Security Across the Cisco Value Chain

Security at every lifecycle stage:

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

Our Comprehensive Approach:

Solutions Lifecycle
Touch every stage of the solutions 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 solutions from inception.

Layered Approach
Use a layered approach to strengthen anti-counterfeiting, traceability, and anti-tampering.

Industry Leadership
Work to develop a limited set of standards, policies, and tools across the industry.

Why Cisco

We are dedicated to helping you assess and address security threats and vulnerabilities. Our Value Chain Security capability continually assesses, monitors, and improves our value chain security capabilities throughout the entire lifecycle of our solutions. We consistently strive to enhance security and earn our customers' trust.

Cisco Value Chain Security Program

Protecting Customers with Value Chain Security Throughout the Solutions Lifecycle

Cisco recognizes the important role of value 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 value 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 Value 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 Value Chain Security Process

We manage a coordinated program across our engineering, manufacturing, and technical services teams, together with our global suppliers and channel partners to:

- Retain Cisco products and solutions in controlled development, manufacturing, logistics, and channel environments, using approved processes and tools together with software modules and hardware components
- Limit introduction of malware and/or rogue raw materials that could compromise functionality
- Develop technology, build devices, and deploy processes that make it more difficult to produce undetectable counterfeit Cisco solutions

Cisco Value Chain Security Focus Areas

- Tainted Solutions
- Counterfeit Solutions
- Misuse of Intellectual Property

Elements of Cisco Value 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. Cisco Value Chain Security helps ensure that data is transmitted via dedicated lines and/or uses encryption. This helps establish and validate adherence to scrap handling processes and mandate 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 innovations used in securing our value chain