

Dell EMC's Enhanced Supply Chain Assurance and Product Security Program



Dell EMC is committed to being the preferred supplier of end-to-end, cutting-edge technology solutions to customers.

Delivering Trustworthy Products Straight Out of the Box

Security-sensitive organizations are becoming increasingly aware of the potential threats to Information and Communication Technology (ICT) supply chains. Cyber threats continue to evolve as nefarious actors try to find the most efficient, effective, or easiest way to take advantage of any weak link in the supply chain that will allow them to gain access to protected information or to disrupt the ability of their targets to accomplish their mission. Threats to the ICT supply chains include malware, coding vulnerabilities, and counterfeit electronic components that are inserted into products within the supply chain—any time between the initial design and development of the product through actual delivery to customers.

Recognizing the risk to their national security missions, federal agencies in the U.S. continue to lead the demand for the development of stronger ICT supply chain security requirements and regulations. Other government entities and critical infrastructure industry sectors like finance and energy are not far behind.

Dell EMC is committed to being the preferred supplier of end-to-end, cutting-edge technology solutions to customers whose mission demands trustworthy product security straight out of the box. Dell EMC leverages a robust Supply Chain Risk Management (SCRM) Program to ensure foundational controls for all product supply chains meet or exceed customer expectations and industry standards. Our Supply Chain Assurance Program focuses on giving customers the confidence that the products they acquire from Dell are exactly what they expected them to be, nothing more and nothing less, and that they will operate as intended. This is accomplished through an evolving strategy of defense-in-depth and defense-in-breadth that relies on multiple layers of supply chain security and integrity controls throughout the entire supply chain:

Supply Chain Security

Preventive and detective control measures that protect physical assets, inventory, information, intellectual property and people.

Physical Security

- Protecting products in manufacturing and fulfillment facilities as well as during transport.
- Participation in the Customs-Trade Partnership Against Terrorism (C-TPAT) program.
- Adherence to Transported Asset Protection Association's (TAPA) Facility Security Requirements (FSR) certification requirements at key facilities.

Personnel Security

- Hiring practices include thorough background check of potential employees
- Employees must take and pass annual workplace security and compliance training

Information Security

- Protecting customer information
- Protecting production systems and corporate networks
- Protecting proprietary information

Supply Chain Integrity

Controls to ensure the product received by the customer is the product the customer expected, and that the product will operate as intended.

Hardware Integrity

- Mitigate risks of counterfeit components*
- ISO 9001 Quality Management System
 - Traceability of key components
 - Functional testing of all products prior to shipment

Software Integrity

- Mitigate risks of malware, taint, and coding vulnerabilities*
- Rigorous Security Development Lifecycle (SDL) based on industry standards (ISO/IEC 27034) and best practices (SAFECode)
 - BIOS protections support NIST 800-147 guidelines
 - Multiple validation and verification capabilities and tools deployed throughout the solution life cycle and supply chain





What is Dell EMC's Enhanced Supply Chain Assurance and Product Security Program?

Many security-sensitive government agencies and customers already require their suppliers to comply with industry-standard protections or relevant guidelines that have been published by organizations such as the National Institute of Science and Technology (NIST). However, quite a few have determined that they need to go above and beyond common ICT practices to mitigate the risk further. Implementing additional requirements will result in a higher level of confidence and trust in the ICT products they acquire. Based on input from customers across a variety of key industries, Dell EMC is developing a service offering program that employs the most advanced supply chain integrity threat protection at competitive pricing while maintaining its industry-leading quality and support.

Dell EMC expects to release its Enhanced Supply Chain Assurance and Product Security Program in 2018. The Program is an optional premium bundle of services that further ensure integrity and document custodial control through the product's journey to its final destination. It establishes the root of trust for these Dell EMC systems and their key components in an existing US-based custom solution fulfillment center. Dell EMC will leverage existing service offerings as part of the premium services bundle as much as possible to avoid attracting unwanted attention to these systems. Only those employees with "need to know" are aware that specific systems will receive the enhanced security controls, allowing the systems to "hide in plain sight" throughout the fulfillment process. Some new tamper-evident and tamper-resistant control measures are being implemented throughout the process to increase further the confidence that the system integrity is being protected.

This program leverages industry-leading software vulnerability scanning tools to detect risks for each unique system configuration with ongoing analysis and security assessments as new coding vulnerabilities are discovered and as new device drivers and firmware patches are released. After each customer system arrives in the fulfillment center, the hard drive is wiped in accordance with NIST media sanitization guidelines (NIST SP 800-88 Rev.1). The system image is then securely reloaded ensuring that approved device drivers are installed. Several tamper-resistant and tamper-evident controls are employed to provide additional layers of risk mitigation. The systems are then transported on a dedicated trailer with a team of qualified drivers from the fulfillment center directly to the customer destination. In transit, additional tamper-resistant and tamper-evident controls are leveraged, including GPS tracking of the shipment (monitored 24/7) to ensure no unauthorized stops or route deviations are made and a serial numbered bolt seal that is verified by the customer upon arrival.

Dell EMC will continue to collaborate with interested customers as the program is finalized and scaled across product lines to ensure that our value-added offering meets the needs of our customers.

	<p>Software Assurance</p> <p>Validated source code and system images to enhance software security</p>	<ul style="list-style-type: none"> • Each configuration is validated using industry-leading tools to detect malicious code and coding vulnerabilities including <ul style="list-style-type: none"> ○ Signature-based anti-virus scans and ○ Signature- and behavior-based coding vulnerability detection. • On-going threat analysis and security assessments.
	<p>Hardware Security</p> <p>Trusted components that have been tested against known vulnerabilities</p>	<ul style="list-style-type: none"> • Storage sanitization in accordance with NIST SP 800-88 standards prior to final system imaging. • Any variation in components that results in a unique configuration will be assessed thoroughly to ensure that the new components are trusted
	<p>Solution Integrity</p> <p>Functional testing, software verification, and tamper-evident & tamper-resistant controls</p>	<ul style="list-style-type: none"> • Verify BIOS and image and perform functional test. • Port blockers added to prevent tampering of USB and RJ45 ports. • White glove audit of key controls • Tamper-proof and tamper-evident packaging
	<p>Last Mile Secure Logistics</p> <p>Dock-to-dock chain of custody with monitored GPS tracking</p>	<ul style="list-style-type: none"> • Dock-to-dock dedicated team delivery • Verified driver team qualification per destination requirements • GPS-based location tracking and real-time monitoring of route • Bolt seal verified by customer at destination

For more information, please contact your Dell EMC Services Representative.