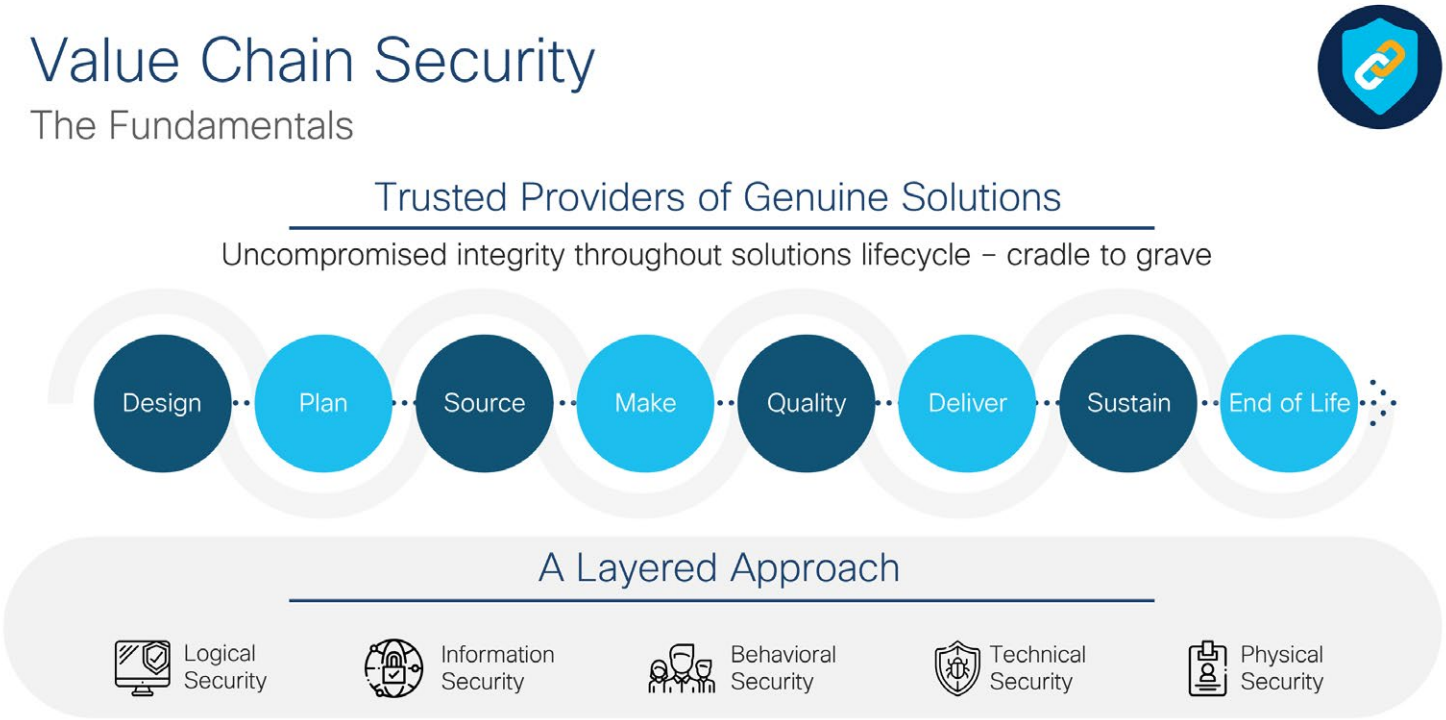
Cisco Value Chain Security Key Questions/Answers

The Cisco Trust Transformation Office (TTO) offers a number of documents that provide insight into how Cisco mitigates the potential risk of adversaries penetrating our supply chain. The following Overview discusses how Cisco protects its value chain against attempts to breach Information Communications Technology (ICT) in order to gain unauthorized access to data, alter that data, interrupt communications, or disrupt critical infrastructures. The Cisco Value Chain Security approach also applies to parts manufacturers, completed product (and/or the warehouse where it is stored), distribution centers, and channel partners from whom customers acquire Cisco products and services. These Cisco strategic security measures are dynamic, designed to continually assess, monitor, and improve security throughout the Cisco value chain.

What is the Cisco value chain and how is it secured?

See below for a graphical overview of the Cisco value chain and its approach to security.



While we do not disclose the specific members of our value chain, Cisco drives a layered security approach through the entire ecosystem at all stages of a product's lifecycle, whether hardware, software, or cloud offerings. To the extent that the use of an enterprise's technology is restricted in any manner by government regulations, Cisco complies with all such requirements. In addition to mandatory regulatory requirements, Cisco's practices have garnered the status of Tier III C-TPAT, as well as PIP, AEO, OAE, among others.

Cisco Value Chain Security is designed to:

- Produce Cisco solutions in securely controlled development, manufacturing, logistics, and channel environments. In addition, Cisco solutions are developed using Cisco approved processes and tools with approved software modules and hardware components
- Secure processes are designed to prevent introduction of malware and or rogue raw materials that could compromise functionality.
- Secure develop, build, and deploy processes are designed to make it very difficult for malicious actors to produce counterfeit solutions.

What specific processes and practices are embedded throughout the Cisco value chain?

Cisco is committed to eliminating tainted solutions, counterfeit solutions, and misuse of intellectual property throughout the Cisco value chain, a rigorous set of security practices, processes, and technology are deployed. Specific examples include:

1. **Logical Security Processes** Cisco Value Chain Security ensures that data is transmitted via dedicated lines and/or uses encryption. The Logical Security process also establishes and validates adherence to scrap handling processes, such as mandating certifications for the production and destruction of key counterfeit protection labels so they cannot be misused.

2. **Technical Security** Applying technological innovation to enhance counterfeit detection, terminate functionality, or identify non-authorized components or users is embedded throughout the Cisco value chain. Smart chips, data-extracting test beds, and proprietary holographic or intaglio security labels are a few of the innovations used to secure the value chain.

3. **Physical Security Practices** Physical aspects of security, such as camera monitoring, security checkpoints, locking devices, alarms, and electronic access control govern physical locations.

What quality control practices are deployed throughout the Cisco value chain?

Cisco has a comprehensive quality plan and organization that support our entire value chain ecosystem.

- Product quality engineering – Pervasively monitoring and assuring product quality throughout the new product introduction cycle, manufacturing, and with customers in the field.
- Customer quality engineering – Driving continuous improvement for customer hardware quality and reliability, and managing high touch customer quality escalations, should they occur.
- Software quality engineering – Driving software quality requirements, measurements, and improvements.
- Failure analysis – Providing root cause and corrective action to prevent future failure events using material science and failure analysis data analytics.
- Highly accelerated life testing – Performing overstress tests to precipitate defects not found in normal test to drive quality and reliability in the early development lifecycle.
- Quality Management Operation System – Governing processes, metrics, and capabilities that guide quality efforts across all of Supply Chain Operations. Also, driving quality improvements across the extended supply chain partner ecosystem.
- Reliability Engineering –Driving design for reliability across all product lines.

More Information

More information about the Cisco Value Chain Security Architecture, can be found at: www.cisco.com/go/valuechainsecurity.

Cisco's Supply Chain Resilience Management (SCRM) practices are outlined in a NIST Cyber SCRM Case Study located at: https://csrc.nist.gov/CSRC/media/Projects/Supply-Chain-Risk-Managements/documents/case_studies/USRP_NIST_Cisco_071515.pdf

Supplier's secure development lifecycle (SDL) practices are as outlined at: https://www.cisco.com/c/en/us/about/security-center/security-programs/secure-development-lifecycle.html.

Reach out to the Trust Transformation Office with any further questions or assistance requirements: https://www.cisco.com/c/en/us/about/trust-center.html