A Partnership of Trust: Dell Supply Chain Security

DELL Technologies

Table of Contents

Why Supply Chain Security Matters

Information technology is creating a more connected world, and our dependence on technology for all aspects of our lives continues to increase. However, the advanced technology and sophisticated logistics networks that support this connectivity are facing unprecedented attacks, which risk undermining the trust on which growth, prosperity and international relations rest. Complicating matters further, the complexity, sophistication and potential impact of attacks also have increased substantially over time.

A single ransomware incident can lead to operational disruptions, lost revenue, compromised data, diminished productivity and a tarnished brand or corporate reputation. For these reasons, customers are rightly seeking assurance that the technology products they purchase have not been tampered with or maliciously modified, jeopardizing customers' ability to protect the data stored and processed on those devices.

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

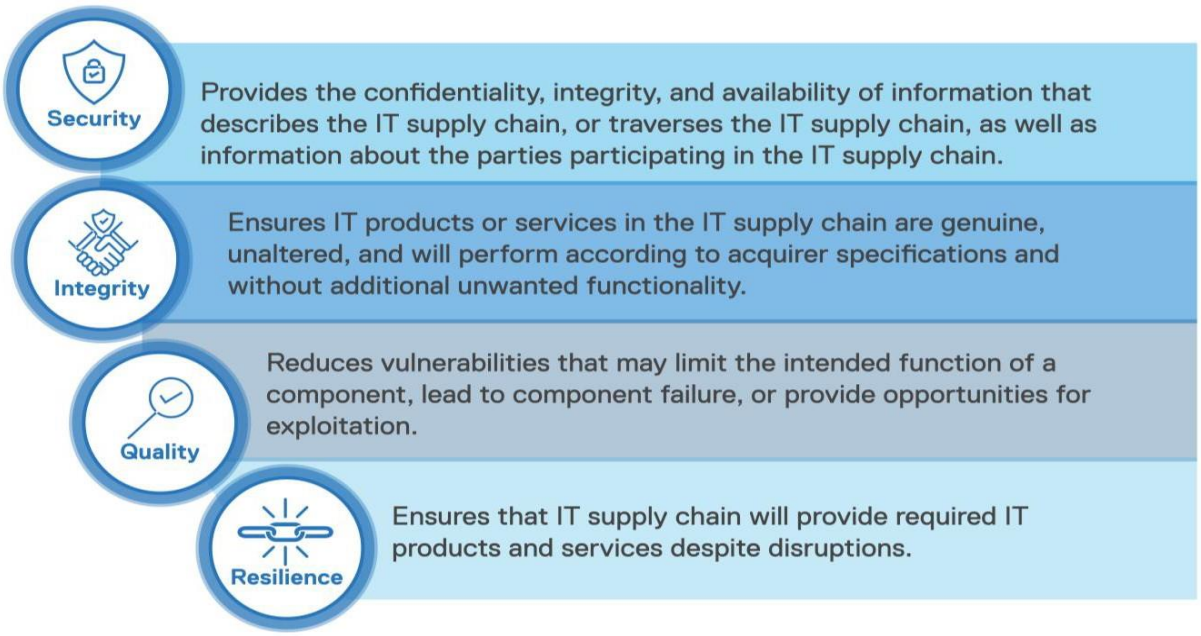
The security of IT hardware and the supply chain that supports its production and delivery has never been more at the forefront of our customers' minds. In *Four Keys to Navigating the Hardware Security Journey* by Futurum, the author noted that 44% of organizations said they have had at least one Hardware-Level or Basic Input Output System (BIOS) attack during the prior 12 months, making securing IT hardware a priority.

These reasons drive our focus at Dell Technologies on creating and maintaining world-class supply chain security measures. A safe and trusted environment reduces systemic risk while increasing the security of the supply chain ecosystem. Dell constructed its business model with that environment in mind through the creation of a partnership of trust among its people, customers and suppliers. The two-way collaboration Dell has with key stakeholders in a diverse supply base – both upstream and downstream – enables us to deliver the best value and technology to customers while leveraging our agility, integrity and ingenuity.

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*.

There are several capabilities that are valued at Dell when determining what controls should be implemented throughout each phase of the supply chain. These capabilities are security, integrity, quality and resilience.



Security in the Dell Supply Chain

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

Dell employs a multifaceted approach to protect its supply chain, delivering solutions that customers can trust. Whether it is a desktop, laptop, server or a data storage array, product features are conceived, designed, prototyped, implemented, set into production, deployed, maintained and validated with supply chain security as a top priority.

Securing Data

Securing data in the supply chain involves those practices, policies and principles utilized to 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 innovative 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 are built around 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 extraordinary 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. Numerous measures are used to guard sensitive information against exposure and exploitation. For example, data transfers between Dell and its partners use a combination of encryption methods and private communication channels. Secure protocols and encapsulation technologies are also used in accordance with industry best practices, where appropriate. Production lines have also been designed and built to manage the ability to transfer information.

Dell's internal network environment and associated assets are secured through controls such as virus detection, strong password enforcement, email attachment scanning, system and application patch compliance, intrusion prevention and firewalls. Additional controls have been implemented to protect against malware and misuse of assets.

Dell also employs the National Institute of Standards and Technology (NIST) 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 ensure that access to sensitive information is only granted to individuals to the degree needed to perform their assigned duties.

Personnel Security

Screening employees and restricting employee rights to access, use and manipulate company data, assets and resources provide needed assurance that internal security efforts will be effective. 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, which is designed to mitigate the risk of behavior that may put products at risk throughout the supply chain. Employees are also encouraged to remain informed of the latest security developments throughout the year by reading corporate newsletters, internal and external security websites, customer whitepapers, attending seminars, participating in corporate security awareness campaigns and taking additional online courses and video training. Additionally, they, along with contractors, must sign and agree to confidentiality provisions that protect intellectual property, customer information and other sensitive data not only during their tenure as employees but also after they leave.

Physical Security

Facilities where Dell products are designed, built, customized or fulfilled must demonstrate compliance with several internationally recognized physical security standards such as those defined by 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 audits suppliers and facilities on various topics, including the use 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 internationally recognized by member states of the World Customs Organization and demonstrate "best in class" supply chain security standards within the private sector. These programs 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 ensures that customers' products are safely delivered and once received, operates as intended. An important feature of supply chain integrity is the development of a baseline specifications of hardware and software that is preserved securely and later used as a reference to verify that no unauthorized modifications have been made.

Hardware Integrity

Dell has a variety of quality control processes to help minimize the risk of counterfeit components infiltrating our supply chain. The new Dell product introduction process verifies that materials are sourced only from Dell's approved vendor list and match the bill of materials. Parts are procured 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, all key components are uniquely identified 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. Adherence to these processes and controls helps minimize the risk of counterfeit components being embedded within Dell products.

Software Integrity

Software engineering best practices integrate security throughout the development process for any code, including operating systems, applications, firmware and device drivers. Third-party components integrated into software developed by Dell are obtained from trusted suppliers, and the integrity of these components are verified prior to integration. Dell reduces opportunities for the exploitation of software 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] and ISO 27034[2].

Proactive verification, validation and security testing activities throughout the lifecycle help to ensure secure software and reduce the likelihood of malware or coding vulnerabilities being inserted into software. A robust cybersecurity program improves 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 a limited number of 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

As hardware products are designed and the software code is developed to enable the hardware to perform its functions as designed, Dell utilizes the practice of intrinsic security. This practice includes processes and policies that ensure security features are implemented at the time of product hardware and software inception and continue throughout the development cycle. In essence, it is security that is 'built' in. In order to effectively execute this practice, engineers are required to take mandatory security training before handling the code in any way. Security champions are assigned to each development team to drive a security culture within the organization.

Secure Development Lifecycle

Dell's Secure Development Lifecycle (SDL) program is based on 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 the ISO 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 identified key risk areas. Analysis activities, such as threat modelling, static code analysis, vulnerability scanning and security testing, are integrated to more effectively uncover and remediate thousands of potential security weaknesses and vulnerabilities throughout the development lifecycle. SDL helps mitigate many common design weaknesses in the software and in web applications, including 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 all software and firmware. When engineers begin designing new features and functionality, they are required to follow a set of strict procedures defined by the SDL, which prevents vulnerabilities, in both proprietary code and third party components. During product design, the engineering team creates threat assessments and a model to determine what the threat surface is and where testing should be focused after the code is developed. Once they have created and refined the code, they must follow a rigorous three-part testing process. Typically for the engineers developing software or firmware, this starts with a static code analysis—an automated process which uses special tools for finding and fixing weaknesses and vulnerabilities. The second phase of the testing process features a comprehensive approach, where a team of engineers conduct a line-by-line reading of the source code. It is rigorous work that usually points to previously unknown mistakes in the code rather than malicious activities. However, it provides further assurance that the source code has been designed in a safe way.

[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, risk assessments are conducted using special tools to scan for known security vulnerabilities, and, when finalized, 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 is sometimes directed to undertake penetration testing—depending on the outcome of the threat assessment and model. This red team may find potential vulnerabilities that were missed in the earlier phases. These findings are mitigated again based on risk, so that any additional identified exposure has been 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.

The process follows these steps:

- Dell's Core BIOS is architected and developed predominately 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.
- Select platform-specific features are developed and technology partner firmware is integrated into Dell's
  Core BIOS by the Dell firmware development team in Taiwan.
- 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 "pentesting", has become synonymous with mature security practices across the industry. Dell leverages in-house teams and external vendors to pentest its PCs, servers and storage devices while these products are still in the engineering phases of development. These tests focus on physical access and are prioritized based on risk assessments of individual components integrated into the device.

BIOS Protections

BIOS is firmware which facilitates the hardware initialization process and transition control to the operating system. In effect, it controls the device, so if an attacker managed to corrupt the BIOS,

they would be able to gain control of the device because of the BIOS's unique and privileged position within the device architecture.

Dell has implemented procedures across our commercial servers and PCs in accordance with the NIST SP 800-147, BIOS Protection Guidelines. They 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 encryption 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, BIOS safeguards have been created that comply with SP 800-193 NIST Platform Firmware Resiliency 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

With Dell PowerEdge products, if the chassis has been opened, an entry is 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—and this makes it possible to track the source of the 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 PowerEdge servers have enjoyed robust security for many years. The 14th Generation PowerEdge servers are "cyber-resilient," meaning they have a hardened server design for protecting against, detecting and recovering from cyber-attacks. The latest servers also have reliable recovery features that ensure any firmware-based cyber-attacks can be overcome with little or no interruption to the business. For example, the iDRAC allows customers to backup and restore a PowerEdge server's configuration and firmware with minimal effort, should the motherboards fail or become corrupted and need to be replaced.

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 the PowerEdge security resiliency features directly.

- Next generation PowerStore, PowerScale and PowerMax build on top of the current features to include HwROT at the disk array and fabric levels, setting Dell apart from its competitors. In addition, the BMC HwROT has been upgraded to support National Security Agency (NSA) Top secret grade algorithms in order to support their longer service life. 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, stored data is protected by passwords, firewalls, basic encryption and anti-virus software, but the PowerMax and PowerStore have data-at-rest encryption that is validated to the Federal Information Processing Standard (FIPS) 140-2. It encrypts 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 technologies for its commercial PCs, resulting in the industry's most secure commercial PCs. Some of these features are more applicable to PCs in use than in production, but some features can be used during the production process to provide a higher level of assurance and prevent potential malware intrusion.

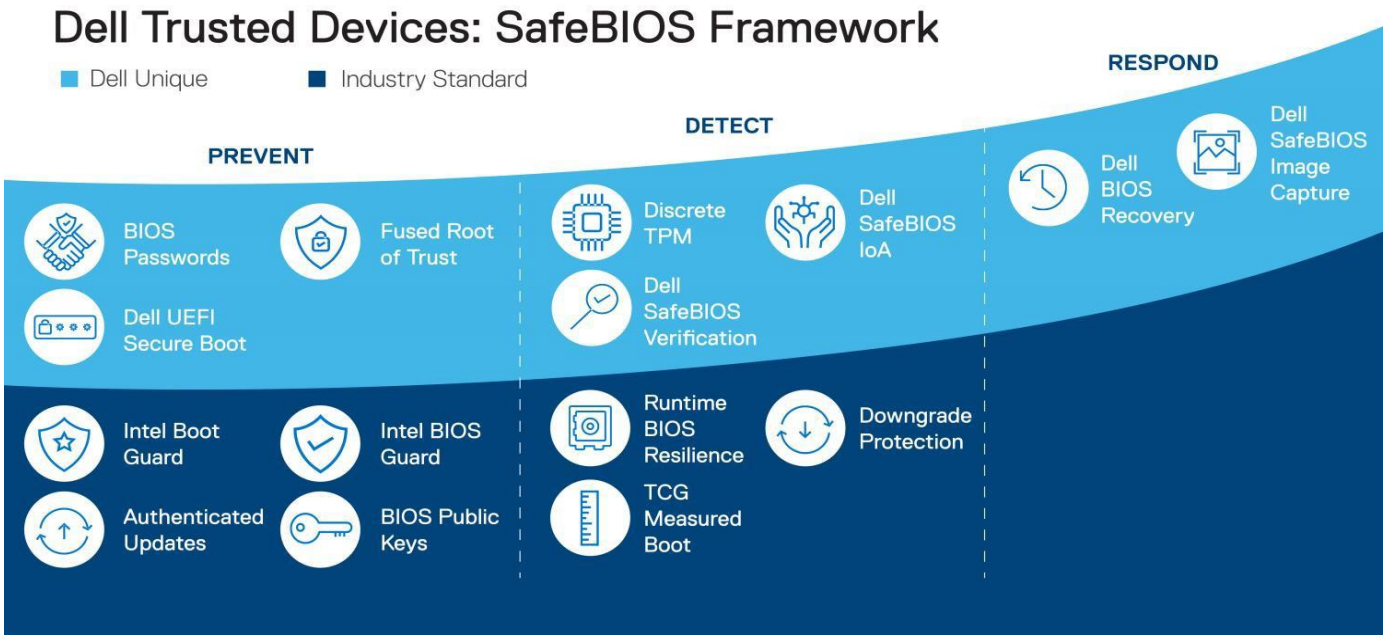
These built-in security features include:

- 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, which is 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 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

Once a product design has been completed, it is ready to be transformed into a finished product. Dell directly manages approximately half of the global manufacturing sites it utilizes, while also working with 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 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 the 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, each is sent a very detailed set of product specifications, where they must provide a clause-by-clause response, showing how they could meet the specifications. Those suppliers then undergo an in-depth Quality Process Audit (QPA), which includes a stringent security assessment. The QPA is conducted on site and evaluates the end-to-end activities at the location. The security requirements often go beyond industry standards in order to meet Dell standards. Second, a "bench" level test of the devices that can be supplied is conducted —for instance, the motherboards or hard drives are evaluated. 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. Suppliers are comprehensively reviewed 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. Facility Security Requirements (FSR) are embedded in Procurement contracts. Typically, supplier factories are assessed and audited against Dell'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.

Our collaborative approach with partners in our supply chain spans many 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, security management systems and 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 Resiliency Organization.

Through our continuous improvement model spanning numerous supply chain focus areas, we partner

with suppliers and provide robust capability building programs 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 sites that produce approximately 53 million Dell PCs 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 TAPA facility security requirements as well as comply with Dell Supplier Security Standards.

These standards cover:

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

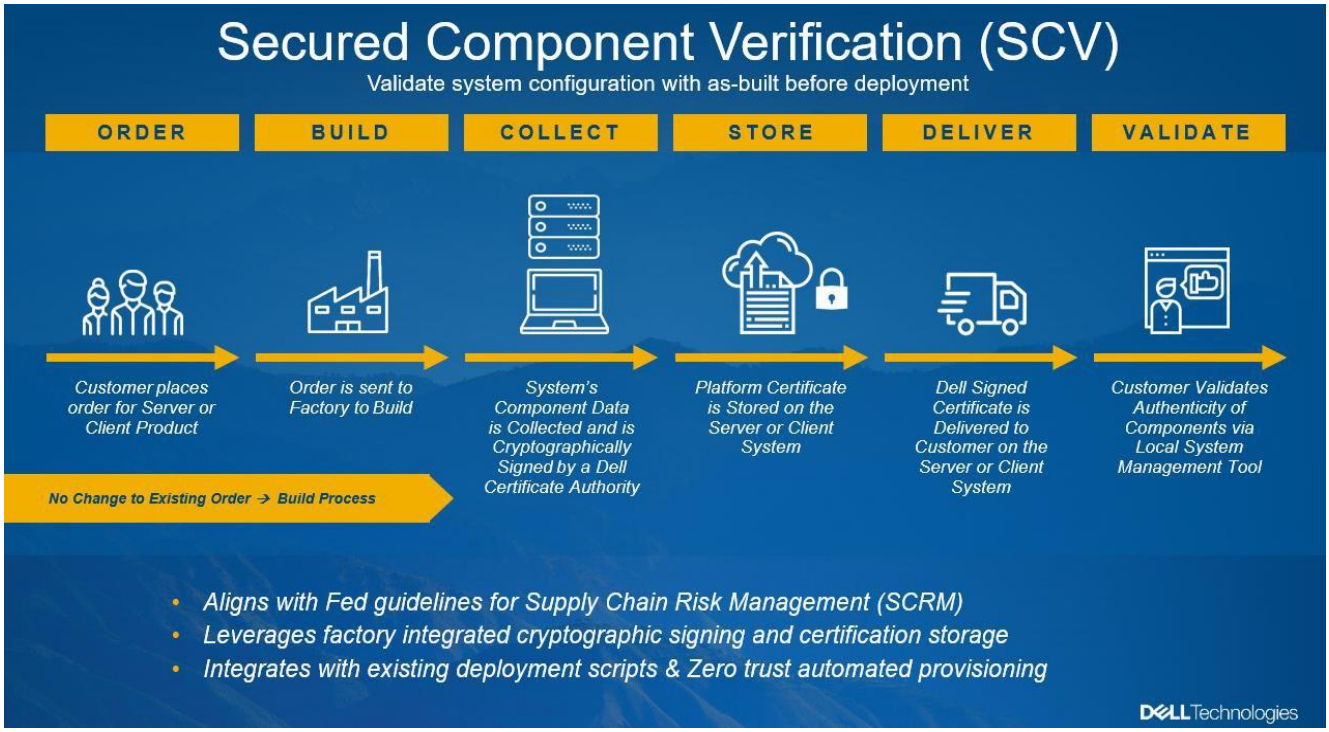
In addition to the security practices in the manufacturing facilities, we ensure that all the parts, components and raw materials that arrive at the site are genuine, authentic and new. The parts for Dell products are procured directly from the OCMs or an authorized reseller of the OCM on the approved vendor list. Once the necessary components have been acquired, they are handled through 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. After motherboards are assembled, there are robust processes to verify the motherboards are manufactured as designed.

Verification and Tracking

One of those controls in place for servers and client products is a requirement to affix a unique PPID label to specific high-risk components so that Dell can identify, authenticate and track. 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 the unique system tracking identification number 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.



For certain 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 and 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 finished, it is either shipped directly from the factory to the customer, or it is routed to one of the many fulfilment hubs operating around the world. To get the product to the customer, Dell works with numerous 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

A feature of Dell's logistics security program is a series of risk management command-and-control centers located around the world that are staffed 24/7 with experts who can draw on the latest information about transport hotspots and track shipments using various monitoring technologies to ensure products reach their destination without disruption. The command centers collate real-time data and other information about planned routes to be taken by road vehicles. Specialists monitor various sensors on truck and cargo assets with an eye towards the changing threat levels in different regions, providing information that can be used to make decisions about the required level of security. With this intelligence, the 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, a variety of tracking devices are offered ranging from telematics data, imbedded GPS, Bluetooth tags and other covert trackers equipped with radio frequency technology for recovering stolen assets. These can alert the control centers if there are any unauthorized stops or route deviations. If requested and approved, the experts 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, the products stowed in the trucks can be put into boxes that are sealed with security tape that leaves telltale signs if they have been cut or removed.

Additionally, the boxes themselves can then be placed onto pallets where the standard metal crimps are removed and replaced by special reinforced strapping. Once the pallets are loaded onto the truck, the doors can be safely locked with a serial numbered bolt seal that is verified by the customer upon arrival.

After Delivery

Once our customers receive Dell products, the security program does 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 for 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, security updates are released to customers as new threats are encountered. Dell Security Advisories and Notices are posted 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—are cryptographically signed by Dell. 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 our agility are key to the resilience of our supply chain. In addition to our focus on continuous improvement in security, we have established business continuity, crisis management and disaster recovery programs across our operations. Through our strategic programs, Dell takes proactive steps to identify and mitigate risk, including performing business impact analysis and testing. This strategy of resilience 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, and 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

At Dell, our global supply chain footprint is large and complex, and we continue to evolve to better serve the business and our customers. In 2018, we began our digital transformation journey to improve our customer experience and 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 resiliency and robustness. It provides an automated statistical baseline forecast with a suite of anomaly detection tools that identify and manage disruptive demand. The resulting combined forecast drives an inventory optimization engine that balances the highest possible customer service levels with the lowest required working capital structure. The combination 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.

This will be followed up by scaling the digital twin to incorporate various aspects of the supply chain, as well as challenges such as constrained supply, natural disasters, business expansion, geopolitical tensions and cyber-attacks. This will help executives evaluate strategies and footprint investments, compare expected results, assess business and financial risks and understand potential shortcomings under different market and economic conditions.

We are 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 the material rebalancing strategies at hundreds of sites across the globe.

Cost-effective supplier selection and business allocation are well-known and crucial aspects of procurement planning for multi-sourced commodities. With myriad factors influencing the buyer's decision-making, optimizing the 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 the 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 journey towards an autonomous state of the 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 and responsibilities and the operating model.

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. Dell is guided by the Supply Chain Risk Management framework that outlines how risks are mitigated and how security objectives must be met. 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 numerous 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 participates in industry wide engagements with governmental agencies around the world. One of the recent engagements 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 the industry groups and public-private partnerships are tremendously helpful in raising the bar for the industry, Dell's most important initiatives are typically 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.

Security is 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. Our aim, as it has been since Michael Dell founded the company in 1984, is to deliver trustworthy products straight out of the box and into the hands of our valued customers.

Resources

1. Cyber Resilient Security in Dell PowerEdge Servers, 2020
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 2022