Dell Supply Chain Assurance

Dell Supply Chain Assurance

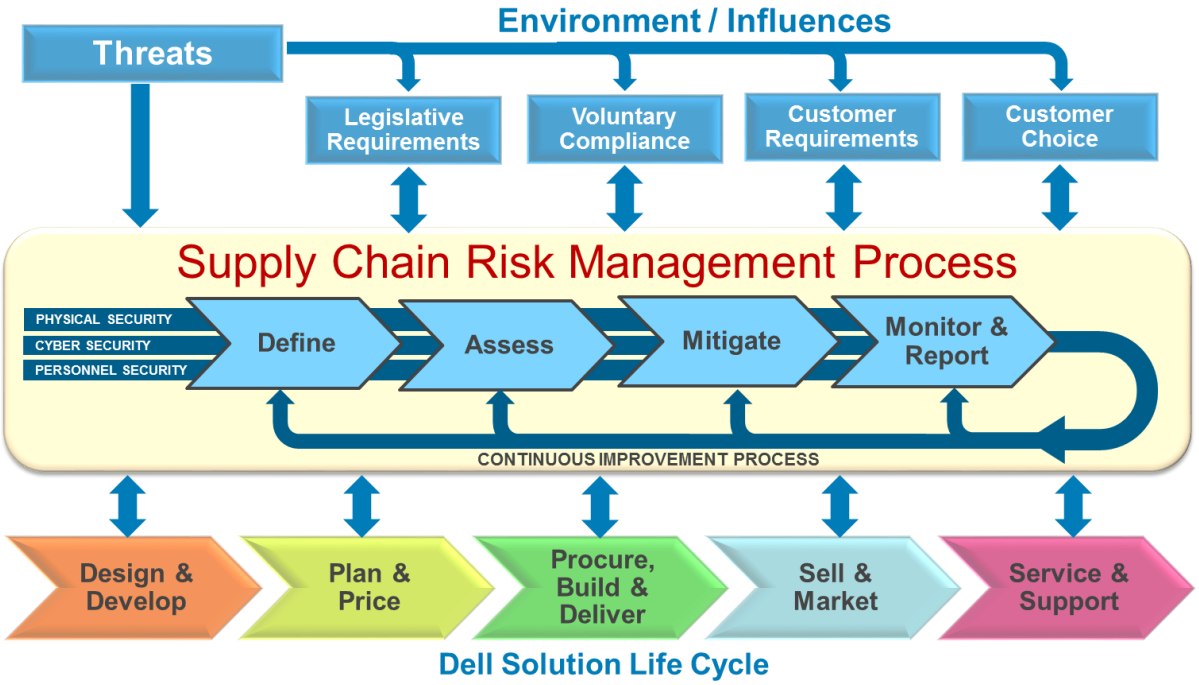
Introduction

Security-sensitive customers of information and communications technology (ICT) solutions must be vigilant to protect the confidentiality, availability, and integrity of the data and systems they depend on to conduct their business. Disruption of those ICT solutions or unauthorized and unintended exposure of data could put organizations and people at significant risk. Unfortunately, malicious adversaries continue to identify and exploit potential supply chain security gaps with greater persistence and ingenuity than ever. There are multiple opportunities for product tampering in the ICT supply chain that must be addressed by providers of ICT solutions, including the insertion of counterfeit components, the embedding of malware, or the insertion of coding vulnerabilities in firmware.

Dell takes a holistic and comprehensive approach to protect its supply chain and deliver solutions that customers can trust. Dell's strategy of defense-in-depth and defense-in-breadth involves multiple layers of controls to mitigate risks that could be introduced in the supply chain. These controls help establish ***supply chain assurance***, defined as the confidence that the aggregated set of processes and controls throughout the supply chain and product lifecycle will produce and deliver products, processes and information that are free of unintended elements and that function as designed and intended. This document provides a brief overview of Dell's strong governance mechanisms and supply chain security and integrity practices for Dell EMC and the Dell Client Business.

Continuous risk assessment and improvement

Dell's Supply Chain Risk Management framework (below) mirrors that of the comprehensive risk management framework of the National Infrastructure Protection Plan (NIPP), which outlines how government and the private sector can work together to mitigate risks and meet security objectives. Dell's framework incorporates an open feedback loop that allows for continuous improvement. Risk mitigation plans are prioritized and implemented as appropriate throughout the entire solution life cycle.



Supplier governance

Supplier governance is critical to safeguarding the performance and integrity of the supply chain. Dell's supplier governance begins with a thorough review of potential suppliers and partners prior to onboarding. Analysis prior to awarding work may include initial site surveys and manufacturing qualification builds in conjunction with the completion of the product-specific request for information (RFI) or quote (RFQ). As part of our ongoing relationship with suppliers:

1. Dell conducts several types of audits that contribute to our security oversight of the supply chain. For instance, process compliance audits are performed regularly at each of our Original Design Manufacturers (ODMs) and contract manufacturers. These audits utilize both onsite quality teams, as well as site visits to confirm that ODMs and contract manufacturers are following prescribed processes.
2. Dell enforces a Global Inventory Control Policy that applies to Dell-owned inventory held by Dell or a third party. Dell and third-party facilities must meet security, physical handling, storage, and segregation requirements for holding inventory. The policy also includes requirements for global analysis and reporting as well as quality control processes for missing and damaged products. These inventory processes and controls provide day-to-day governance that augments official audits.
3. Dell also measures suppliers' security practices against industry best practices for physical security and for mitigating counterfeit components, tainted software and firmware, and intellectual property theft. When gaps are identified, Dell issues corrective actions and works with suppliers to build their capabilities in meeting industry best practices.
4. Quarterly Business Reviews are conducted with all key suppliers to evaluate performance against Dell's expectations. Key performance indicators and other specified metrics are monitored so that Dell's customers continue to receive high-level product quality at a competitive price. Frequent executive-level interactions also help Dell and its partners to respond quickly and effectively to changes in technology, demand, legislation, or customer requirements.

Supply chain security

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

Physical Security

Factories where Dell products are built must meet specified Transported Asset Protection Association (TAPA) facility security requirements, including the use of closed circuit cameras in key areas, access controls, and continuously guarded entries and exits. Additional controls are applied at Dell and supplier-managed facilities and for air, rail, and ocean shipments to address the variety of risks faced across transportation modes and regions. Some of these protections include tamper-evident packaging, security reviews of shipping lanes, locks or hardware meeting required specifications, and container integrity requirements. GPS tracking devices may also be placed on any container and monitored 24x7 until confirmation of delivery.

Dell also maintains certification with the United States Customs and Border Patrol's Customs-Trade Partnership Against Terrorist (C-TPAT). This logistics security program is recognized as compatible with similar programs around the world, including the Authorized Economic Operator (AEO), Canada's

Partners in Protection, and Singapore's Secure Trade Partnership programs. While the primary focus of those programs is to prevent contraband, the required protections also guard against tampering with products being imported.

Information Security

Through the normal course of business, Dell collects and uses sensitive information about products, solutions, customers, suppliers and partners throughout the supply chain lifecycle. Numerous measures are used to guard this sensitive information against exposure and exploitation. For example, data transfers between Dell and its partners use a combination of encryption methods and private circuits. 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 limit 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 "segregation of duties" and "least privilege," 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 duties.

Personnel Security

Personnel security controls are a critical part of information security and supply chain assurance. 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 also undergo regular security awareness training, which helps reduce behavior that may put products at risk throughout the supply chain. As part of Dell's annual compliance training, employees are required to complete courses regarding information security and other Dell security practices. Employees are also encouraged to self-educate through various informal avenues, such as reading corporate newsletters, internal and external security websites and customer whitepapers, attending seminars, or taking additional online courses and video training as appropriate.

Dell protects its confidential data by disclosing only pursuant to a non-disclosure agreement (NDA) or other binding contractual provisions that restrict permissible uses and disclosures of the data. As a condition to employment at Dell, employees are required to sign an NDA that protects intellectual property, customer information, and other sensitive data even beyond the date of their departure from Dell.

Supply chain integrity

Supply chain integrity defines the effort to ensure that the product received by the customer is the product the customer expected and will operate 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

Dell has put in place a variety of quality control processes to help minimize the opportunity for counterfeit components to infiltrate our supply chain. Dell's new product introduction process verifies that materials are sourced from the approved vendor list and match the bill of materials as appropriate. Parts are procured directly from the original design manufacturer (ODM) or Original Component Manufacturer (OCM) when possible.

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. Additionally, Dell maintains ISO 9000 certification for quality control practices at global manufacturing sites. Adherence to these processes and controls helps minimize the risk of counterfeit components being embedded within Dell products.

Software

Industry software engineering best practices include security throughout the development process for any code, including operating systems, applications, firmware, and device drivers. Dell reduces opportunities for the exploitation of software security flaws by incorporating Secure Development Lifecycle (SDL) measures throughout the development process. These measures are tightly aligned with Software Assurance Forum for Excellence in Code (SAFECode) guidelines and ISO 27034.

Proactive verification, validation, and security testing activities throughout the life cycle help to ensure more secure software and reduce the likelihood of malware or coding vulnerabilities from 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.

Dell has also implemented procedures across our commercial servers, desktops, and laptops in accordance with the guidance and recommendations outlined in NIST SP 800-147, Basic Input/Output System (BIOS) Protection Guidelines. Dell's protected BIOS and signed update mechanism help prevent unauthorized modification of the platform firmware and reduce the risk of pre-boot malware or unwanted functionality.

Dell PSIRT (Product Security Incident Response Team) monitors vulnerabilities impacting Dell products and coordinates rapid security remediation to help customers maintain the security posture of Dell products after delivery.

Stronger together

Dell participates in supply chain risk management activities with trusted industry groups and public-private partnerships. This demonstrates Dell's commitment to partnering with leading organizations that further the development of standards and industry best practices for mitigating supply chain and product security risks. Dell has been actively engaged in the Open Group Trusted Technology Forum (O-TTPF), the Software and Supply Chain Assurance Forum, SAFECode, the Supply Chain Risk Leadership Council, the Internet Security Alliance, and the IT Sector Coordinating Council. Dell is also an active member of the Government Information Data Exchange Program (GIDEP).

Dell has participated in the development of numerous standards and best-practice guidelines related to supply chain integrity including the Open Group Trusted Technology Provider Standard (O-TTPS) which is also recognized as ISO 20243, SAFECode, ISO 27036, and National Institute of Science and

Technology (NIST) Interagency Report (IR) 7622, NIST Special Publication (SP) 800-161, NIST SP 800-53, and the NIST Cybersecurity Framework. To address customer concerns about product tampering and supply chain assurance, Dell continues to monitor and influence the development and potential impact of legislation, regulations, voluntary standards, and contract language.

Dell is uniquely positioned to leverage insights, best practices, technology and expertise from industry-leading, trusted and respected brands in the Dell Technologies portfolio like Pivotal, RSA, SecureWorks, Virtustream, and VMware. Dell believes that it is critical to listen to and work with customers, suppliers, and partners to continue to improve how Dell delivers supply chain assurance. For more information, please contact your Dell Sales Representative.