Cisco is committed to building trustworthy systems, with embedded security across multiple platforms. The combination of secure processes and technology is part of how we provide a rock-solid network foundation.

** CISCO SECURE DEVELOPMENT LIFECYCLE **

A repeatable and measurable process designed to increase the resiliency and trustworthiness of Cisco products.

- **10** Years of SecCon, the Cisco Security Conference
- **35,000** Employees with Continuous Security Education
- **1000+** Features Per Quarter
- **200+** Specific Security Requirements
- **Whitehat Hacking**
- **Leverages Several Automated Vulnerability Testing Tools**
- **Checks Protocol Robustness**
- **ISO 27034 COMPLIANT**
- **3000 NUMBER OF PRODUCTS REVIEWED SINCE 2006**

GLOBAL GOVERNMENT CERTIFICATIONS

All Cisco customers benefit from rigorous testing and certification requirements.

© 2017 Cisco and/or its affiliates. All rights reserved.
Leveraging Cisco’s 3rd party ecosystem to deliver uncompromised integrity across the solution lifecycle

Addressing Threats & Exposures at Every Stage:
- Espionage
- Counterfeit Products
- Misuse of Intellectual Property

A Layered Security Approach:
- Physical
- Technical
- Logical

TRUSTWORTHY TECHNOLOGIES
Embedded security features that provide an added layer of protection across the network

TRUST ANCHOR
- Authentically hardware & provides
  » Highly secure foundation
  » Immutable identity
  » Secure storage
  » Random number generator
  » Encryption

SECURE BOOT
- Ensures only authentic & unmodified Cisco software boots up on Cisco platforms
- Mitigates advanced persistent threats, physical possession & part replacement attacks

IMAGE SIGNING
- Digitally signed software protects against insertion of counterfeit & tampered software
- Cryptographically signed images ensure software is authentic and unmodified

MODERN CRYPTO
- Up-to-date and secure algorithms with support for international ECC curves
- Research and standards collaboration on Postquantum Crypto and Internet of Things

RUN-TIME DEFENSES
- Protect running devices from attacks that change product software execution
- Built-in operating system protections that increase system resilience