



# A Partnership of Trust: Dell Supply Chain Security

© 2021 Dell Inc.

© 2021 Dell Inc. or its subsidiaries. All Rights Reserved. Dell, EMC and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

**DELL**Technologies

# Table of Contents

- Why Supply Chain Security Matters .....3**
- The Dell Supply Chain .....3
- Security in the Dell Supply Chain .....4**
- Data Security .....4
- Information Security*.....5
- Personnel Security*.....5
- Physical Security* .....5
- Integrity in the Dell Supply Chain .....6**
- Hardware Integrity*.....6
- Software Integrity* .....6
- Design and Develop .....7**
- Dell Secure Development Lifecycle* .....7
- Dell Firmware Digital Signing* .....8
- Penetration Testing*.....9
- BIOS Protections* .....9
- Chassis Intrusion* .....9
- Additional Built-In Security Measures: Dell Servers, Storage, and Client* .....10
- Additional Built-In Security Measures: Dell PCs*.....10
- Source .....12**
- Supplier Relationship Management* .....12
- Make .....13**
- Verification and Tracking* .....13
- Resilience in the Dell Supply Chain .....15**
- Deliver .....15**
- Above and Beyond: How Dell Protects Products During Delivery* .....15
- After Delivery .....16**
- The 24/7 Approach: Continuous Improvement.....16**
- Resources .....18**

## 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 their ability to protect the data they intend to store and process on those devices.

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](#), they noted that 44% of organizations said they have had at least one Hardware-Level or 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.

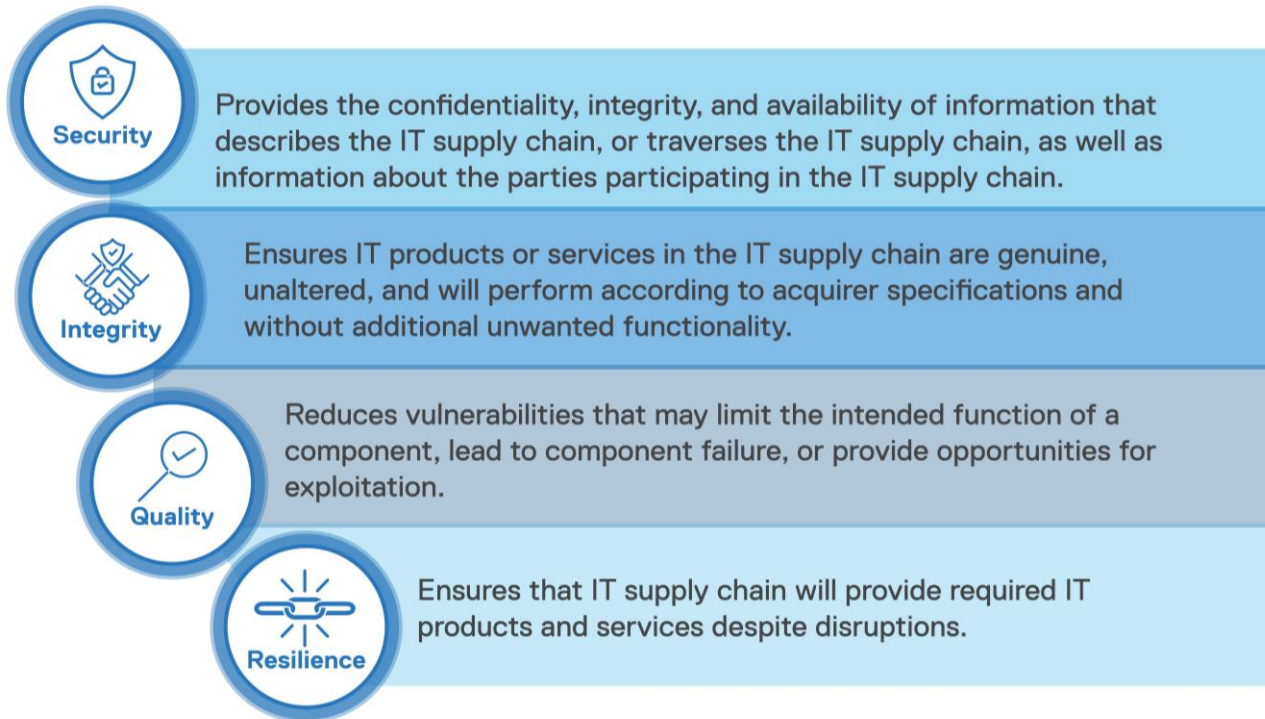
*Dell constructed its business model with a partnership of trust among its people, customers, and suppliers.*

## The Dell Supply Chain

Dell takes a holistic approach to protecting its supply chain and delivering solutions that customers can trust. Dell's 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

Dell Technologies takes a holistic and multifaceted approach to protect its supply chain and delivering solutions that customers can trust. Whether it's 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.

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.

### Data Security

Data security 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.

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's 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 way 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 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 and customer whitepapers, attending seminars, participating in corporate security awareness campaigns, and taking additional online courses and video training. Additionally, they, along with employees and 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 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 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 helps ensure that the product received by the customer is the product the customer expected, and it operates as intended. An important feature of supply chain integrity is the development of a baseline specification 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. Dell's new 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 [Secure 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<sup>1</sup> and [ISO 27034](https://www.iso.org/standard/44378.html)<sup>2</sup>.

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.

## 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 prioritizes 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 in order to drive a security culture within the organization.

### *Dell Secure Development Lifecycle*

Dell’s Secure Development Lifecycle (SDL) defines security controls that Dell product teams adopt while developing new features and functionality. Dell collaborates through many industry standard venues such as SAFECode<sup>3</sup>, Building Security In Maturity Model (BSIMM), and IEEE Center for Secure Design to ensure that industry practices are followed.

Dell’s SDL includes both analysis activities and prescriptive proactive controls around key risk areas. The analysis activities, such as threat modelling, static code analysis, scanning and security testing, are integrated to discover and address thousands of potential security weaknesses and vulnerabilities throughout the development lifecycle. It helps mitigate many common design weaknesses in the software and in web applications, including unauthenticated code updates, exposed/enabled debug interfaces, insecure default settings and hard-coded passwords. Our 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)<sup>4</sup> and CWE (Common Weaknesses Enumeration)<sup>5</sup> published by MITRE, the OWASP (Open Web Application Security Project) Top 10<sup>6</sup>, and the SANS Top 25 Most Dangerous Software Errors<sup>7</sup>.

---

<sup>1</sup> <https://safecode.org/>

<sup>2</sup> <https://www.iso.org/standard/44378.html>

<sup>3</sup> <https://safecode.org/>

<sup>4</sup> <https://cve.mitre.org/>

<sup>5</sup> <https://cwe.mitre.org/>

<sup>6</sup> <https://owasp.org/www-project-top-ten/>

<sup>7</sup> <https://www.sans.org/top25-software-errors>

The Dell SDL 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, including 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 conducts 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.



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 was accurate. Software in the combined integration and delivery pipeline leverage 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](#).

### *Dell 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 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 Core BIOS by Dell's 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*

The 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 National Institute of Standards and Technology (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 won't 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 SCCM and Dell Command Suite.

## *Additional Built-In Security Measures: Dell Servers, Storage, and Client*

Dell EMC PowerEdge servers have enjoyed robust security for many years. Dell EMC 14<sup>th</sup> Generation PowerEdge are “cyber-resilient,” meaning they have a hardened server design for protecting against, detecting and recovering from cyberattacks. The latest servers also have reliable recovery features that ensure any firmware-based cyberattacks 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 client and storage platforms employ similar strong security measures required to protect our customers and our customer data.

- Our Dell EMC 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 TPM, digitally signed firmware updates, UEFI secure boot, Intel bootguard and HwROT product capabilities. Additionally, PowerScale and PowerProtect products built on PowerEdge hardware benefit from the Dell EMC PowerEdge security resiliency features directly.
- Next generation Dell EMC 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 NSA Top secret grade algorithms in order to support their longer service life. Similarly, with the enablement of secure Unified Extensible Firmware Interface (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 being fitted with additional lines of defense in the shape of Trusted Platform Module (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 innovative and world-class technologies to 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.

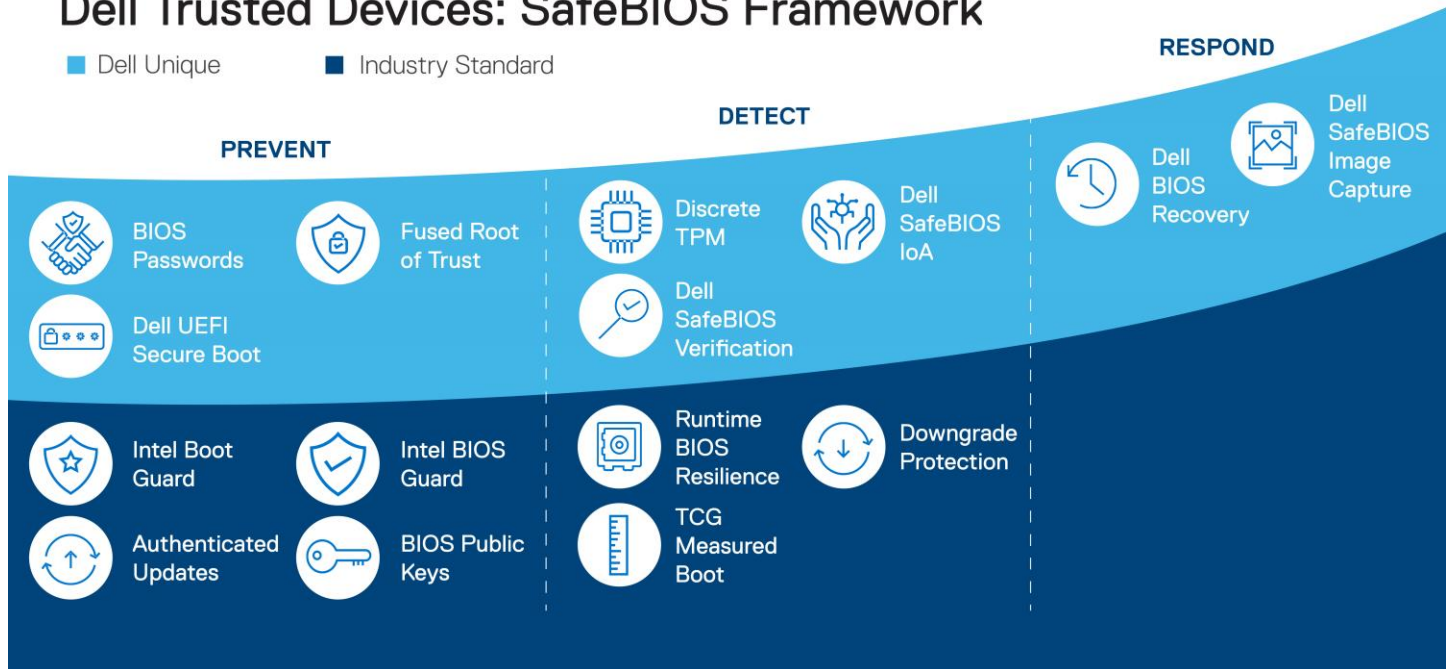
These built-in security features include:

- Off-Host SafeBIOS Verification – A secure verification of the BIOS image against a Dell-hosted off-host source.
- Dell SafeID with ControlVault – Provides hardened storage of end user credentials - the highest-value target for attackers - in a single chip.
- 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 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 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 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 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*

Dell's 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 standard in order to meet Dell's 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. Third, the supplier's component or device is placed into the finished desktop, server or other product in order to see how it performs.

As a routine part of our Supplier Relationship Management (SRM) strategy and approach, strategic suppliers must undergo periodic performance reviews. They are judged using a preset and comprehensive list of criteria, including cost, delivery, innovation, security, and adherence to Dell's strict principles, which are a condition of doing business. Typically, supplier factories are assessed against Dell's expectations, and they are audited. Dell will assist with corrective actions when necessary and support the supplier in building new capabilities.

Our collaborative approach with partners in our supply chain spans many direct and sub-tier supplier facilities. In 2020, Dell assessed 313 factories across 12 countries and audited 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 Original Design Manufacturing (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. Through our continuous improvement model spanning

*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.*



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 customer teaches us the most, which is why Dell is constantly challenging its suppliers to refine their 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, Original Design Manufacturers (ODM) or contract manufacturers, all are required to meet the Transported Asset Protection Association's (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.

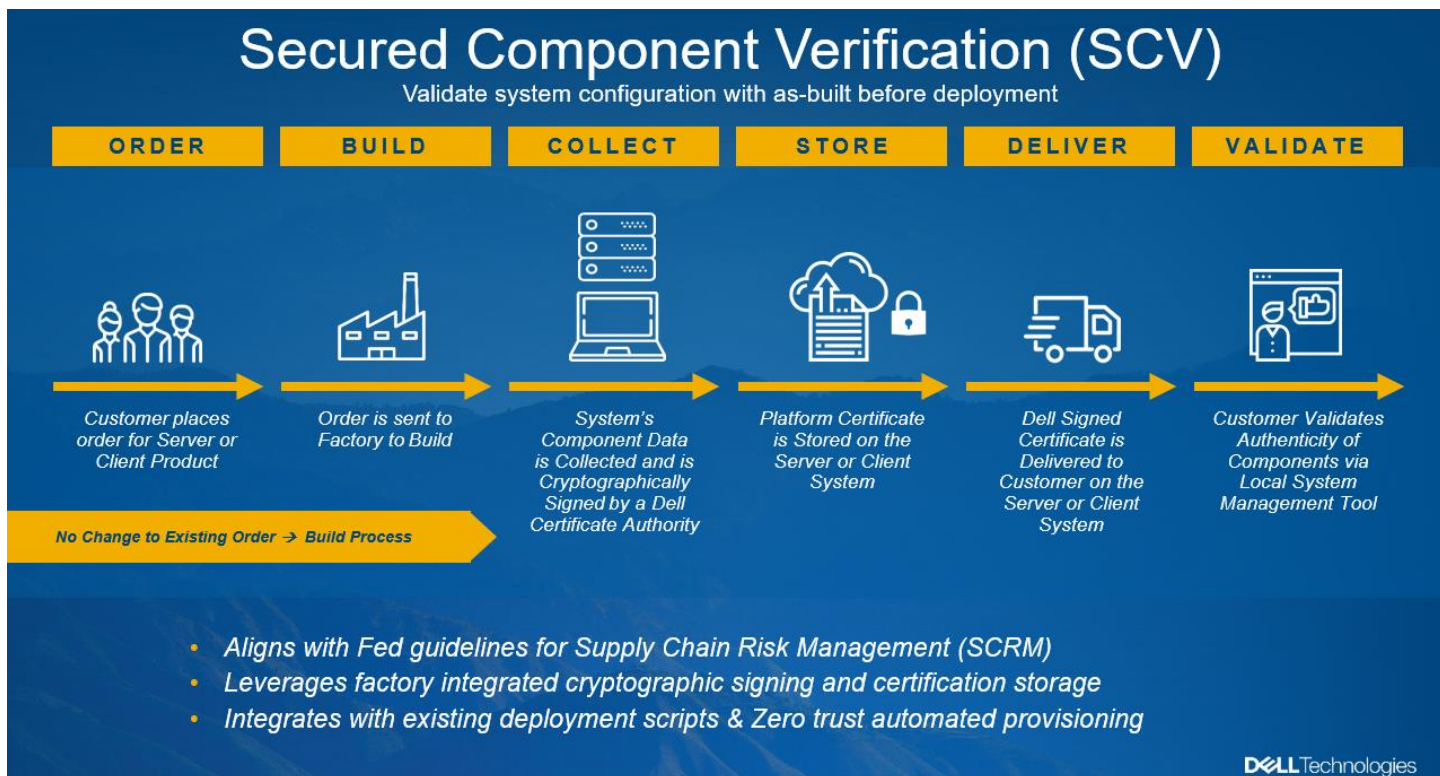
In addition to the security practices in the manufacturing facilities, we ensure that all the parts, components, and raw materials that arrive to the site are genuine, authentic, and new. The parts for Dell products are procured directly from the OCMs (Original Component Manufacturers) or an authorized 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 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 **Piece Part Identification Number (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 this year 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 will be 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 (EIDs) 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.

## Resilience in the Dell Supply Chain

Dell's global footprint, flexibility, and supplier relationships 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.

## Deliver

The 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 fulfillment hubs operating around the world. To get the product to the customer, Dell works with numerous trusted logistics providers by air, land, and sea that help fulfill more than 179,000 orders daily by carrying millions of products—enough to fill 34,000 sea 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.

### *Above and Beyond: How Dell Protects Products During Delivery*

A feature of Dell 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.

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 into pallets where the standard metal crimps are removed and replaced by special reinforced strapping. Once the pallets are loaded on to 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 their Dell product, 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 to [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's 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.

## The 24/7 Approach: Continuous Improvement

Dell's 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.

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 EMC 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, CA 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 (DHS) ICT SCRM (Supply Chain Risk Management) 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 now 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 EMC 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.com/Security](#)
8. [Dell Technologies: Secured Component Verification](#)
9. [Dell Signed Firmware Update \(NIST SP800-147\)](#)
10. [NIST Platform Firmware Resiliency SP800-193](#)
11. [Supply Chain Sustainability Progress Report 2020](#)