

# Dell Supply Chain Resilience



# Table of contents

<b>How Does Dell Ensure a Secure and Resilient Supply Chain?</b>	<b>3</b>
<b>Security and Resilience in the Dell Supply Chain</b>	<b>4</b>
Enterprise Resiliency: From Business Continuity Planning to Crisis Management	5
<b>Securing Data and Information in the Supply Chain</b>	<b>5</b>
<b>Plan: Design and Develop</b>	<b>6</b>
Software Integrity	6
Secure Development Lifecycle (SDL)	7
<b>Source</b>	<b>8</b>
Geodiversity and Multisourcing	8
Supplier Relationship Management	8
Personnel Security	9
Physical Security	10
Third-Party Risk Management	10
<b>Make</b>	<b>11</b>
Verification and Tracking: Secured Component Verification	11
Verification and Tracking: Absolute Custom Factory Installation	12
Hardware Integrity: Counterfeit Parts Prevention	13
<b>Delivery</b>	<b>13</b>
Above and Beyond: How Dell Protects Products During Delivery	14
<b>After Delivery</b>	<b>15</b>
Dell Services Supply Chain	15
<b>Supply Chain Digital Transformation</b>	<b>16</b>
Future-Focused: Leveraging Machine Learning (ML) and Artificial Intelligence (AI)	16
<b>The 24x7 Approach: Continuous Improvement</b>	<b>18</b>
Industry Collaboration	18
<b>Resources</b>	<b>20</b>
<b>Appendix</b>	<b>21</b>
Firmware Digital Signing	21
Penetration Testing	21
BIOS Protections	22
Chassis Intrusion	22
Additional Built-In Security Measures: Dell Servers and Storage	22
Additional Built-In Security Measures: Dell PCs	23

# How Does Dell Ensure a Secure and Resilient Supply Chain?

Dell Technologies has a long-standing commitment to security, which has been a core part of its operations for over 40 years. This dedication to security is integrated into every stage of their supply chain, from the initial planning and design of products to sourcing components, manufacturing and delivery. Dell Technologies ensures that security is prioritized at each step to provide customers with reliable and secure products right out of the box.

In 2020, the COVID-19 pandemic posed significant challenges to global supply chains, including Dell's. Despite these unprecedented difficulties, Dell continued to meet customer needs, demonstrating the robustness and adaptability of their supply chain. A crucial element of this resilience is their multisourcing strategy, which ensures that disruptions in any single region or supplier do not hinder their ability to fulfill demand. Additionally, Dell Technologies actively monitors global geopolitical developments, enabling them to proactively develop contingency plans to mitigate potential disruptions.

Dell Technologies offers unique capabilities like Secured Component Verification (SCV) to reinforce their commitment to security. SCV allows customers to check the manifest of their product components upon receipt and compare it with the original manifest. This ensures that the product was built and shipped as ordered, providing assurance that it has not been tampered with during the process.

Security is integrated into every aspect of Dell Technologies' ecosystem. They work closely with leading industry partners and vendors to establish, refine and share best practices in product security. This collaborative effort strengthens the security of all IT products and reinforces the integrity of their supply chain.

Dell Technologies understands the importance of providing a safe and secure digital environment. This foundational document details their comprehensive approach to supply chain security and resilience, which remains a top priority. By maintaining the highest standards of security and resilience, Dell delivers innovative technologies and reliable solutions to customers, fostering enduring partnerships built on collaboration and trust.

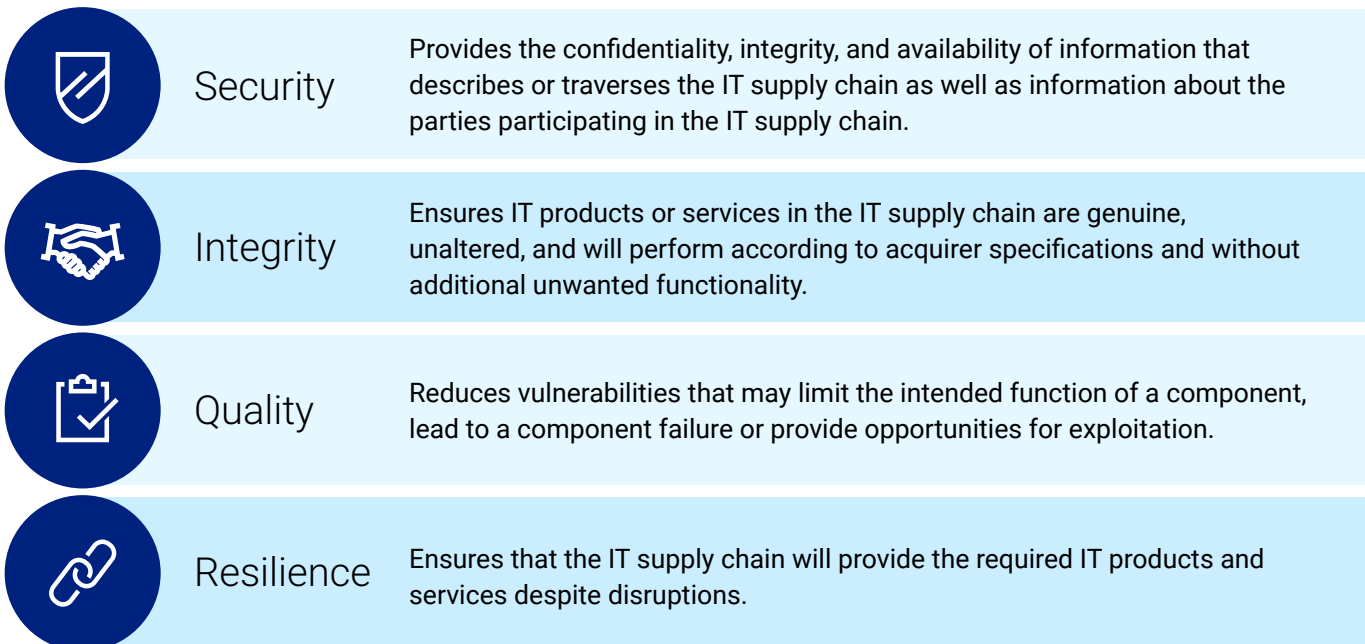


Dell constructed its business model with a partnership of trust among its people, customers, and suppliers.

# Security and Resilience in the Dell Supply Chain

Dell Technologies employs a comprehensive approach to securing its supply chain and providing trustworthy solutions to customers. Their cybersecurity strategies, “defense-in-depth” and “defense-in-breadth,” incorporate multiple layers of controls to mitigate potential threats within the supply chain. These layered controls combined with effective risk management, ensure robust supply chain security.

Dell Technologies prioritizes security, integrity, quality and resilience when determining controls at every stage of the supply chain. These values guide their decisions and ensure that each phase of the supply chain is robust and secure.



Supply chain security involves implementing and monitoring control measures to protect physical assets, inventory, information, intellectual property and personnel. By addressing information, personnel, and physical security, it helps secure the supply chain and reduces risk of maliciously introduced malware and counterfeit components.

The Dell Technologies global footprint, supplier relationships and agility are key aspects of its resilient supply chain. The company continues to enhance its security and establish best-in-class business continuity, crisis management and disaster recovery programs across its operations. Through these strategic initiatives, Dell Technologies proactively identifies and mitigates risk, including conducting business impact analysis and testing. This resilience strategy enables Dell Technologies to develop a coordinated approach to assessing risk and making critical decisions in response to complex supply chain threats. Dell Technologies values security, integrity, quality and resilience when implementing controls throughout each phase of the supply chain.

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

# Enterprise Resiliency: From Business Continuity Planning to Crisis Management

The Dell Technologies Business Continuity Program helps maintain the continuity of supply and operations for critical functions and supplier locations.

By fostering trusted relationships and upholding high standards of responsibility and integrity across our supply chain network, Dell enhances its flexibility in sourcing and manufacturing, earning the trust of its stakeholders. This approach equips Dell Technologies with a unified and robust response to incidents that significantly impact its ability to operate normally. The programs are designed based on risk and are aligned with recognized international industry standards, including [ISO 22301](#).

## Securing Data and Information in the Supply Chain

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

Dell Technologies employs overlapping practices to secure digital data, including robust administrative and physical controls and multilayered access protocols to protect sensitive customer data. The company's data governance efforts focus on optimizing relationships and security postures to proactively identify vulnerabilities and mitigate risk. To protect the confidentiality, integrity, and availability of customer data, Dell Technologies extends trust and assurance throughout its end-to-end value chain. Multiple steps are taken to protect digital data and other customer-sensitive information while minimizing the impact on end-user functionality.

In the normal course of business, Dell Technologies collects and uses information about products, solutions, suppliers and partners throughout the supply chain lifecycle. Robust security measures

guard sensitive information against exposure and exploitation. For example, Dell Technologies and its partners use a combination of encryption methods and private communication channels to transfer data, including secure protocols and encapsulation technologies that align with industry best practices.

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

Additionally, Dell Technologies employs the principles of "separation of duties" and "least privilege" to guide key controls throughout the supply chain, preventing the misuse of data access across the business. These principles ensure that access to sensitive information is granted only to individuals that have a need to perform their assigned duties.

# Plan: Design and Develop

Dell Technologies employs a mature and proven Secure Development Lifecycle (SDL) program to ensure security in the designs of its hardware products and developments of its software/firmware code. The SDL program includes processes and policies that guarantee secure code implementation from the inception of product hardware and software, continuing throughout the development cycle. Essentially, security is integrated from the start. To effectively execute this program, Dell requires its engineers to complete mandatory security training before handling any code. Additionally, Dell Technologies requires its engineers to be security champions to each product development team to drive a security culture within the organization.

## Software Integrity

Dell Technologies adheres to software engineering best practices by integrating security throughout the development process for all code, including operating systems, applications, firmware and device drivers. Third-party components integrated into Dell Technologies software are sourced from trusted suppliers and their integrity is verified prior to integration. Dell Technologies reduces the opportunities for the exploitation of product security flaws by incorporating SDL measures throughout the Design and Development process. By incorporating Secure Development Lifecycle (SDL) measures throughout the design and development process, Dell Technologies reduces the opportunities for the exploitation of product security flaws. These measures are closely aligned with Software Assurance Forum for Excellence in Code ([SAFECode](#)) guidelines, [ISO/IEC 27034](#) and the National Institute of Standards and Technology (NIST) Secure Software Development Framework (SSDF).

Dell's proactive verification, validation, and security testing activities throughout the software component lifecycle help ensure integrity and reduce the likelihood of malware or malicious code introduction. A robust cybersecurity program enhances software integrity by preventing unauthorized access to source code and minimizing the potential for malware introduction before products are shipped to customers.

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

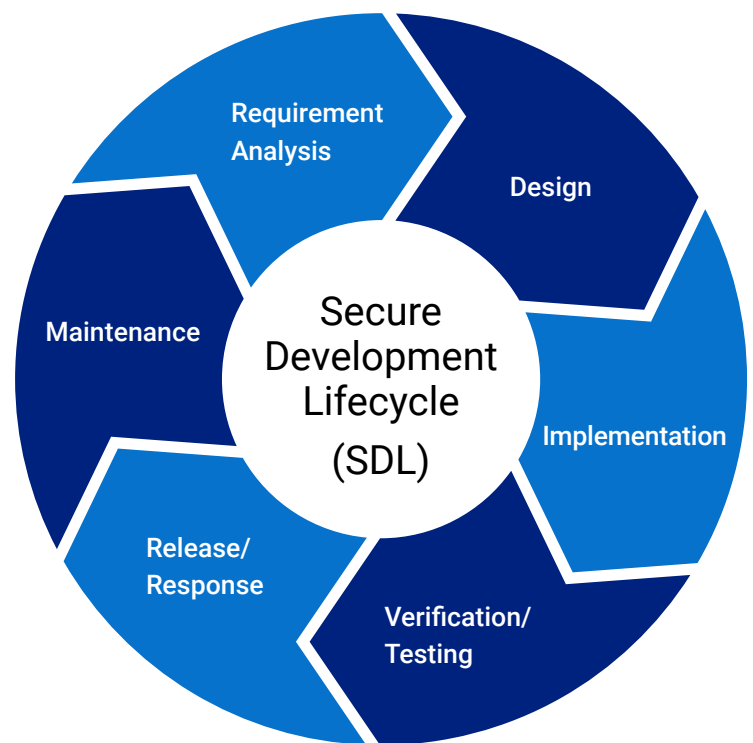


# Secure Development Lifecycle (SDL)

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

The SDL program includes analysis activities and prescriptive/proactive controls around all risk areas. Dell Technologies integrates analytic activities, threat modeling, static code analysis, vulnerability scanning, and security testing to holistically identify and remediate security weaknesses and vulnerabilities throughout the development lifecycle. SDL helps mitigate many common design weaknesses in software and firmware, including unauthenticated code updates, exposed or enabled debug interfaces, insecure default settings and hard-coded passwords. The SDL program leverages tools 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 Common Vulnerabilities and Exposures (CVE) and Common Weakness Enumeration (CWE) published by MITRE, the Open Worldwide Application Security Project (OWASP) Top 10 and the [SANS Top 25 Most Dangerous Software Errors](#).

The SDL program governs the design and testing of software and firmware. Engineering teams must adhere to a set of strict protocols defined by the SDL when designing new product features and functionalities. This process helps to prevent vulnerabilities in both proprietary code and third-party components. During product design, engineering teams create threat assessments and models to determine the threat surface and focus of testing following code development. Engineers developing software or firmware start with static code analysis – an automated process which uses special tools to find and fix weaknesses and vulnerabilities. They then test the process features by analyzing the source code line by line. This is a rigorous process that usually points to previously unknown mistakes in the code rather than malicious activity. However, these protocols provide additional assurances that the source code is safe and secure.



Toward the end of the design stage, engineering teams provide risk assessments by using special tools to scan for known security vulnerabilities and verify that the threat model is accurate. Software in the combined integration and delivery pipeline leverages the SDL automation in the building, testing and deployment of applications, ensuring that security is integrated at each phase of the lifecycle.

Finally, based on the outcome of the threat assessment and model, a team of expert hackers may be directed to conduct penetration testing. This team can identify potential vulnerabilities that were missed in earlier phases. These findings are mitigated based on risk, and any additional identified exposure is documented and corrected.

Additional information on the Dell Technologies SDL program can be found on the [Dell Security and Trust Center](#).

# Source

Following product design completion, it is transformed into a finished product. Dell Technologies directly manages about half of the global manufacturing sites it utilizes, while collaborating with partner companies that provide additional manufacturing facilities, raw materials and individual components. The Dell Technologies supplier selection process includes a rigorous onboarding course with several key procedures to ensure each supplier meets the company's high standards for integrity, security, quality and reliability. These suppliers are crucial for successfully delivering high-quality products and mitigating the increasing number of security threats.

Dell Technologies remains thorough in its selection process, aiming to choose not just a supplier, but a partner.

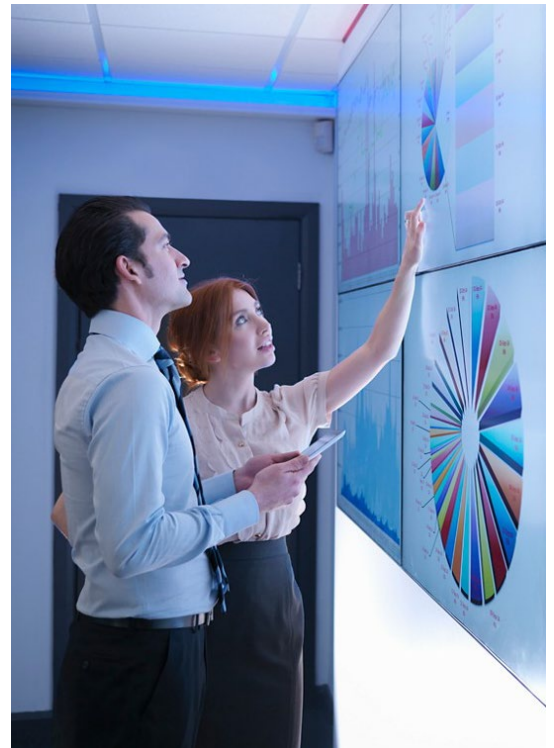
## Geodiversity and Multisourcing

Dell Technologies actively qualifies and tracks multiple sources of supply for our products to maintain resilience and continuity of supply. When parts are not multisourced, we establish comprehensive business continuity plans and supply chain strategies, reviewing them regularly to ensure continuity is maintained. Our multisourcing approach includes tracking the following:

- Supplier dual sources
- Product multisourcing by part
- Percent (%) multisourced or single sourced
- Pre- and post-general availability analysis

## Supplier Relationship Management

The Dell Technologies supplier selection process begins with the commodity managers preparing a target list of suppliers that align with the broader category strategy including country, region, cost, financial health, quality needs and more. Next, potential suppliers receive a detailed set of product specifications for which they must provide line-by-line responses showing how they can meet the specifications. Those suppliers then undergo an in-depth Quality Process Audit (QPA), which includes a stringent security assessment. On-site QPAs evaluate the end-to-end activities at the location with security requirements exceeding industry standards to meet Dell Technologies criteria. Additionally, there is a "bench" level test of the devices, such as motherboards or hard drives. This typically 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 then placed into the finished desktop, server or other product to assess its performance.



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

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

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

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

The Dell Technologies continuous improvement model for supply chains creates a partnership with suppliers

that produces robust program capability building to enable suppliers to build their own in-house capabilities.

The toughest customers are our best teachers, which is why Dell Technologies 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 Technologies to build stronger ties with our suppliers, providing customers with greater levels of assurance.

## Personnel Security

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

Dell Technologies employees maintain a culture of security and must undergo annual security awareness and compliance training designed to mitigate the risks that could affect products throughout the supply chain. This training conforms to government standards and industry protocols for supply chain security. Additionally, employees receive security developments throughout the year via corporate newsletters, internal and external security websites, customer white papers, seminars,

corporate security awareness campaigns, and online courses and video training sessions. Employees and contractors must also sign and agree to confidentiality provisions that protect intellectual property, customer information and other sensitive data during and after their employment.

## Physical Security

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

The Dell Technologies physical and cybersecurity audits of suppliers and facilities include inspecting digital closed-circuit TV cameras, access control systems, intrusion detection and guard service protocols. Additional controls are applied to protect Dell Technologies cargo during shipping and logistics, 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 and escalate any security noncompliance events observed during transit.

Dell Technologies also maintains certifications in multiple secure trade and commerce programs to include Tier 3 status with the U.S. Customs Trade Partnership Against Terrorism (CTPAT), Canada's

Partners in Protection (PIP), Singapore's Secure Trade Partnership (STP) and Authorized Economic Operator (AEO) status in several other nations. These programs are recognized by international member states of the World Customs Organization (WCO) and demonstrate best-in-class supply chain security standards within the private sector. Additionally, these programs focus on supplier accountability, security management policies, counter-smuggling, trafficking controls and tamper prevention to secure trade across international borders.

## Third-Party Risk Management

Dell's Third-Party Risk Management (TPRM) Program is designed to proactively manage third-party risks by identifying, prioritizing, assessing, and remediating risks throughout the supplier lifecycle. This comprehensive program covers security and privacy risks for suppliers within Dell's Direct supply chain, including hardware/firmware, ODMs, direct software, and logistics suppliers. TPRM is crucial for keeping pace with the evolving security and privacy regulatory landscape. The framework outlines stringent requirements across the supplier lifecycle, both before and after onboarding. This includes thorough supplier risk vetting and profiling, contracting, continuous monitoring, and addressing any control gaps identified during the lifecycle.

The program aims to seamlessly integrate these requirements into existing business processes to ensure user adoption and leverage automation for scalability. By embedding TPRM within our operations, Dell ensures robust risk management and compliance, safeguarding our supply chain and enhancing overall security.



# Make



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

These standards cover the following requirements:

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

## Verification and Tracking: Secured Component Verification

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

Another control available is [Secured Component Verification \(SCV\)](#), a Dell Technologies capability intended to provide last-leg assurance of product integrity from the time an order is fulfilled at the Dell Technologies factory to the 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 were made to the components.

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

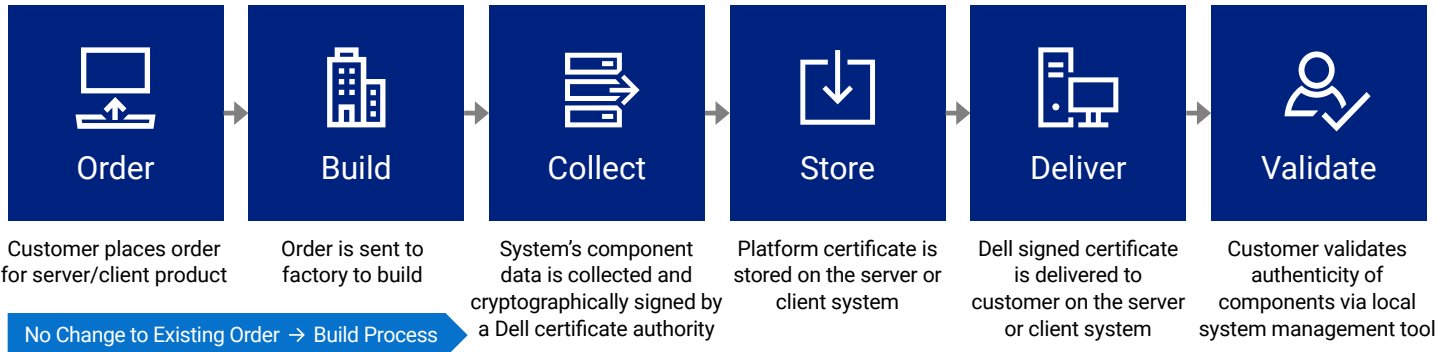
Unauthorized modifications of components in a product can introduce significant risks, potentially compromising both the security and functionality of the device. Customers could experience security breaches, data loss or system instability if unauthorized component replacements go undetected because these changes may create vulnerabilities that malicious actors could exploit. SCV helps customers identify any alterations to a customer's components and advises when to take appropriate action, if needed, to mitigate these risks.

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

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

## Secure Component Verification (SCV)

Validate system configuration with as-built before deployment



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

## Verification and Tracking: Absolute Custom Factory Installation

Dell Technologies collaborates with trusted partners to offer solutions that enhance security and supply chain assurance. A key example is Dell Custom Factory Installation (CFI). Customers can opt to have the Absolute Persistence Agent in the BIOS of commercial PCs. With that in place, customers can geolocate, geofence and remotely wipe data from their devices as well as self-heal critical applications – whether on or off the network. By installing these defensive countermeasures in the factory, customers can more effectively counter emerging cyberattacks and protect fleet integrity. CFI is a one-touch process handled directly from a Dell Technologies–owned and managed factory, removing a step in the procurement process in a safe and controlled environment.



## Hardware Integrity: Counterfeit Parts Prevention

Dell Technologies has implemented robust quality control processes to help minimize the risk of counterfeit components infiltrating its supply chain. The company's product introduction process verifies the sourcing of materials from the Dell Technologies–approved vendor list and matches the bill of materials (BOM). Dell Technologies procures parts directly from the ODM or OCM.

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

To enable appropriate traceability, Dell Technologies identifies all key components by a serial number label or marking, a PPID label or an electronic identifier that can be captured during the manufacturing process. PPIDs provide a foundation for the downstream component verification capabilities that Dell Technologies offers, such as SCV. Additionally, Dell Technologies maintains [ISO 9001](#) certification for quality control practices at all global manufacturing sites. Dell's adherence to these processes and controls minimizes the risk of counterfeit components from being embedded within Dell Technologies products.

## Delivery

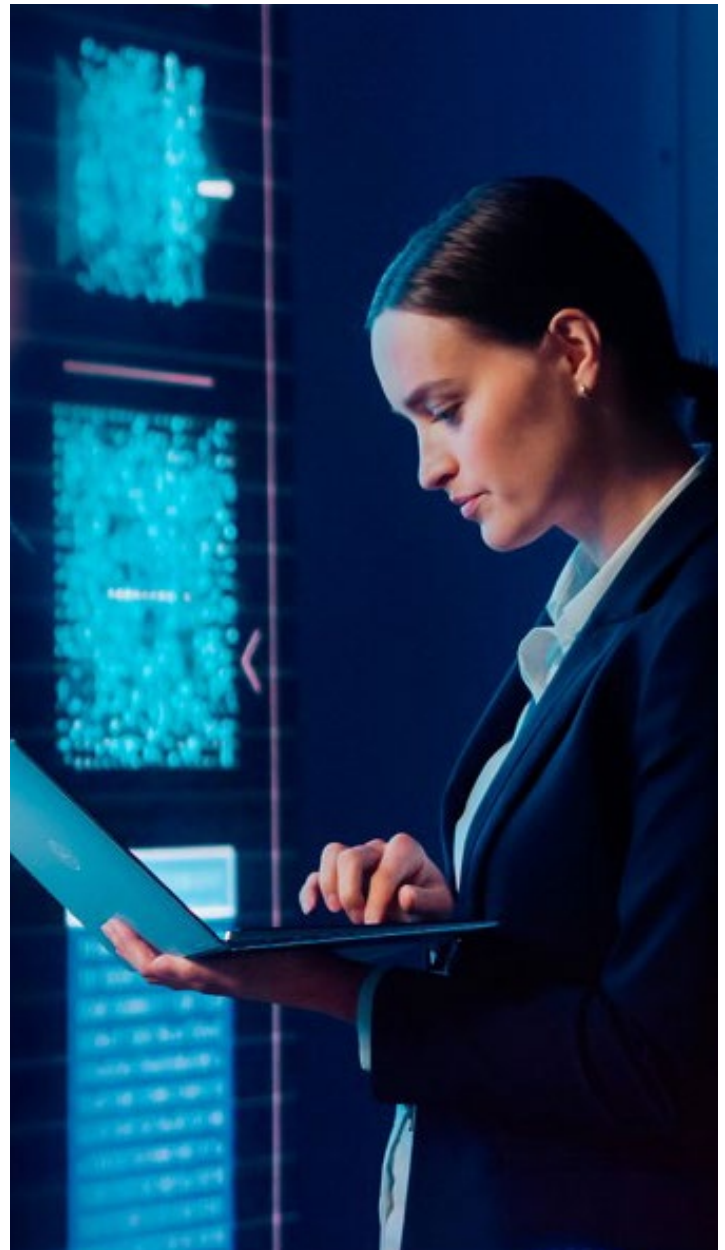
The final delivery of a product to the customer is the last stage of our supply chain process. Once a product is complete, it is either shipped directly from the factory to the customer or routed to a fulfillment hub. To get the product to the customer, Dell Technologies works with trusted logistics providers by air, land, rail and sea, fulfilling more than 179,000 orders daily and 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 the Dell Technologies specially developed Freight Security Requirements, including a cybersecurity framework, is also required.

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

One core feature of Dell Technologies logistics security program is a global set of risk management command and control centers. Located around the world, these centers are staffed 24x7 with subject matter experts who evaluate the latest information about transportation hotspots and track shipments using various monitoring technologies to ensure products reach their destinations without disruption. These nodes utilize intelligence to advise real-time data and other information about planned routes. Specialists monitor various sensors on truck and cargo assets with an eye toward the changing threat levels in different regions, providing information to make decisions about the required level of security. Command center specialists can advise on in-transit security risks for the suppliers responsible for moving Dell Technologies products.

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

In addition to security offerings, Dell Technologies offers more services that further ensure integrity and document custodial control through the product's journey to its destination. Initially developed for a unique Supply Chain Program, these services are now available to others. For example, products stowed in the trucks can be placed into sealed boxes with security tape to prevent and signal tampering. And boxes placed on pallets have metal crimps removed and replaced by special reinforced strapping. Following the loading of the pallets onto the truck, the doors are safely locked with a serial numbered bolt seal that is verified by the customer on arrival.



# After Delivery

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

Dell Technologies releases security updates to customers as new threats emerge. Dell Technologies posts security notices on the [Security Advisories, Notices and Resources](#) page. These updates might relate to our products or non-Dell products that customers use on Dell systems. Dell Technologies ensures that all updates to critical components – including BIOS, iDRAC, network adaptors and power supplies – have a cryptographic signature. When combined with the hardware Root of Trust (RoT) 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.

## Dell Services Supply Chain

Data-containing devices (DCDs) such as hard drives, solid state drives (SSDs) and motherboards, could be returned to Dell Technologies. Data integrity and the protection of the data within the services supply chain are critical components of delivering end-to-end supply chain assurance. Dell's services supply chain incorporates various data protection controls to include product controls at the BIOS level, or in the firmware, or software, whether the parts are new or refurbished in a Dell facility. For more information on the Dell Services Supply Chain, please review the [Services Supply Chain Security White Paper](#).



# Supply Chain Digital Transformation

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

In 2018, Dell began its digital transformation journey to improve its customer experience by building greater operational agility and optimizing our efficiencies. The company delivered these capabilities by focusing 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 tool set and orchestration layer to create seamless interactions between the twins and enterprise systems.

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

Diving deep into Dell Technologies' scalable applications, these tools ensure its supply chain team has end-to-end control across demand generation, supply matching, disruption management and setting inventory-level targets. Some of the solutions are described below.

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





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

Dell is scaling its digital twin capabilities for the build-to-stock supply chain for “what-if” scenario analysis to evaluate business outcomes and assess risks when deploying new strategies.

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

The company is also developing ML models that can optimize inventory to minimize shortages and lower overstock inventory. As an extension of that, Dell is also building a dynamic inventory-balancing application to facilitate and optimize rebalancing decisions to accelerate material rebalancing strategies at hundreds of sites across the globe.

Looking toward an autonomous supply chain, Dell is investing in building a frictionless supply chain. This supply chain will utilize the existing layer of digital

experiences to create an end state where machines and humans have seamless interlocks to do what they do best to their fullest extent. The frictionless supply chain will not just be an incremental advancement over existing tools and processes but will focus on a fundamental change in roles, responsibilities and operating models.

The frictionless supply chain 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 more agile:** Build seamless supply chain flows with the agility to rapidly adjust to changing markets and meet evolving customer demands.

Dell Technologies is committed to advancing its supply chain security with the digital transformation of our processes and orchestration of decisions with AI and ML in our future frictionless supply chain. Dell’s goal is to be a highly trusted, intelligent, and responsive supply chain ecosystem by creating a secure supply chain with multiple levels of cybersecurity, physical management, and endpoint security.

# The 24x7 Approach: Continuous Improvement

The Dell supply chain security process continues to evolve with the threat landscape. The Supply Chain Risk Management (SCRM) framework guides Dell Technologies toward navigating risks and meeting security objectives. The SCRM framework outlines how Dell Technologies 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 Technologies hosts cross-functional security governance forums that constantly review existing threats and scan the horizon for potential threats. Externally, Dell Technologies 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 Technologies 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 Technologies industry collaboration include:

- Dell Technologies co-founded and currently chairs the [SAFECode](#) Board of Directors. Other board members include representatives from Microsoft, Adobe, SAP, Intel, Siemens and Symantec. SAFECode members share and publish software assurance practices and training.
- Dell Technologies is an active member of the Forum of Incident Response and Security Teams. [FIRST](#) is a recognized global leader in incident and vulnerability response.
- Dell Technologies was one of the nine companies that were first assessed by the [BSIMM](#) Technologies representative as part of the BSIMM Board of Advisors.
- Dell Technologies employees were founding members of the [IEEE CSD](#), which was launched under the IEEE cybersecurity initiative to help software architects understand and address prevalent security design flaws.
- Dell Technologies is a member of [MITRE's System of Trust™ Community](#) initiative, which was created to offer a comprehensive and consistent methodology that can be tailored to meet industry and company needs to address supply chain security issues, leading to better traceability, reliability and security of supply chains.
- Dell Technologies is a member of the Open Group and holds the Open Trusted Technology Provider™ Standard ([O-TTPS](#)) certification, which provides a set of guidelines, recommendations, and requirements that help assure against maliciously tainted and counterfeit products throughout commercial off-the-shelf information and communication technology product lifecycles.
- Dell is on the Governing Board of the Open Source Security Foundation ([OpenSSF](#)) and is a member of the Trusted Computing Group ([TCG](#)).

Dell Technologies participates in industry-wide engagements with governmental agencies around the world. One recent engagement with the potential to help address these threats throughout the Information and Communications Technology (ICT) sector is the U.S. Department of Homeland Security's ICT SCRM Task Force.

The ICT SCRM Task Force consists of 20 federal partners as well as 20 companies across the IT and Communications sectors. Additionally, Dell Technologies contributed to NIST's National Cybersecurity Center of Excellence ([NCCoE](#)) in creating a guide through the project [Validating the Integrity of Computing Devices](#).

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

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



# Resources



1. [Client Solutions Dell Trusted Device: BIOS Security White Paper, 2024](#)
2. [Cyber Resilient Security in Dell PowerEdge Servers White Paper, 2023](#)
3. [Dell Client BIOS: Signed Firmware Update \(NIST SP800-147\)](#)
4. [Dell Environmental, Social and Governance Report, 2024](#)
5. [Dell ISO Certifications](#)
6. [Dell Modern Workplace](#)
7. [Dell SafeData: The Absolute Platform Datasheet, 2022](#)
8. [Dell SafeID Datasheet, 2024](#)
9. [Dell SafeID White Paper, 2024](#)
10. [Dell Secured Component Verification for Commercial PCs](#)
11. [Dell Secured Component Verification for Servers](#)
12. [Dell Security and Trust Center](#)
13. [Dell Supplier Principles, 2024](#)
14. [NIST SP800-193 Platform Firmware Resiliency Guidelines](#)
15. [Dell Services Supply Chain Security White Paper](#)

This white paper is for informational purposes only and may contain typographical errors and technical inaccuracies. The content is provided as is, without express or implied warranties of any kind.

Copyright © 2025 Dell Inc. or its subsidiaries. All Rights Reserved. Dell Technologies, Dell and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

# Appendix

## Firmware Digital Signing

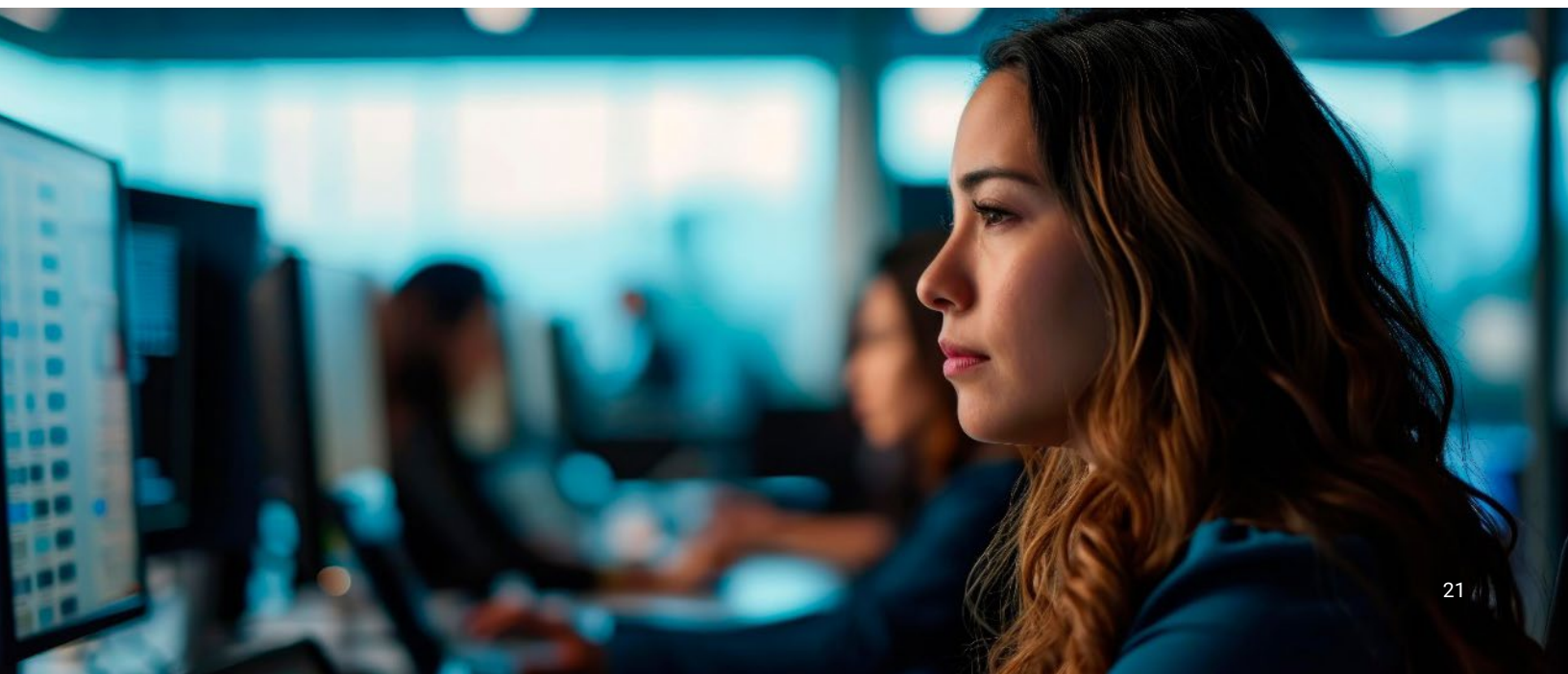
One potential threat to any supply chain is the risk of unauthorized code or data modifications. Dell Technologies engineers add a cryptographic digital signature to software, application, and firmware to enable confirmation of authenticity and integrity – a process known as code signing.

Digital signing follows these basic steps:

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

## Penetration Testing

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



## BIOS Protections

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

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

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

Additionally, Dell Technologies created BIOS safeguards that comply with the [NIST SP 800-193](#) Platform Firmware Resiliency Guidelines. These ensure that unauthorized BIOS and firmware code simply cannot run. If the code is somehow replaced with malware, the device will not function. This resilience is intended to last for the device's lifespan, from deployment to decommissioning.

## Chassis Intrusion

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

Similarly, many Dell Technologies commercial client devices include a chassis intrusion capability that can be

monitored via management tools, including Microsoft Endpoint Configuration Manager and Dell Client Command Suite.

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

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

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

- Platform silicon RoT anchors and other security controls including Unified Extensible Firmware Interface (UEFI) Secure Boot.
- Component attestation through Security Protocol and Data Model (SPDM).
- Firmware integrity through cryptographically signed updates.
- Protecting data integrity and confidentiality through strong flexible encryption controls.
  - Protecting data-at-rest against unauthorized access with self-encrypting drives and local and external key management.
  - Data-in-use encryption with confidential compute.
- Establishing a secure, encrypted connection using SSH and SSL/TLS 1.3 and updating with Automatic Certificate Renewal.
- Having a dedicated iDRAC network module.
- Enforcing least privilege access with strong identity using multifactor authentication (MFA), single sign-on, and role- and scope-based access control.
- Dynamic System Lockdown mode.

For more information, please refer to the [Cyber Resilient Security in Dell PowerEdge Servers White Paper, 2023](#).

Like its servers, the Dell Technologies 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, UEFI Secure Boot, Intel Boot Guard and hardware RoT product capabilities.
- Additionally, PowerScale and PowerProtect products built on PowerEdge hardware benefit from PowerEdge security resilience features directly.
- Next-generation PowerStore, PowerScale and PowerMax build on top of the existing features to include hardware RoT at the disk array and fabric levels, setting Dell Technologies apart from its competitors. In addition, we have upgraded the baseboard management controller (BMC) hardware RoT to support the National Security Agency (NSA) top secret grade algorithms and longer service requirements. Similarly, with the enablement of UEFI Secure Boot features and cryptographic signing, hardware RoT 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 Technologies data storage devices – PowerMax and PowerStore – are fitted with more lines of defense in the shape of TPM-by-default, data-at-rest and data-in-flight encryption and configuration locking. Typically, data is stored and protected by passwords, firewalls, basic encryption and antivirus software. But PowerMax and PowerStore have data-at-rest encryption that is validated to the Federal Information Processing Standard ([FIPS](#)) [140-2](#). Our solutions encrypt the data and deliver integration with external key managers, enabling customers to simplify security through a centralized key management platform.

## Additional Built-In Security Measures: Dell PCs

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

These built-in security features include:

### Secure Off-Host SafeBIOS Verification

A secure verification of the BIOS image against a Dell-hosted off-host source.

### Dell SafeID with ControlVault

Provides hardened storage of end-user credentials – the highest value target for attackers in a single chip.

### SafeBIOS Indicators of Attack

Detects advanced endpoint threats using behavior-based threat detection at the BIOS level.

### Secure Off-Host Firmware Verification

A secure verification of the critical firmware leveraging the Intel Management Engine associated with Intel vPro.

### 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.

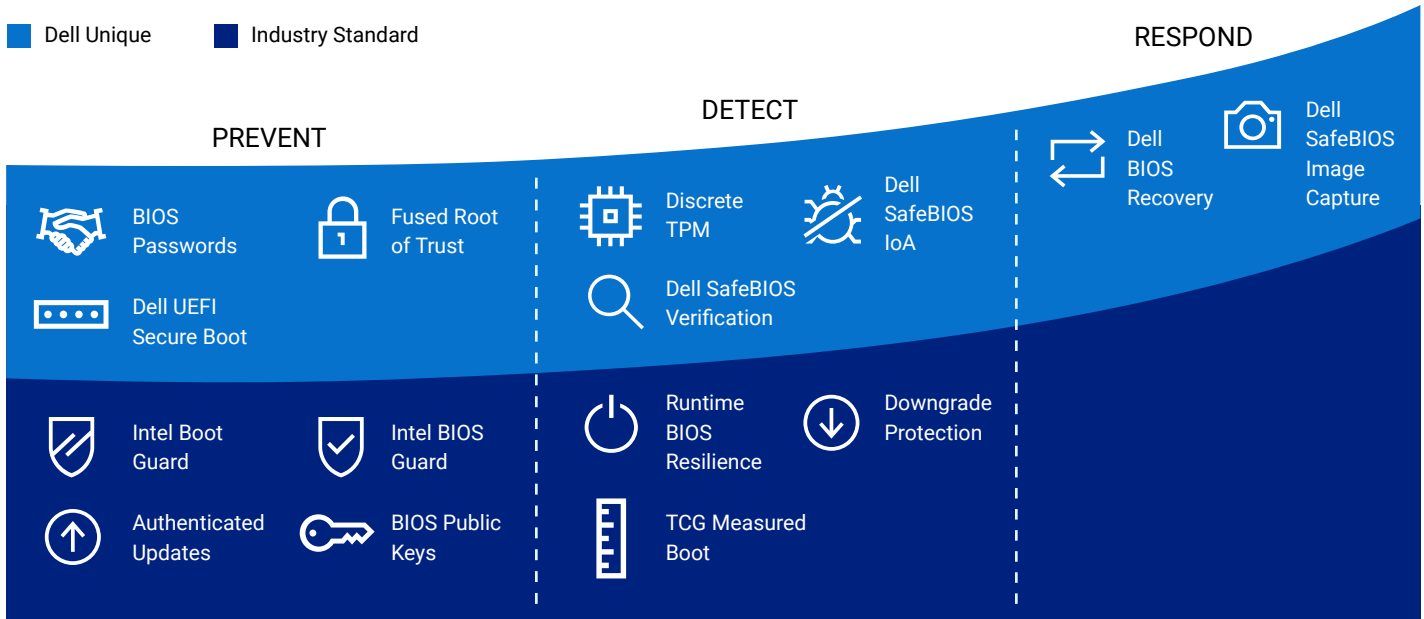
### Dell SCV

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.

Commercial Dell PCs incorporate a TPM, which coordinates with the BIOS during the UEFI Secure 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 TCG's Trusted 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 attestation.

# Dell Trusted Devices: SafeBIOS Framework



Dell SafeBIOS 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 Random Access Memory (NVRAM) 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 the 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.

