

# Cisco Value Chain Security Key Questions/Answers

Cisco employs a dynamic and layered risk management approach to ensure the security and authenticity of products throughout their full lifecycle, a strategy we refer to as “Value Chain Security” (VCS). The following key questions and answers address how Cisco protects its value chain against attempts to breach Information Communications Technology (ICT) to gain unauthorized access to data, interrupt communication, or disrupt critical infrastructure.

The Cisco VCS approach includes a security policy and program embedded with product and part manufacturers, distribution centers, and channel partners from whom customers acquire Cisco products and services. These strategic measures are dynamic as they continually involve assessing, monitoring, and improving security throughout the Cisco Value Chain.



## What is Cisco Value Chain Security?

Cisco VCS helps safeguard every layer by implementing robust security measures, fostering a culture of vigilance, and continuously adapting to emerging threats. We are committed to protecting our customers, partners, and suppliers by ensuring that every link in our value chain operates securely and efficiently.

Through proactive risk management, collaborative efforts, and innovative solutions, we strive to build a resilient and trustworthy ecosystem that upholds the highest standards of Cisco security and compliance.

Cisco VCS is applied across engineering, manufacturing, and technical services teams, along with our global suppliers and channel partners, to:

- Produce Cisco solutions in securely controlled development, manufacturing, logistics, and channel environments. In addition, Cisco solutions are developed using established processes and tools, along with approved software modules and hardware components.
- Secure and harden processes designed to prevent introduction of malware and/or rogue raw materials that could compromise functionality.
- Implement a Secure Development Lifecycle and a vulnerability management program.
- Develop and maintain risk, resiliency, and incident response plans.
- Build and deploy processes that make it exceedingly difficult, if not impossible, to produce counterfeit solutions.

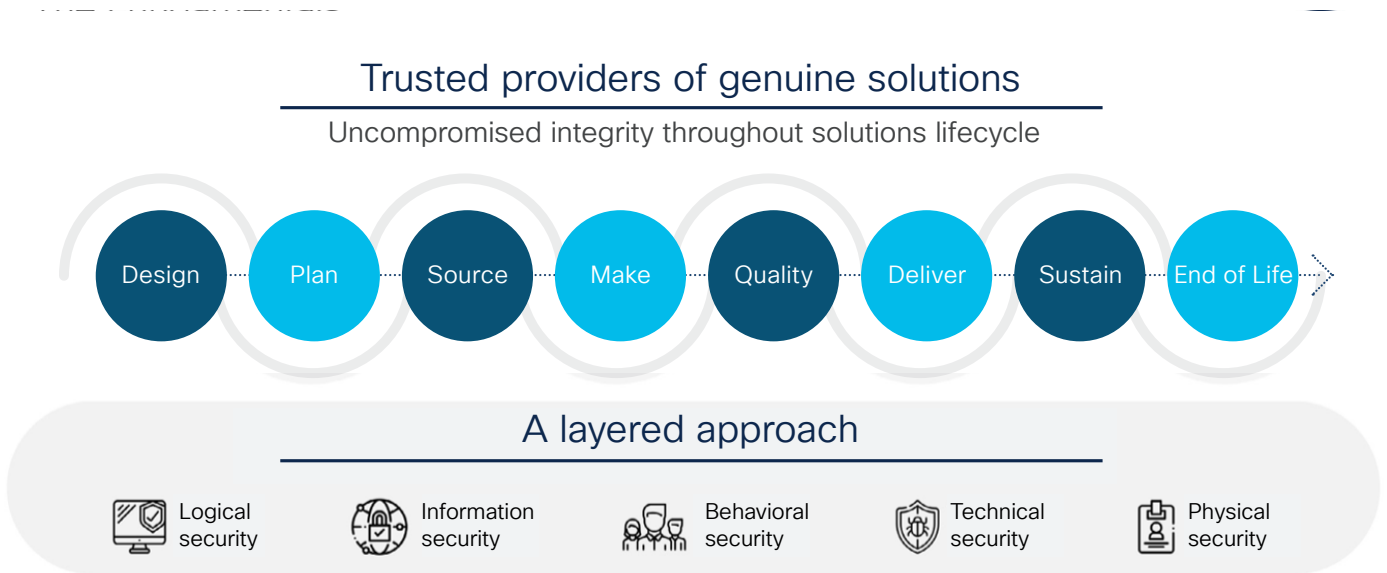
## What third-party vendors are included in the Cisco Value Chain?

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 many industry accolades and acknowledgements, including Best Practices in Cyber Supply Chain by NIST, Gartner's Top 25 Supply Chains list, and Tier III C-TPAT, among others.

# What specific security processes and practices are embedded throughout the Cisco Value Chain?

To eliminate the possibility of tainted solutions, counterfeit solutions, and misuse of intellectual property throughout the Cisco Value Chain, a rigorous set of security practices, processes, and technologies are deployed and audited. Specific examples include:

- **Logical Security Processes** Cisco VCS 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 to prevent misuse.
- **Technical Security** Technological innovations 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.
- **Physical Security Practices** Physical aspects of security, such as camera monitoring, security checkpoints, locking devices, alarms, and electronic access control, govern physical locations.



## Where can I learn more about Cisco VCS?

More information on these topics, as well as other Cisco security initiatives can be found on the [Cisco Trust Center](#).

