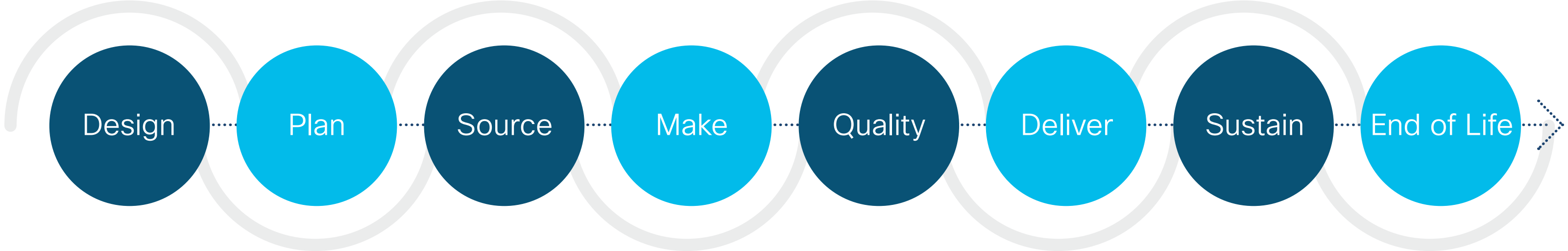
What is a Value Chain?

The end-to-end lifecycle for hardware, software or services that delivers value

What Is **The Cisco Value Chain**?

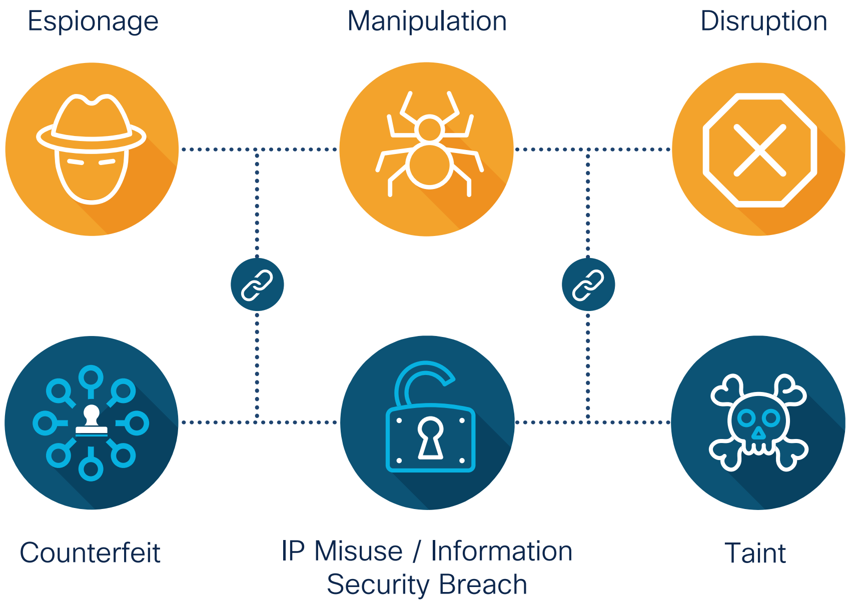
The interconnected ecosystem that supports the lifecycle of **Cisco solutions**

Value Chain Stages



Design → Plan → Source → Make → Quality → Deliver → Sustain → End of Life

Value Chain Threats Lead to Value Chain Exposures



Espionage

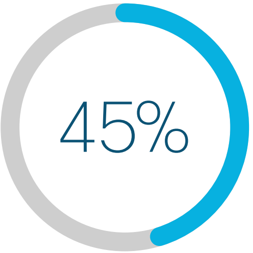
Manipulation

Disruption

Counterfeit

IP Misuse / Information Security Breach

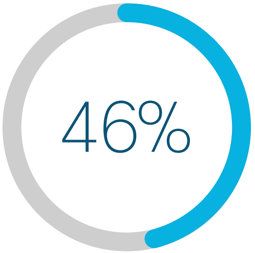
Taint



45%

of organizations have experienced a security incident in the last 12 months due to the use of 3rd-party - compared to 21% in 2021 *

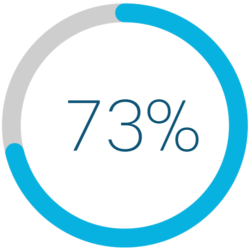
* The 2022 Prevalent 3rd-Party Risk Management Industry Study



46%

say suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process **

** Aviation ISAC Cyber Risk Survey, 2022

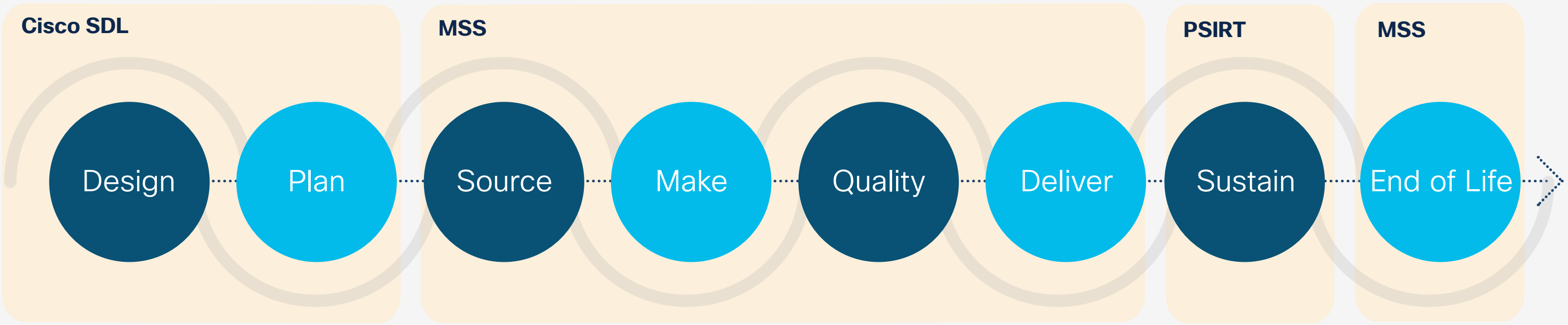


73%

say inefficiencies in 3rd-party risk managment expose their organization to reputational risk ***

*** KPMG 3rd-Party Risk Management Outlook 2022

Security at **every** lifecycle **stage**



Cisco SDL: Design, Plan

MSS: Source, Make, Quality, Deliver

PSIRT: Sustain

MSS: End of Life

Cisco’s Value Chain Security Program

The right **security** in the right **place** at the right **time**

Logical Security

- Secure development lifecycle
- Scrap weight validation
- Role-based access

Trustworthy Technologies

- Encryption
- Smart Chips
- Data-extracting test beds
- Trust Anchor Module

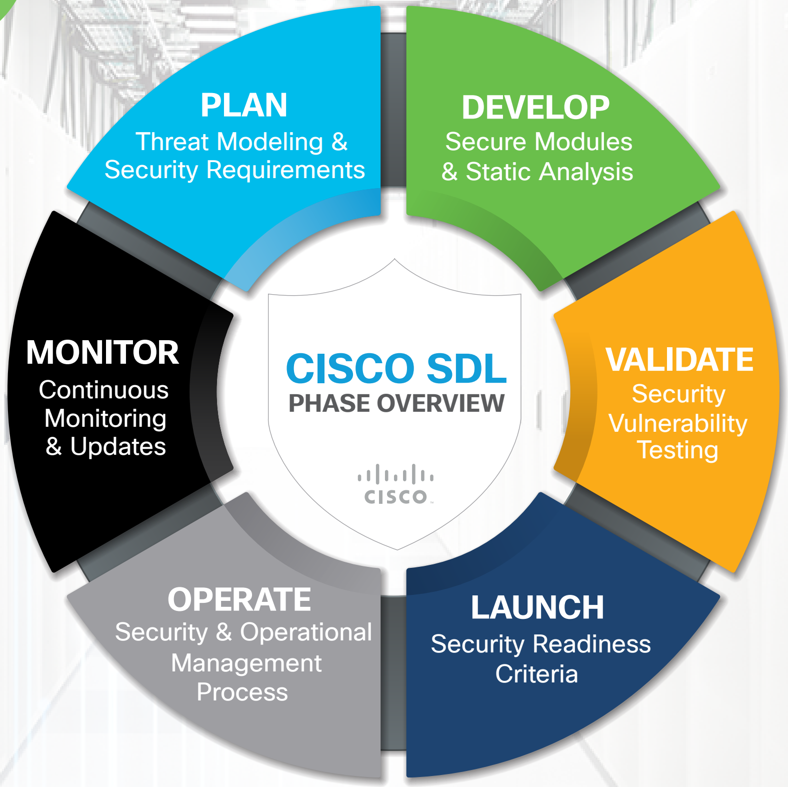
Physical Security Practices

- Camera monitoring
- Security checkpoints
- Electronic or biometric access control

Secure Development Lifecycle

Let’s explore the Cisco SDL core processes:

- **Plan** – security and privacy controls and risk assessment
- **Develop** – secure modules and static analysis
- **Validate** – security vulnerability testing
- **Launch** – security and privacy readiness
- **Operate** – security and operational management
- **Monitor** – continuous monitoring and updating


PLAN
Threat Modeling & Security Requirements
DEVELOP
Secure Modules & Static Analysis
VALIDATE
Security Vulnerability Testing
LAUNCH
Security Readiness Criteria
OPERATE
Security & Operational Management Process
MONITOR
Continuous Monitoring & Updates
CISCO SDL
PHASE OVERVIEW
CISCO

CISCO

Master Security Specification (MSS) Domains

- Security Governance
- Security in Manufacturing and Ops
- Asset Management
- Security Incident Management
- Security Services Management
- Security in Logistics & Storage
- Physical & Environmental Security
- Personnel Security
- Information Protection
- Security Engineering & Architecture
- 3rd Tier Partner Security

200+ Controls

PSIRT Product Security Incident Response Team

Protect the **Customer.**
Protect the **Company.**

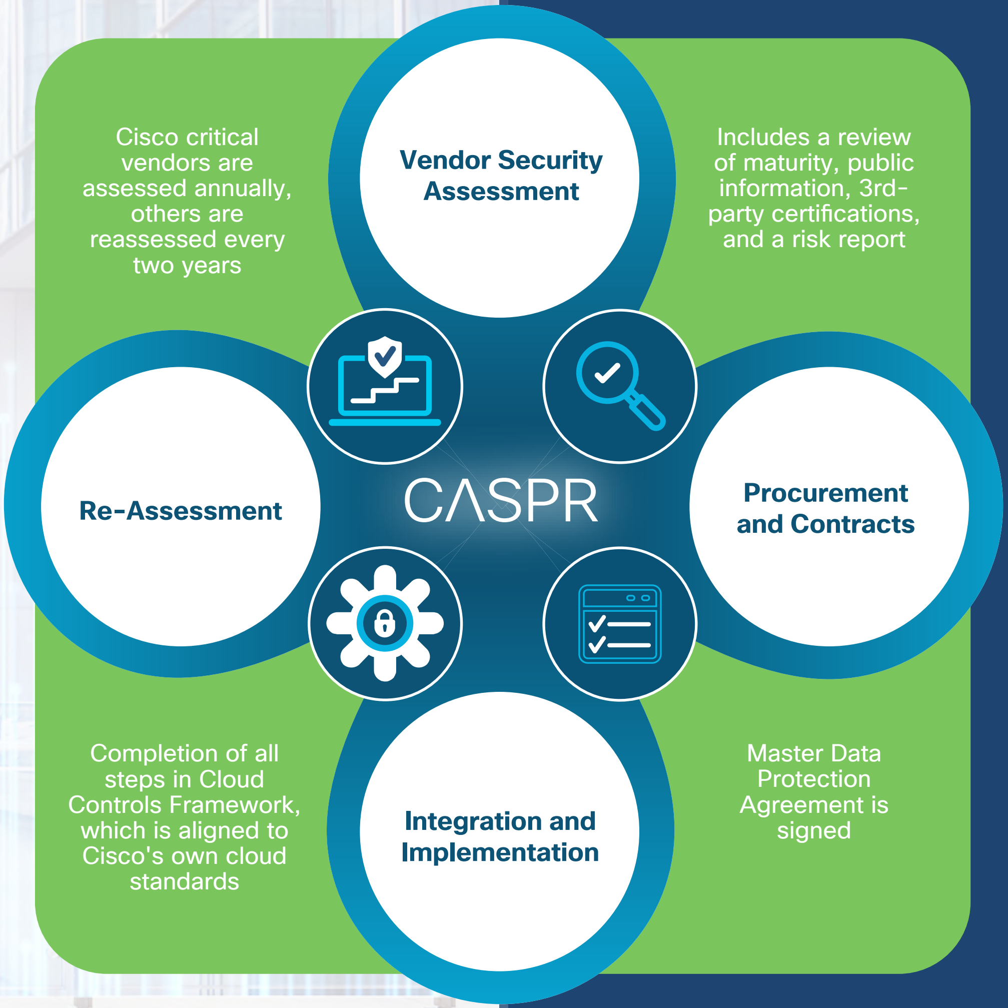
Proactive and Consistent Engagement:
Applies the same mature process across the Cisco portfolio, even as the product line grows

Incident Response With Speed:
Quickly assigns CVE IDs for security vulnerabilities

Vulnerability Management to Industry Standards:
Follows standard rules, policies and scoring systems and is ISO 29147 compliant

CASPR 3rd Party Cloud Security

CASPR is the process in which Cisco assesses the risk posture of ALL third-party processors and vendors (**IaaS**, **PaaS**, **SaaS**) to whom Cisco entrusts its data



CASPR

Vendor Security Assessment

Cisco critical vendors are assessed annually, others are reassessed every two years

Includes a review of maturity, public information, 3rd-party certifications, and a risk report

Procurement and Contracts

Master Data Protection Agreement is signed

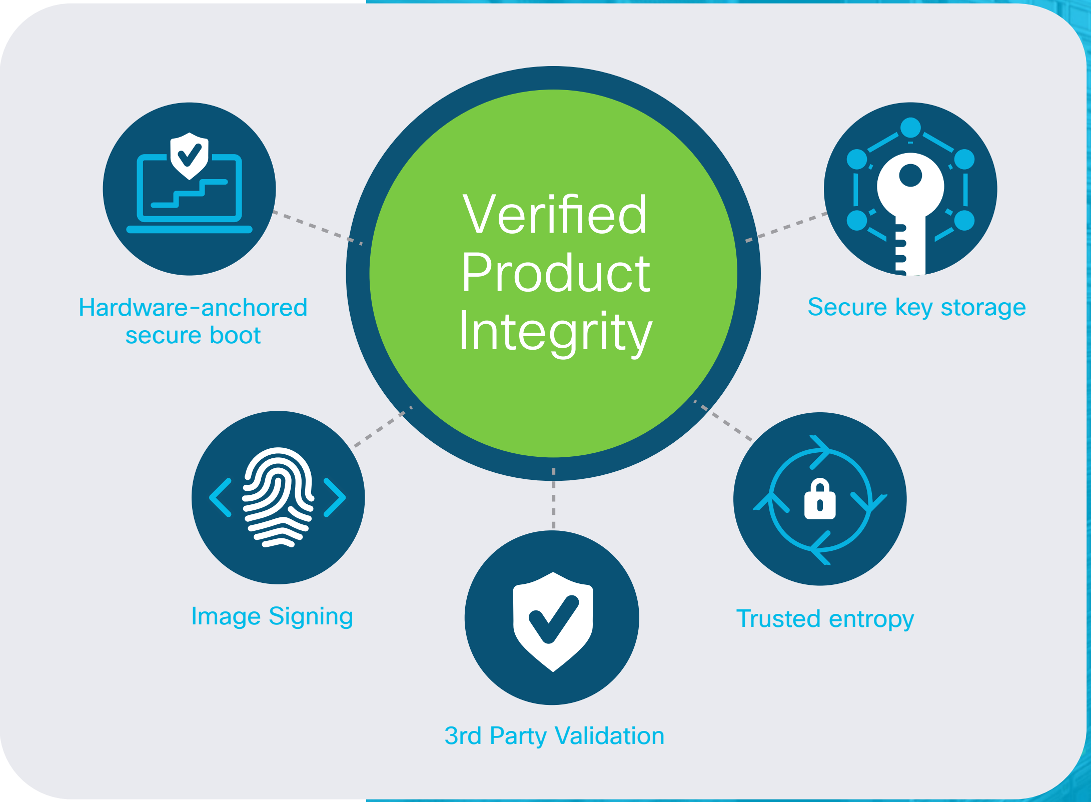
Integration and Implementation

Completion of all steps in Cloud Controls Framework, which is aligned to Cisco's own cloud standards

Re-Assessment

Trustworthy Technologies

Trustworthy solutions encompass Cisco's commitment to deliver products and solutions with multilayered security that protect against today's threats. Trustworthy technologies such as image signing, secure boot, Cisco Trust Anchor module (TAm), and runtime defenses help ensure that the code running on Cisco hardware platforms is authentic, unmodified, and operating as intended.


Verified Product Integrity
Hardware-anchored secure boot
Secure key storage
Image Signing
Trusted entropy
3rd Party Validation