Technical Paper

Supply Chain Security

Supply Chain Security Goes Digital

Intel and Dell have spent years innovating to provide industry-leading solutions to help secure compute supply chains.

Authors

Patrick Bohart
Director of Initiatives, Intel

Rick Martinez
Sr. Distinguished Engineer, Sr. Director at Dell

Table of Contents

Growing Attention to Supply Chain Security

Recent high-profile attacks on critical infrastructure have pushed supply chain security into the news and helped foster new and emerging industry requirements and recommendations. The SolarWinds attack of 2020 within the U.S. Treasury Department, the White House's Executive Order on America's Supply Chain, and emerging standards and recommendations from organizations such as the National Institute of Science and Technology (NIST) highlight growing interest and investment in securing computer supply chains.

Alongside the increase in incidents and headlines, there are also significant recent advances in supply chain security for IT infrastructure and devices. Industry leaders are innovating around modern supply chain security practices and technologies to augment existing approaches. Recent innovations in high tech manufacturing enable the highest levels of device traceability and transparency ever available. Dell and Intel have been leaders in developing innovative supply chain security capabilities, for their own products as well as for the industry more broadly.

Expanding the Definitions of Supply Chain and Supply Chain Security

Innovating around supply chain security requires broadening previous definitions of the supply chain itself. Traditionally, and depending on customer context, the supply chain for IT infrastructure and compute devices has focused on sourcing parts and materials, device manufacturing, and "last mile" product delivery to customers. Today, it is important to extend our conception of the supply chain across the entire lifecycle of the device, as shown in Figure 1.

Figure 1. Defining the supply chain across the entire device lifecycle.

This perspective spans sourcing, manufacture, integration, transfer, deployment, operation, and retirement of the device. Many leaders in supply chain security employ this lifecycle model to enable a holistic approach, ensuring that systems are built in the most secure manner possible and remain in the most secure posture possible as they travel through the integration channel and into their operational lifespans.

It is also important to expand the traditional definition of supply chain to include the concept of digital supply chain security, as illustrated in Figure 2. Discussion of supply chain security has typically focused on physical supply chain security (e.g., facilities, personnel, and tamper-evident packaging). Digital supply chain security expands this scope to encompass recording and tracking key information about a device's entire lifespan, including details about how, when, and by whom it was manufactured and subsequently modified.

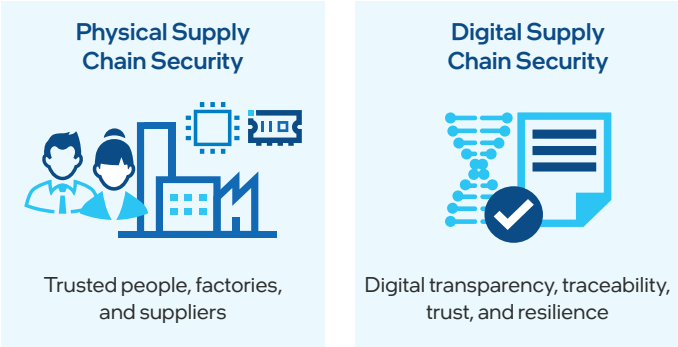


Figure 2. Expanding supply chain security to include both physical and digital elements.

Digital supply chain security is sometimes referred to as exposing and recording the digital DNA of the device, as represented in Figure 3, and then tracking that information in a secure, trusted, and reliable manner as it travels through the supply chain and into operation within an IT infrastructure.

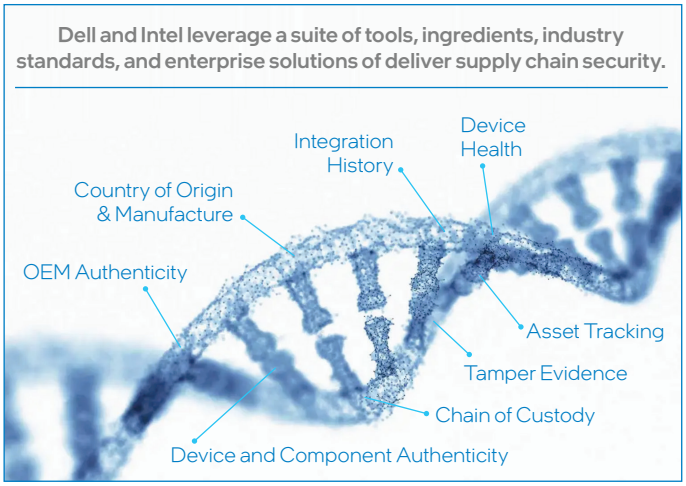


Figure 3. Digital DNA of a device.

Dell and Intel Roles Within Supply Chain Security

Dell and Intel have shared a common vision and direction to supply chain security for several years, drawing on their separate but interconnected roles in the supply chain. Dell Trusted Device and Dell SafeBIOS enhance the security of enterprise PCs. On PowerEdge servers, Intel® Boot Guard mitigates against CPU sleep attacks, as a complement to the PowerEdge platform hardware root of trust, and as part of its end-to-end secure boot. These enterprise-class security solutions employ foundational ingredients from Intel, such as Server Platform Services (SPS), secure fuses, and Authenticated Code Module (ACM).

Intel has a leadership position in the industry based on its role as an integrated design and manufacturing (IDM) leader. The presence of Intel software and manufacturing tools in silicon manufacturing facilities worldwide and the operation of Intel tools early and consistently prior to manufacturing and assembly provides advantages that improve Dell solutions.

Both Dell and Intel contribute extensively to the industry standards processes that influence future supply chain security initiatives and provide technology support for existing and emerging standards and capabilities. Dell and Intel participate and lead in the development of technologies and solutions based on industry standards and recommendations. This role includes influencing industry bodies such as the Trusted Computing Group (TCG) and cross-industry collaboration projects such as the NIST National Cybersecurity Center of Excellence (NCCoE). These solutions, ingredients, and standards are innovating businesses and increasing the value of their technology.

Physical Supply Chain Security

Dell, as a manufacturer and supplier of IT devices, and Intel, as a supplier of hardware components within Dell devices, both have a long history of protecting their physical supply chains, as illustrated in Figure 4. These supply chain security measures involve years of investment and innovation in areas such as screening and managing employee data access, building and maintaining secure facilities, and tightly managing and auditing vendors and suppliers to help prevent the presence of malicious or counterfeit ingredients in Dell and Intel products.

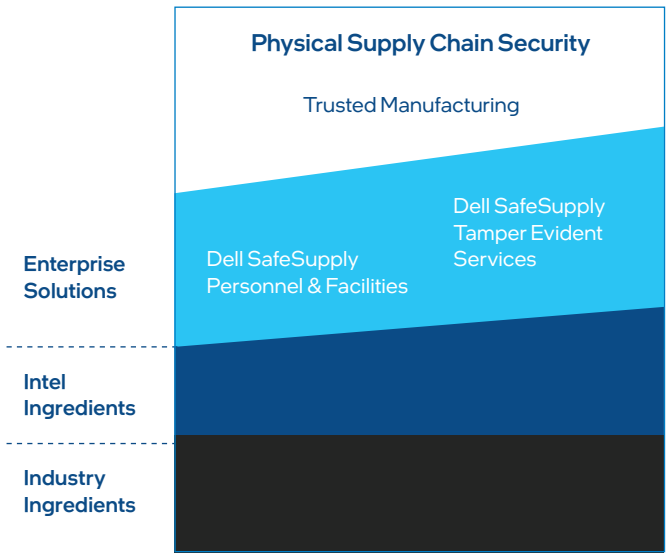


Figure 4. Dell and Intel physical supply chain security.

Digital Supply Chain Security

Digital supply chain security includes innovations that capture digital DNA snapshots of devices. Those innovations can be categorized into four areas of capability, as illustrated in Figure 5: traceability and transparency, device trust, resilience, and hygiene.

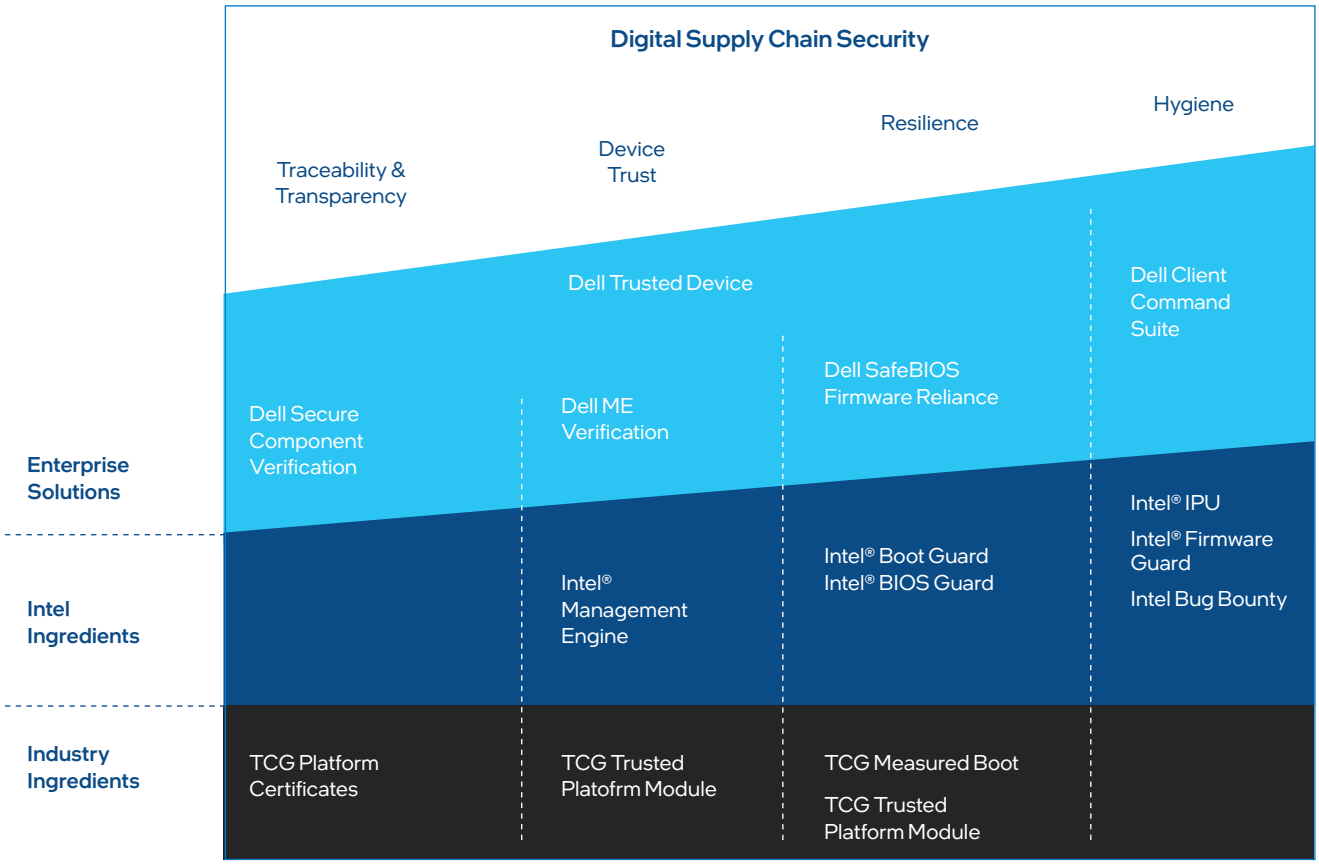
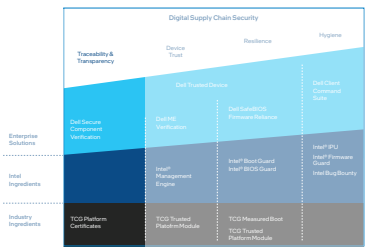


Figure 5. Dell and Intel digital supply chain security.

Traceability and Transparency



Dell and Intel have been leaders in driving compute device traceability and transparency for many years, through both investment in enterprise class solutions and leadership within the industry standards bodies and working groups that define and recommend available solutions. At the heart of these solutions from Dell and ingredients from Intel are platform certificates that provide cryptographically signed inventory documentation according to definitions driven through the TCG industry consortium. The TCG Platform Cert Spec v1.1 released in April, 2020 aligns with emerging standards for supply chain security, which are particularly important to industries where cybersecurity is a top priority.

TCG platform certificates capture snapshot attributes of platforms during manufacturing, assembly and test, and integration. These platform attributes are then cryptographically linked to the specific device using the Trusted Platform Module (TPM) as the hardware root of trust.

TCG platform certificates provide key device provenance, traceability, and visibility into the device digital supply chain. TCG platform certificates can be used to reduce risk and improve detection of counterfeiting, unauthorized production, tampering, theft, and insertion of unexpected hardware.

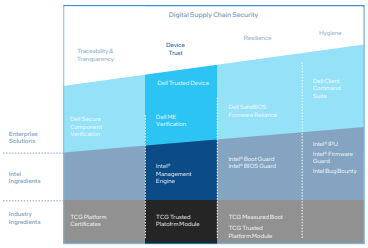
As a supplier of enterprise solutions, Dell has implemented TCG platform certificates within the Dell Secured Component Verification (SCV) solution for commercial PCs and PowerEdge servers. SCV delivers cryptographically signed inventory certificates to IT for supported Dell devices. With secure self-verification tools, SCV helps assure full hardware integrity during transit to IT environments and allows customers to verify that Dell commercial PCs and key components arrive as they were ordered and built. Platform certificates and Dell SCV tools are designed to be integrated with existing scripts to facilitate the validation process, making trusted deployment an automatable process.

Similarly, Intel has been enabling vendors with base digital supply chain transparency and traceability for many years. Intel® Transparent Supply Chain (Intel® TSC) delivers TCG platform certificates and component data for supporting

Intel technology-based platforms using a cloud API available to IT through the Intel TSC web portal. Although Dell and Intel opted to implement independent solutions, TCG platform certificates are a common ingredient between Intel TSC and Dell SCV. This commonality provides compatibility and interoperability that enable enterprise and government buyers to deploy TCG platform certificates for improved digital supply chain security of Intel technology-based devices.

The NIST NCCoE also takes an active role in driving digital supply chain security. NIST NCCoE Special Publication 1800-34 is currently underway. SP-1800-34 has the goal to demonstrate how organizations can verify that the internal components of the computing devices they acquire are genuine and have not been tampered with. This solution relies on device vendors storing information within each device, so that customers can use a combination of commercial off-the-shelf and open-source tools to validate the stored information. Vol B [Prelim Draft Aug 2021] specifies TCG platform certificates as a key industry standard way of reducing risk and increasing visibility into high tech supply chains. Vol C [Prelim Draft Jan 2022] recommends solutions that include Intel TSC and Dell SCV.

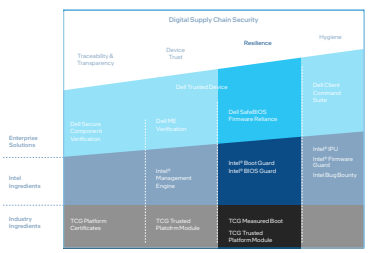
Device Trust



In addition to transparency and traceability requirements for a device's digital supply chain journey, it is also key for IT managers to ensure that the devices they deploy are authentic. Intel and Dell enable new levels of device trust using the Intel® Manageability Engine (Intel® ME). The Intel ME is an energy-efficient computing subsystem within Intel chipsets that enables hardware-enhanced platform features. Among its many functions, it provides a CPU- and OS-isolated environment to perform key security and manageability operations.

Dell employs the unique identification capability of the Intel ME to enhance device trust through Dell ME Verification. This capability aids in verification and authenticity of Dell desktop and laptop systems and helps ensure that only validated and approved Intel ME software updates are deployable on Dell hardware.

Resillience



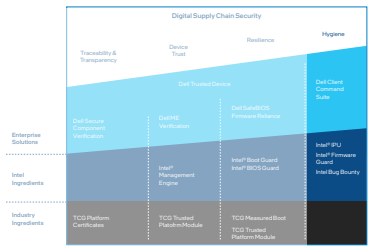
Device resilience includes the ability to detect tampering of critical BIOS or firmware during the device's journey through the supply chain. Although the technology and capability innovations in this area were originally designed to protect firmware and BIOS from runtime attacks seeking to go below the OS, these same technologies provide tamper evidence and protection as the device moves through the supply chain.

To protect device firmware and BIOS, Dell SafeBIOS employs innovative off-host verification against known good BIOS measurements. Deviations from these known good BIOS measurements may indicate unauthorized firmware or BIOS tampering within the supply chain. Dell SafeBIOS is a key component of the Dell Trusted Device portfolio of technologies that draws on two key ingredients of Intel® Hardware Shield on Intel vPro® platforms:

- **Intel Boot Guard** is designed to protect critical system boot functions. It serves as an effective detection mechanism to verify that the integrity of the earliest and most critical code executed by the processor—the Initial Boot Block (IBB)—remains intact. If Intel Boot Guard detects modifications to the IBB, Dell policy incapacitates the system to prohibit further unauthorized activity.
- **Intel® BIOS Guard** provides key BIOS safeguards that improve trust and resilience within the device supply chain. It reduces the risk of flash-based attacks on the BIOS of Intel platforms and protects against BIOS tampering within the supply chain.

As board members of the TCG, Dell and Intel have made significant contributions and investments in TCG standards designed to improve the resilience of the device through the supply chain and into its operational phase. For example, the TCG specification for measured boot on Intel architecture-based Dell devices employs storage of key BIOS, firmware, and bootloader configurations within the industry-standard Trusted Platform Module. This approach enables the devices to detect unauthorized changes or modifications to BIOS, firmware, or bootloader code within the supply chain.

Hygiene



Device hygiene consists of applying technology and industry best practices to ensure that devices are fully updated and as secure as possible. Intel continues to invest significantly in the areas of vulnerability detection and mitigation. One of the largest and most visible of these investments is Intel's global bug bounty program, which invites the hacking and vulnerability research community to partner with Intel to detect and remove vulnerabilities on devices. The program provides recognition to encourage external security researchers to report security vulnerabilities they find in Intel products and then collaborate and coordinate with Intel on disclosure. Founded in 2017, the program ranked fourth in the industry in terms of total payouts in 2020.[1]

Working closely with the ecosystem to uncover and mitigate vulnerabilities is critical, but it is only one part of the necessary solution. Packaging, validating, and working collaboratively with Intel's OEM customers is also needed to ensure that mitigations make their way into functioning systems within IT environments.

To ensure optimal device hygiene, Intel regularly releases functional and security updates for supported products and services by means of Intel Platform Update (IPU). Due

to the highly integrated nature of hardware, firmware, and software, updates may require additional validation and integration from Intel's ecosystem partners participating in the coordinated vulnerability handling process.

Critical patches and vulnerability mitigations ultimately make their way into IT supported devices through patch and vulnerability management software, such as Dell Client Command Suite, which manages and automates system updates for Dell devices. Dell Client Command Suite simplifies patch management by easily identifying, locating, and installing the latest BIOS, firmware, drivers, and applications.

Looking Forward

Supply chain security will continue to capture headlines and drive action within industry standards and regulatory bodies for the foreseeable future. Many IT, information security, and government organizations are just now beginning the journey to identify advancements and available capabilities to help secure their computer supply chains. Dell and Intel have decades-long records of investment and involvement with industry standards bodies to foster innovation in supply chain security. Across the spectrum of traceability and transparency, device trust, resilience, and hygiene, today's solutions offer levels of digital supply chain security that were unavailable commercially just a few years ago.

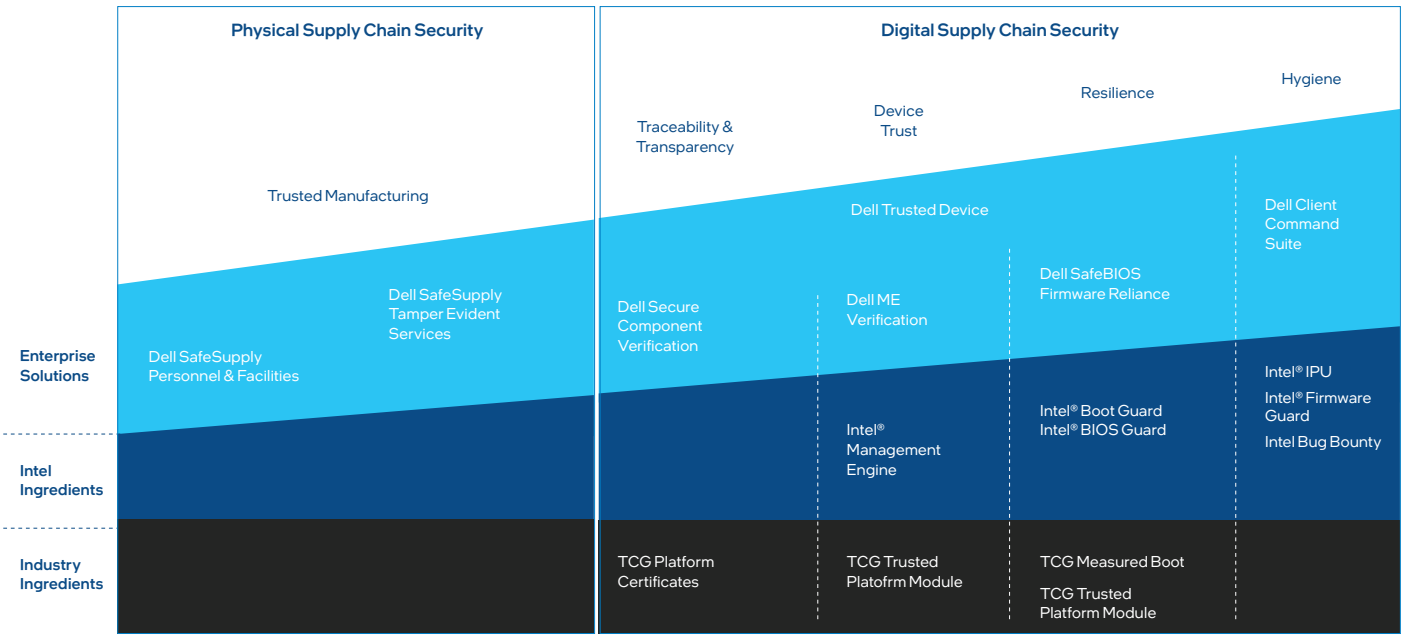


Figure 6. Industry-leading supply chain solution leveraging Dell and Intel innovations.

More Information

Intel: Securing Your Business Throughout the Supply Chain –
intel.com/content/www/us/en/products/docs/servers/transparent-supply-chain.html

A Partnership of Trust: Dell Supply Chain Security –
i.dell.com/sites/csdocuments/CorpComm_Docs/en/supply-chain-assurance.pdf

[1] ZDNet, June 29, 2020. "HackerOne's 2020 Top 10 public bug bounty programs." https://www.zdnet.com/article/hackerones-2020-top-10-public-bug-bounty-programs/.
Performance varies by use, configuration, and other factors. Learn more at https://www.intel.com/PerformanceIndex.
No product or component can be absolutely secure.
Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.
Your costs and results may vary.
Intel technologies may require enabled hardware, software, or service activation.

0222/PB/MESH/346433-001US