Trustworthy Solutions Glossary of Terms

Feature	Description	Benefits
Cisco Secure Development Lifecycle (SDL)	Cisco Secure Development Lifecycle (SDL) is a repeatable, measureable process designed to reduce vulnerabilities and continually enhance the security and resilience of Cisco solutions.	• Comprehensive and evolving product security requirements • Reduces design vulnerabilities, risk, and cost of ownership • Implements consistent security policy across product lines • Establishes a culture of security awareness
Secure boot	Cisco Secure Boot helps to ensure the code executed on Cisco hardware platforms is authentic and unmodified. Secure boot anchors the microloader in tamper-resistant hardware, establishing a root of trust and preventing Cisco network devices from executing tainted network software.	• Automated check of software integrity at boot-up • Monitors the startup process and can shut down the boot process if it detects a compromise • Helps to ensure that only genuine, unmodified software boots on a Cisco platform
Image signing	Image signing is a two-step process for creating a unique digital signature for a given block of code. First, a hashing algorithm, similar to a checksum, is used to compute a hash value of the block of code. The hash is then encrypted with a Cisco private key, resulting in a digital signature that is attached to and delivered with the image. Signed images may be checked at runtime to verify that the software has not been modified.	Cryptographically signed images: • Help ensure that the firmware, Basic Input Output System (BIOS), and other software are authentic and unmodified • Provide a critical check so only genuine, unmodified software can boot on a Cisco device • Can effectively mitigate persistent attacks

Feature	Description	Benefits
Value chain security	The Cisco Value Chain Security program focuses on counterfeit products, tainted products, and misuse of intellectual property. The program helps to ensure devices delivered with the Cisco name are authentic and unmodified.	▪ Prevents physical tampering ▪ Prevents modified code ▪ Mitigates risk of unknowingly using counterfeit products
Hardware authenticity check	A process that uses the X.509 SUDI certificate installed in the Trust Anchor module to verify that Cisco hardware is authentic (manufactured by Cisco). The hardware authenticity check runs only after the secure boot process has been completed and the software has been verified to be trusted.	▪ Verifies hardware authenticity ▪ Protects against counterfeit
Trustworthy technologies	An evolving range of security technologies designed into Cisco networking devices that protect against counterfeit and software modification, and verify that Cisco products are operating as intended. Trustworthy technologies include the security capabilities in the Trust Anchor module such as Random Number Generation (RNG) and crypto support, secure storage, and Secure Unique Device Identifier (SUDI).	▪ Verifies that hardware is genuine Cisco ▪ Protects against counterfeit and software modification ▪ Supports secure, encrypted communications ▪ Helps to enable device authentication and zero-touch provisioning, reduces deployment costs
Runtime defenses	Runtime defenses target injection attacks of malicious code into running software. Cisco runtime defenses include Address Space Layout Randomization (ASLR), Built-in Object Size Checking (BOSC), and X-space. Runtime defenses are complementary.	▪ Makes it harder or impossible for attackers to exploit vulnerabilities in running software ▪ Runtime defenses are complementary; you can implement these individually or deploy several runtime defenses together
Trust Anchor module (TAm)	This proprietary, tamper-resistant chip is found in many Cisco products and features nonvolatile secure storage, SUDI, and crypto services, including RNG, key store, and crypto engine.	▪ X.509 SUDI certificate installed at manufacturing provides a unique device identity ▪ SUDI helps to enable anti-counterfeit checks, along with authentication and remote provisioning ▪ Secure, on-board storage ▪ RNG/crypto services supports secure communications