Cisco Trustworthy Solutions

Challenge

Global service provider, enterprise, and government networks today rely on the unimpeded operation of complex computing and communications networks. The integrity of your data and IT infrastructure is foundational to maintaining these networks and user trust. With the evolution to anywhere, anytime access to personal data, users expect the same level of access and security on every network. The threat landscape is also changing, with adversaries becoming more aggressive. Protecting networks from attacks by malevolent actors and from counterfeit and tampered products becomes even more critical. Collaborating with a trustworthy partner who can help mitigate these risks is essential for every organization.

Cisco's Commitment to Trustworthy Solutions

Cisco® trustworthy solutions use industry best practices to help ensure full development lifecycle integrity and end-to-end security. This architected approach incorporates a secure development lifecycle, trustworthy technologies, and supply chain security. Cisco's commitment to security goes beyond securing our supply chain. We work with suppliers as well as with our manufacturing partners and distributors to embed security throughout the full lifecycle of our products. We call that Value Chain Security.

Cisco's Value Chain Security program takes a multi-layered approach to security that uses physical security practices, logical security processes, and security technology to address taint, counterfeit, and misuse of intellectual property. Our comprehensive program continually assesses, monitors, and improves security across the entire lifecycle of our solutions. We consistently strive to enhance security and earn the trust of our customers.

Figure 1. Value Chain Security

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

Hallmarks of Trustworthy Solutions

A trustworthy solution is one that does what it is expected to do in a verifiable way. Building trustworthy solutions requires that security is a primary design consideration. Security must be implemented throughout the entire product lifecycle. This includes using a secure development lifecycle, embedding security into product design, manufacturing, delivering products securely, and ensuring a corporate culture of transparency and continuous innovation. Security and trustworthiness must never be afterthoughts; they must be designed, built, and delivered from the ground up.

- Trustworthy partners strive to assure that a product is designed, developed, manufactured, sold, and serviced as documented.

- Trustworthy partners take steps to secure their manufacturing and distribution supply chains against counterfeiting and tampering, and to prevent the inadvertent installation of unauthorized features such as back doors.

- Trustworthy partners build products with security in mind, from the beginning.

- Trustworthy products incorporate state-of-the-art, built-in security features and functions rather than adding them as overlays to existing hardware and software. Such features include a secure development lifecycle, encrypted internal communications, user and access controls, and policy management controls.

Why Choose Cisco?

Trustworthy solutions exemplify Cisco's commitment to continually enhance the security and resilience of our networking solutions to protect against rapidly-evolving cyberattacks. The scope of Cisco's commitment to the security and resilience of our solutions is unmatched in the industry. The ability to verify the integrity of Cisco platforms with trustworthy technologies such as secure boot of signed images and Trust Anchor module is an example of Cisco security leadership. Cisco uses the security expertise that we've gained defending our own global network infrastructure to enhance the security of our business and our solutions. As the market leader, Cisco is committed to making ongoing investments to address today's cyber landscape, as well as anticipate the threats of tomorrow.

For more information:

Visit the Cisco Trust Center,
trust.cisco.com

- Trustworthy products comply with industry and government security standards relevant to customer business requirements.

- Perhaps most important, trustworthy partners are transparent and accountable. They stand behind their solutions and continually enhance products features, functionality, supply chain integrity, and business practices as threats evolve.

Cisco makes ongoing investments in innovative security technologies to protect our solutions from an evolving range of threats and to provide industry leadership as a trusted networking vendor. Key initiatives include:

- **Cisco Secure Development Lifecycle (SDL):** Part of the Cisco product development methodology, Cisco's Secure Development Lifecycle is a repeatable, measurable process designed to reduce vulnerabilities and continually enhance the security and resilience of our solutions to address today's threats.

- **Cisco Trustworthy Technologies:** Trustworthy technologies are an evolving range of security technologies designed into Cisco solutions. These technologies protect against counterfeit hardware and software modification; help enable secure, encrypted communications; help enable Cisco Network Plug-and-Play; and verify that Cisco products are operating as intended. Key trustworthy technologies include image signing, secure boot, runtime defenses, and security capabilities in the Trust Anchor module such as Random Number Generation (RNG) and crypto support, secure storage, and Secure Unique Device Identifier (SUDI).

- **Certifications:** Cisco is committed to ensuring that our solutions meet international and government standards for information security. Cisco has a team of resources dedicated to the certification process. We work closely with government and standards bodies that define these certifications to increase the value and lower the cost of certifications worldwide.

Figure 2. Cisco Trustworthy Solutions Foundation of Trust

Foundation of Trust

Cisco SDL	Value Chain Security	Secure Boot and Runtime Defenses	Trust Anchor module
Minimizes vulnerabilities; Enhances security	Mitigates supply chain risks	Software authenticity and integrity	Hardware identity, secure storage, crypto services