Cisco Value Chain Security Program

Protecting Customers Throughout the Solutions Life Cycle

A Comprehensive Approach:

Solutions Life Cycle

Security at every stage of the solutions life cycle

Multifaceted Security

Layer security technology, physical security, logical, rules-based security, and information security

Industry Leadership

Cisco collaboratively drives security standards, policies, and tools across the industry

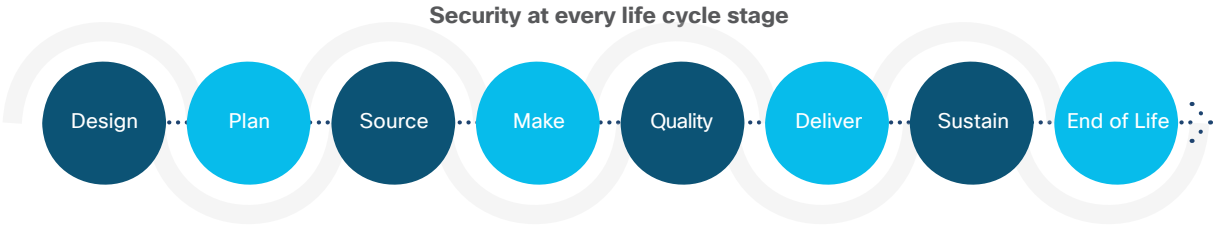
Why Cisco?

A trusted partner that assesses risk and effectively addresses security while enabling our customers' business

We earn your trust

cisco.com/go/valuechainsecurity

Cisco embeds value chain security within its comprehensive Cisco cybersecurity strategy. Value chain security continually assesses, monitors, and improves the security of the third parties who are part of our solutions' life cycles. 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 customers direct them to and are not subject to tampering (not controlled/accessible by 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, software and hardware components
- Limit introduction of malware and/or rogue raw materials
- Develop technology, build devices, and deploy processes that make it more difficult to produce undetectable fake or altered Cisco solutions

Cisco Value Chain Security Exposures Addressed

- Tainted solutions
- Counterfeit solutions
- Misuse of intellectual property
- Third party information security breach

Cisco's Layered Approach to Value Chain Security

- **Physical Security:** Practices including camera monitoring, security checkpoints, alarms and electronic or biometric access control
- **Logical Security:** Systematic, repeatable, and auditable operational security processes including encryption, materials and failure analysis segregation and scrap weight validation
- **Security Technology:** Technical innovation to enhance counterfeit detection, terminate functionality, or identify non-authorized components or users including smart chips, data-extracting test beds, and proprietary holographic or intaglio security labels
- **Information Security:** Data and information systems protection including remote access limitation, configuration management, network segmentation, multi-factor authentication and data classification