Security Across the Cisco Supply Chain

Security at every lifecycle stage:

- Design and Development
- Planning and Ordering
- Sourcing and Manufacturing
- Delivery and Post-delivery (Sustainment)
- End of Life

Our Comprehensive Approach:

PRODUCT LIFECYCLE	Touch every stage of the product lifecycle, from design through end of life.
MULTIFACETED SECURITY	At every stage, apply some combination of security technology, physical security, and logical, rules-based security.
DESIGN	Incorporate security into products from inception.
LAYERED APPROACH	Use a layered approach to strengthen anti-counterfeiting, traceability, and anti-tampering.
INDUSTRY LEADERSHIP	Work to develop stronger standards, policies, and tools across the industry.

Why Cisco

We recognize the important role of supply chain security in a comprehensive cybersecurity strategy. We are dedicated to helping you assess and address security threats and vulnerabilities. Our supply chain security program continually assesses, monitors, and improves our supply chain security capabilities throughout the entire lifecycle of our products. We consistently strive to enhance security and earn our customers' trust.

Cisco Supply Chain Security

PROTECTING CUSTOMERS WITH SUPPLY CHAIN SECURITY THROUGHOUT THE PRODUCT LIFECYCLE

Cisco® recognizes the important role of supply chain security in a comprehensive Cisco cybersecurity strategy. Under that strategy, we deploy a capability that continually assesses, monitors, and improves the security of the Cisco supply chain throughout the entire lifecycle of our solutions. Our commitment is to strive to meet our customers' integrity expectations.

What You Can Expect from Cisco Supply Chain Security

- Our solutions are genuine (not counterfeit)
- Our solutions operate as our customers direct them to (not secretly controlled by or transmitting data to unknown parties)

Cisco Supply Chain Security Process

We manage a coordinated program across our engineering, manufacturing, technical services teams, together with our suppliers and channel partners, to ensure the most effective technology is used to:

- Retain Cisco products in controlled manufacturing and channel environments, using approved components
- Limit introduction of malware and/or rogue components that could compromise functionality
- Build devices and deploy processes that make it more difficult to produce undetectable counterfeit Cisco equipment

Cisco Supply Chain Security Focus Areas

- Tainted Products
- Counterfeit Products
- Misuse of Intellectual Property

Elements of Cisco Supply Chain Security

- **Physical Security Practices**—Physical aspects of security such as camera monitoring, security checkpoints, locking devices, alarms, and electronic access control
- **Logical Security Processes**—Systematic, repeatable, and auditable security processes designed to target areas of security risk and secure them. For example, Cisco Supply Chain Security helps ensure that data is transmitted via dedicated lines and/or uses encryption, establishing, and validating adherence to scrap handling processes, mandating certifications of production, and destruction of key counterfeit protection labels
- **Security Technology**—Applying technological innovation to enhance counterfeit detection, terminate functionality, or identify non-authorized components or users. Smart chips, data extracting test beds, and proprietary holographic or intaglio security labels are a few of the technological innovations used in securing our supply chains