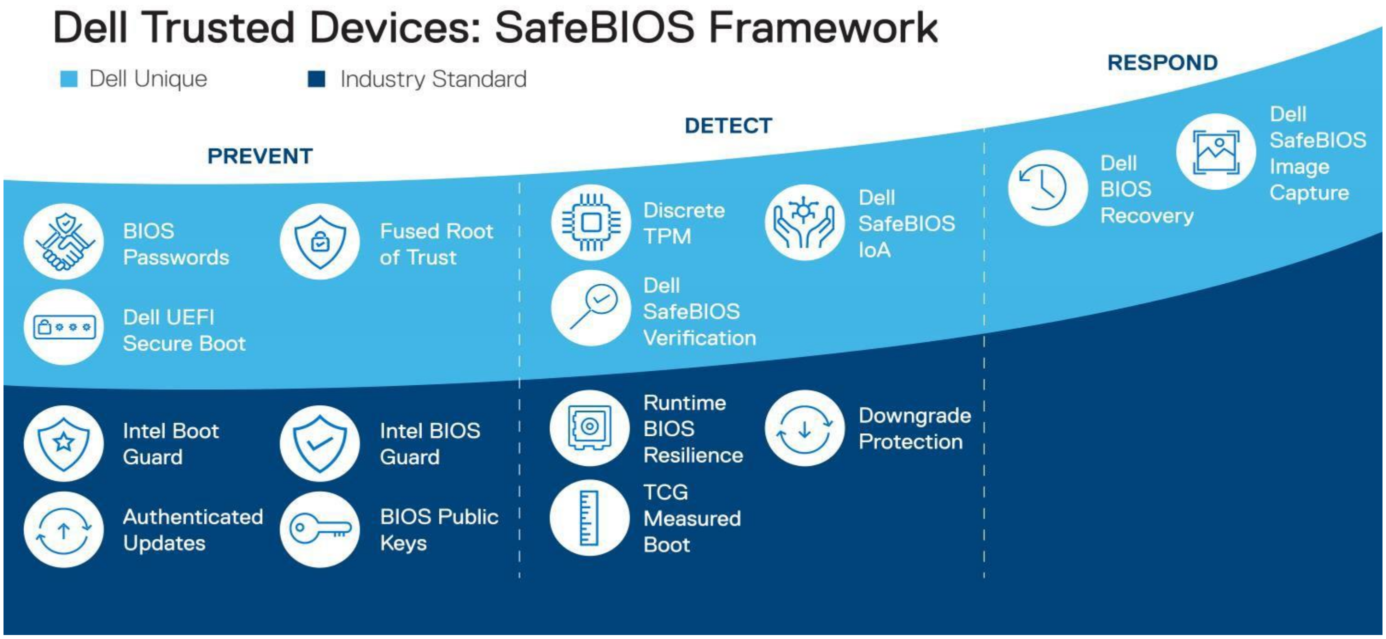
Dell has invested in the development of innovative world-class security technologies for its commercial PCs, resulting in the industry's most secure commercial PCs. While some of these features are more applicable to PCs in use than in production, some features can be used during the production process to increase assurance and prevent potential malware intrusion.

These built-in security features include:

- Secure Off-Host SafeBIOS Verification – A secure verification of the BIOS image against a Dell-hosted off-host source.
- Secure Off-Host Firmware Verification – A secure verification of the critical firmware leveraging the Intel Manageability Engine associated with Intel vPro.
- Dell SafeID with ControlVault – Provides hardened storage of end-user credentials—the highest value target for attackers in a single chip.
- SafeBIOS Indicators of Attack – Detects advanced endpoint threats using behavior-based threat detection at the BIOS level.
- SafeBIOS Image Capture – If a compromised BIOS image is detected, it is captured and stored securely on the PC for retrieval and analysis to determine the nature of the attack.
- Dell Secured Component Verification (SCV) – Captures and generates a manifest of installed components which is cryptographically signed by a Dell Certificate Authority and stored securely within the system for future validation.

Dell commercial PCs incorporate a TPM, which coordinates with the BIOS during the UEFI boot process to maintain the authenticity of BIOS measurements, most importantly a Root of Trust for Measurement (RTM) and a Root of Trust for Reporting (RTR).

The Trusted Computing Group (TCG) Measured Boot uses the PC's TPM as a protected storage area for storing hashes of BIOS and firmware code that is loaded and executed in the boot process. The TPM is designed to store these events in a secure way that can be verified post-boot through a process called attestation.



Dell Trusted Devices: SafeBIOS Framework

Dell Unique
Industry Standard

PREVENT
BIOS Passwords
Fused Root of Trust
Dell UEFI Secure Boot
Intel Boot Guard
Intel BIOS Guard
Authenticated Updates
BIOS Public Keys

DETECT
Discrete TPM
Dell SafeBIOS IoA
Dell SafeBIOS Verification
Runtime BIOS Resilience
Downgrade Protection
TCG Measured Boot

RESPOND
Dell BIOS Recovery
Dell SafeBIOS Image Capture

Dell BIOS supports two independent and persistent ‘tags’ to allow customers to discover and verify devices in their infrastructure. The Service Tag is programmed into the BIOS non-volatile RAM during the manufacturing process and is locked in place for the life of the system. This allows the device to be identified for general asset management and service or warranty support. The Asset Tag is also stored in BIOS Non-Volatile Random Access Memory (NVRAM) and can be set, changed or cleared by the customer. The BIOS Administrator password can be used to provide control of authorization to modify the Asset Tag.

Source

Following product design completion, it is transformed into a finished product. Dell directly manages about half of the global manufacturing sites it utilizes, while also working with and through a range of partner companies who supply additional manufacturing facilities as well as raw materials and individual components. Dell’s supplier selection process includes a rigorous onboarding process that involves several key procedures to help ensure each meets our high standards for integrity, security, quality and reliability. These suppliers are vital to successfully delivering high-quality products and mitigating the rising number of security threats.

Dell remains thorough in its selection process, with the goal of selecting not just a supplier, but a partner.

Supplier Relationship Management

The Dell supplier selection process begins with the commodity managers preparing a target list of suppliers who align to the broader category strategy including country, region, cost, financial health, quality needs, and more. Next, potential suppliers are sent a detailed set of product specifications, where they must provide line-by-line responses showing how they could meet the specifications. Those suppliers then undergo an in-depth Quality Process Audit (QPA), which includes a stringent security assessment. On-site QPAs is evaluate the end-to-end activities at the location. The security requirements go beyond industry standards to meet Dell requirements. Second, there is a "bench" level test of the devices—for instance, the evaluation of the motherboards or hard drives. Typically, this involves a reliability demonstration test and a comprehensive destructive physical analysis, where each device is broken into its component parts. The supplier's component or device is placed into the finished desktop, server, or other product to see how it performs.

Quality control in the Dell Supply Chain is equally as important as security and integrity in a secure supply chain.

This capability is crucial in the Source and Make phases. Processes and controls in place reduce potential vulnerabilities and opportunities for exploitation.

As a routine part of our Supplier Relationship Management (SRM) strategy and approach, strategic suppliers must undergo periodic performance reviews. Dell conducts a comprehensive review of its suppliers using a predetermined list of criteria, including cost, delivery, innovation, security, and adherence to Dell Supplier Principles, all of which are a condition of doing business with Dell. Procurement contracts contain Facility Security Requirements (FSR). Typically, Dell assesses and audits supplier factories against the company's expectations. If corrective actions are warranted, Dell will actively support the supplier's efforts to make necessary adjustments and assist the supplier in building new capabilities.

Dell's collaborative approach with partners includes direct and sub-tier supplier facilities. In 2021, Dell assessed 317 factories across 16 countries and audited them for compliance with the sector-wide Responsible Business Alliance (RBA) code of conduct, which is a set of social, environmental, and ethical industry standards. Additionally, Dell requires adherence to its Supply Chain Security Standards for our Logistics Service Provider (LSP) and ODM partners. These standards cover requirements in areas such as sourcing, cybersecurity, physical security, and security management systems—they are also used to measure against future Dell suppliers. Dell also requires LSPs to complete and submit an annual Risk Assessment and security self-audit to our dedicated Security and Resilience Organization.

Dell's continuous improvement model along supply chain focus areas creates a partnership we partnership with suppliers that produces robust program capability building to enable suppliers to build their own in-house capabilities.

The toughest customers are our best teachers, which is why Dell constantly challenges its suppliers to refine their best practices in security, quality, efficiency, logistics, and excellence. These initiatives—focused on sustainability, responsibility, integrity, quality, and resilience—have allowed Dell to build stronger ties with our suppliers, providing customers with greater levels of assurance.

Make

Today, there are numerous global supplier sites that produce approximately 53 million Dell products every year for tens of millions of customers in 180 countries. Dell directly manages about half of these factories. However, whether they are managed by Dell, ODM or contract manufacturers, all are required to meet the Transportation Asset Protection Association (TAPA) facility security requirements as well as comply with Dell Supplier Security Standards.

These standards cover the following requirements:

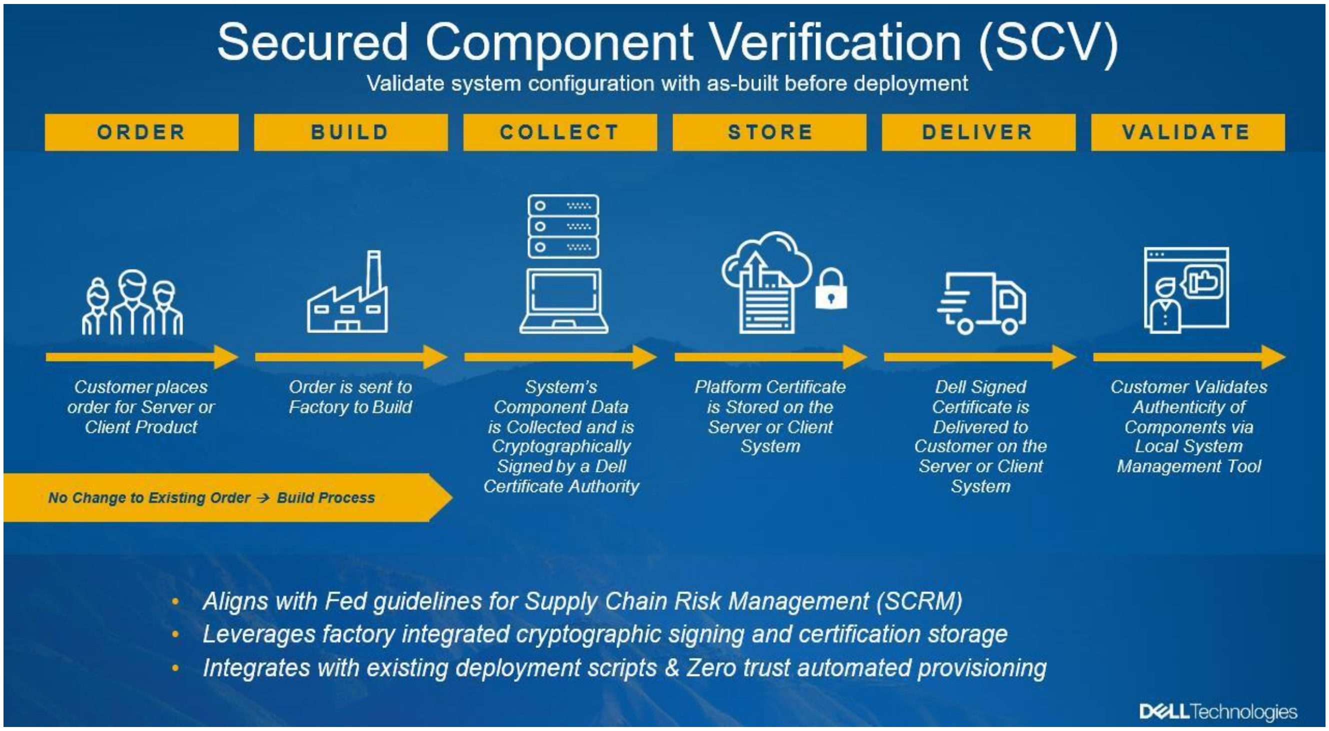
- **Sourcing Security**— requires the management of component sourcing, inventory controls, software and firmware security, and counterfeit mitigation.
- **Cybersecurity**— requires supplier to manage their own digital infrastructure from network security, encryption, patch, and vulnerability to incident management and reporting.
- **Physical Security**— requires the protection of physical assets, both in transit and at the manufacturing facility, by means of access controls, documentation, and other related procedures.
- **Security Management Systems**— requires suppliers to incorporate security into their overall operations, including but not limited to maintaining proper certifications, hiring practices, and security training.

Besides installing robust security practices in manufacturing facilities, Dell implements security protocols that ensure that all parts, components, and raw materials arriving at the site are genuine, authentic, and new. Dell uses an approved vendor list to procure product parts directly from OCMs or an authorized reseller of the OCM. Following the acquisition of the necessary components, OCMS have robust processes designed to minimize the risk of counterfeit components being embedded in hardware products, or malware being inserted into software or firmware. For example, Dell sites implement specific motherboard and Surface Mount Technology (SMT) assembly controls. Quality Engineers continuously augment and refine processes that inspect and verify motherboard parts and guarantee trusted personnel operate SMT lines. Following motherboard assembly, there are robust processes to authenticate their designs.

Verification and Tracking

Dell identifies, authenticates, and tracks high-risk components by affixing a unique PPID label to specific high-risk components. These PPID numbers contain information about the supplier, the part number, the country of origin, and the date of manufacture. Once assembled into the end product, the PPIDs for those components are recorded and associated with unique system tracking identification numbers to provide a history of the as- built configuration.

Another control available is Secured Component Verification (SCV), a Dell capability intended to provide last-leg assurance of product integrity from the time an order is fulfilled at the Dell factory to end-user delivery. Once a client or server product is built, a manifest of installed components is generated, cryptographically signed by a Dell Certificate Authority, and stored securely within the system. Once the product is received, the customer will have a designated SCV validation application, allowing them to verify and validate that no unauthorized system modifications have been made to the components.



Secured Component Verification (SCV)

Validate system configuration with as-built before deployment

ORDER — Customer places order for Server or Client Product

BUILD — Order is sent to Factory to Build

COLLECT — System's Component Data is Collected and is Cryptographically Signed by a Dell Certificate Authority

STORE — Platform Certificate is Stored on the Server or Client System

DELIVER — Dell Signed Certificate is Delivered to Customer on the Server or Client System

VALIDATE — Customer Validates Authenticity of Components via Local System Management Tool

No Change to Existing Order → Build Process

- Aligns with Fed guidelines for Supply Chain Risk Management (SCRM)
- Leverages factory integrated cryptographic signing and certification storage
- Integrates with existing deployment scripts & Zero trust automated provisioning

DELL Technologies

With the SCV, the end users can verify the list of components on-demand, without contacting support/reseller. As a result, validation happens quickly, on-demand, and under the control of the customer. This helps to reduce the time taken for validation and eliminates the need for manual intervention. It also allows the customer to double-check the components and ensure they are up to date. Furthermore, it helps to reduce costs associated with support calls.

Unauthorized modifications of components in a product can introduce significant risks, potentially compromising both the security and functionality of the device. Customers are at risk of experiencing security breaches, data loss, or system instability if unauthorized component replacements go undetected, as these changes may create vulnerabilities that malicious actors could exploit. The use of Secured Component Verification (SCV) helps customers identify alterations to their components and take appropriate action, if needed, which helps to mitigate these risks.

Smaller form factor components like processors and memory (as well as components used in storage and networking products that do not leverage the PPID labeling requirements or SCV capability), these components are uniquely labeled and identified by their OCMs either through serial numbers or electronic identifiers. That information is also associated with the unique system identifier for each of those products. From a quality standpoint, those controls allow Dell to monitor trends in performance for certain suppliers or lot codes. From an integrity and security standpoint, they allow authentication of the components prior to final assembly.

The core of this process is a series of inspections during production that help identify components that are mismarked, deviate from normal performance parameters, or contain an incorrect electronic identifier. Every system is functionally tested during the production process with the goal of closing any gaps in defensive measures to ensure that Dell products meet or exceed customer expectations and operate as intended.

Deliver

The final delivery of a product to the customer is the last stage of our supply chain process. Once a product is complete, it is either shipped directly from the factory to the customer or routed to a fulfilment hub. To get the product to the customer, Dell works with trusted logistics providers by air, land, rail, and sea that help fulfill more than 179,000 orders daily by carrying millions of products—enough to fill 34,000 ocean containers every year and 2.1 cargo jets every day. Each of our logistics service providers is required to conform with TAPA freight security requirements or similar regional guidelines. Compliance with Dell’s specially developed Freight Security Requirements, including a cybersecurity framework, is also required.

Above and Beyond: How Dell Protects Products During Delivery

One core feature of Dell’s logistics security program is a global set of risk management command-and-control centers. Located around the world, the centers are staffed 24/7 with subject matter experts who evaluate the latest information about transportation hotspots and track shipments using various monitoring technologies to ensure products reach their destination without disruption. These nodes utilize intelligence to advise real-time data and other information about planned routes. Specialists monitor various sensors on truck and cargo assets with an eye towards the changing threat levels in different regions, providing information to make decisions about the required level of security. Command center specialists can advise on in-transit security risks for the suppliers responsible for moving Dell products.

For dedicated loads carrying Dell freight, logistics service providers are obligated to use tamper-evident seals and door locking mechanisms. Additionally, Dell uses a variety of tracking devices ranging from telematics data, imbedded GPS, Bluetooth tags and other covert trackers equipped with radio frequency technology to recover stolen assets. These can alert the control centers if there are any unauthorized stops or route deviations. If requested and approved, our specialists can even order an armored truck or a security escort to accompany it and, in an emergency, they can send in a dedicated Emergency Response Team (ERT). Just as cybersecurity defenses are tested by commissioning penetration tests from professional hackers, Dell tests transport and logistics security by commissioning simulations with shipments to test the control center’s response and reaction protocols. Dell also has the capacity to tailor security solutions to meet customer needs.

In addition to security offerings, Dell can offer more services that further ensure integrity and document custodial control through the product’s journey to its destination.

Initially developed for a unique Supply Chain Program, these services are now available to others. For example, products stowed in the trucks can be placed into sealed boxes with security tape to prevent and signal tampering.

Additionally, boxes placed on pallets have metal crimps removed and replaced by special reinforced strapping. Following the loading of the pallets onto the truck, the doors are safely locked with a serial numbered bolt seal that is verified by the customer upon arrival.

After Delivery

Following the delivery of a customer's product, Dell's security protocols do not end there because new vulnerabilities—particularly software- and firmware-related—are discovered regularly across the industry. For this reason, Dell established a Product Security Incident Response Team (PSIRT), which is responsible for coordinating the response and disclosure of all identified product vulnerabilities in accordance with Dell's Vulnerability Response Policy. Dell strives to provide customers with timely information, guidance, and mitigation options to minimize risks associated with security vulnerabilities.

Typically, Dell releases security updates to customers as new threats emerge. Dell posts Security Advisories and Notices on the Security Advisories & Notices site. These updates might relate to our products or non-Dell products that customers use on Dell systems. Dell ensures that all updates to critical components—including BIOS, iDRAC, network adaptors, and power supplies—have a cryptographic signature. When combined with the hardware root of trust and the chain of trust that validates each component in the software and firmware, running the latest security update provides a strong cyber-resilient defensive boundary for Dell products.

Resilience in the Dell Supply Chain

Dell's global footprint, supplier relationships, and agility are key aspects of its resilience supply chain. Dell continues to focus on improving its security, as well as establishing business continuity, crisis management and disaster recovery programs across its operations. Through these strategic programs, Dell is taking proactive steps to identify and mitigate risk, including performing business impact analysis and testing. This resilience strategy has enabled Dell to develop a coordinated approach to assessing risk and making critical decisions with complex supply chain threats. Dell also maintains resilience and continuity of supply plans for critical operations and supplier locations and actively considers alternate locations as a part of our sourcing strategy. Through trusted relationships, high standards of responsibility, and integrity for ourselves and across our supply chain network, we drive greater flexibility in sourcing and reliable manufacturing our stakeholders can trust.

Supply Chain Digital Transformation

Dell's global supply chain footprint is substantial and complex. Therefore, prioritizing security and resiliency is essential to better serving the business and our customers.

In 2018, we began our digital transformation journey to improve our customer experience, build greater operational agility, and optimize our efficiency. Our approach to delivering the key capabilities across these experiences is based on three fundamental principles:

- Creating a modern, centralized, and scalable data infrastructure, and implementing rigorous quality and governance processes that ensure a single source of truth.
- Building custom solutions that are scalable, using an agile development process. This allows us to start quickly, align goals while developing, and at times fail fast if solutions or technologies fail to deliver.
- Creating a supply chain digital twin of our processes, data, relationships, and systems to integrate near real-time visibility and scenario planning into a single toolset and orchestration layer to create seamless interaction between the twins and enterprise systems.

Our data structure enables access to accurate and timely data from internal systems, customers, and suppliers while promoting data-driven solution implementations through:

- Data governance: establishing oversight to ensure data consistency for data created going forward. Includes activities such as establishing frameworks and governance processes, assigning business data owners and stewards, data governance quality monitoring and management.
- Defining the right master and transactional data: master data includes data related to suppliers, sites, items, products, and other reference data. Transactional data is stored using data models. These logical data models develop optimal relationships between fields and tables that help us map data flows to processes and systems.
- Building the right tools and infrastructure: deploying master/transactional data on optimal IT-supported infrastructure to ensure reliability.
- Content management system: creating a single management portal to access outputs of multiple tools across our global operations.

Future Focused: Leveraging Machine Learning and Artificial Intelligence (AI/ML)

Diving deep into our scalable applications, these tools help our supply chain team gain end-to-end control across demand generation, supply matching, disruption management, and setting inventory-level targets. Some of the solutions we have built are described below.

We have built a suite of intelligent planning and forecasting modules that employ various data science models and efficient workflows throughout the end-to-end planning process to improve resilience. These forecasting modules provide an automated statistical forecast with a suite of anomaly detection tools to identify and manage disruptive demand.

Combined forecast drives an inventory optimization engine that balances the highest possible customer service levels with the lowest required working capital structure. The blend of these approaches substantially improves our forecast accuracy, working capital efficiency, lead times, fill rate and on-time delivery.

We are scaling out our digital twin capabilities for the build-to-stock supply chain that would help us conduct what-if scenario analysis to evaluate business outcomes and assess risks when deploying new strategies.

Scaling the digital twin to incorporate potential challenges to the supply chain, such as constrained supply, natural disasters, business expansion, geopolitical tensions, and cyber-attacks will inform and assist executives to evaluate risk and develop strategies.

We are also developing machine learning models that can optimize inventory to minimize shortages and lower overstock inventory. As an extension of that, we are also building a dynamic inventory balancing application to facilitate and optimize rebalancing decisions to accelerate material rebalancing strategies at hundreds of sites across the globe.

Cost-effective supplier selection and business allocation are well-known and are crucial aspects of procurement planning for multi-sourced commodities. With myriad factors influencing buyer decision-making, optimizing volume to source from each supplier for each part is a highly challenging task. To address those challenges, we are building a Total Addressable Market (TAM) optimizer engine to determine the optimal share of business to suppliers. The objective is to achieve cost competency and reduce the risks for continuity of supply.

We have also built a one-stop self-serve performance management and insights platform for our logistics and trade operations to track on-time performance, carbon measure, cycle times, direct-ships and consolidation opportunities, late order root causing and more. The platform helps track different key performance indicators (KPIs) across trade compliance use cases such as restricted third-party screening, product classification, license management and more.

Looking at the future towards an autonomous supply chain, we are investing in building a ‘Frictionless’ supply chain. This supply chain will utilize the existing layer of digital experiences to create an end state where machines and humans have seamless interlocks to do what they do best to their fullest extent. The Frictionless supply chain will not just be an incremental advancement over existing tools and processes but will focus on a fundamental change in roles, responsibilities, and operating models.

It will enable us to:

- **Connect our ecosystem**: get more value from our data across new and existing solutions with a platform that connects your entire supply chain.
- **Better navigate disruption**: predict supply chain disruptions before they happen and proactively address risks through intelligent orchestration.

- **Be agile**: build seamless supply chain flows with the agility to rapidly adjust to changing markets and meet evolving customer demands.

Dell is committed to advancing our supply chain security with digital transformation of our processes and orchestration of decisions with AI/ ML in our future frictionless supply chain. We want to create a secured supply chain with multiple levels of cybersecurity, physical management, and endpoint security so that we continue to be a highly trusted, intelligent, and responsive supply chain ecosystem.

The 24/7 Approach: Continuous Improvement

The Dell supply chain security process is continuously evolving with the threat landscape. The Supply Chain Risk Management framework guides Dell’s actions towards navigating risks and meeting security objectives. The framework sets out how Dell continuously improves by responding to a range of factors, including changing threats, new legislative requirements, and new customer requirements and concerns.

Industry Collaboration

Internally, Dell hosts cross-functional security governance forums that constantly review existing threats and scan the horizon for potential threats. Externally, Dell follows the belief that we are “stronger together” by sending Dell supply chain assurance experts to work with trusted industry groups and public-private partnerships in the development of industry standards and regulatory requirements, often taking a leadership role. Because security touches so many different vendors, Dell participates in industry-wide groups to collaborate with other leading vendors in defining, evolving, and sharing best practices on product security that further enhance the secure development of all IT products.

Examples of Dell industry collaboration include:

- Dell co-founded and currently chairs the Board of Directors of The Software Assurance Forum for Excellence in Code (SAFECode: https://www.safecode.org). Other board members include representatives from Microsoft, Adobe, SAP, Intel, Siemens and Symantec. SAFECode members share and publish software assurance practices and training.
- Dell is an active member of the Forum of Incident Response and Security Teams (FIRST: https://www.first.org). FIRST is a recognized global leader in incident and vulnerability response.
- Dell was among the nine companies that were first assessed by the Building Security In Maturity Model (BSIMM: https://www.bsimm.com/) project in 2008 and has continued to be part of the project. A Dell representative is part of the BSIMM Board of Advisors.
- Dell employees were founding members of the IEEE Center for Secure Design, which was launched under the IEEE cyber security initiative to help software architects understand and address prevalent security design flaws.

- Dell is a member of MITRE’s System of Trust Community initiative, which was created to offer a comprehensive and consistent methodology that can be tailored to meet industry and company needs to address supply chain security issues, leading to better traceability, reliability, and security of supply chains.

- Dell is a member of the Open Group and holds the Open Trusted Technology Provider Standard (O-TTPS) certification, which provides a set of guidelines, recommendations and requirements that help assure against maliciously tainted and counterfeit products throughout commercial off-the-shelf information and communication technology product lifecycles.

- Dell is on the governing board of the Open Source Security Foundation and is a member of the Trusted Computing Group.

Dell participates in industry wide engagements with governmental agencies around the world. One recent engagement with the potential to help address these threats throughout the ICT (Information and Communications Technology) sector is the U.S. Department of Homeland Security’s ICT Supply Chain Risk Management (SCRM) Task Force. The Task Force consists of 20 federal partners as well as 20 companies across the IT and Communications sectors. Additionally, Dell contributed to NIST’s National Cybersecurity Center of Excellence (NCCoE) in creating a guide through the project *Validating the Integrity of Computing Devices*.

While industry groups and public-private partnerships are tremendously helpful in raising the bar for the industry, Dell’s most important initiatives are identified through direct collaboration with our customers. From our earliest days, it has been a hallmark of Dell to listen to, learn from, and deliver for our customers. Dell has a vast sales force, who actively engage and interact with customers worldwide. Dell hosts Executive Briefing Programs that provide customers the opportunity to engage directly with Dell’s top leaders, designers, technologists, and engineers to explore ideas, strategize, and share insights.

This foundational document outlines Dell’s holistic approach to protecting its supply chain because it wants to provide solutions that customers can trust. Dell will continue to prioritize security at every stage of the supply chain because it wants to ensure the delivery of trustworthy products into the hands of its valued customers.

Resources

1. Cyber Resilient Security in Dell PowerEdge Servers, 2023
2. Dell Security and Trust Center
3. Dell ISO Certifications
4. Dell Trusted Device
5. Dell Technologies Trusted Device Whitepaper, 2020
6. Dell SafeID
7. Dell Technologies: Secured Component Verification
8. Dell Signed Firmware Update (NIST SP800-147)
9. NIST Platform Firmware Resiliency SP800-193
10. Environmental, Social and Governance Report 2023
11. Dell Supplier Principles