Trustworthy Systems FAQ

Overview

Q **What are trustworthy systems?**

A A “trustworthy system” is one that does what it is expected to do in a verifiable way. Building trustworthy systems requires that security is a primary design consideration. Security must be implemented holistically across the entire product lifecycle. This includes using a secure development lifecycle, embedding security into product design, manufacturing and 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.

Q **Why is Cisco investing in trustworthy systems?**

A Trustworthy systems are an example of Cisco’s commitment to continually enhance the security and resilience of our networking solutions to protect against rapidly-evolving cyber attacks. Trustworthy systems are Cisco products and solutions developed with multilayered security, ensuring verifiable trust.

Being a trustworthy partner means we earn customer trust by constantly evolving protections across our ecosystem, solutions and company, along with demonstrating an unwavering dedication to trustworthiness, transparency and accountability.

Threat landscape

Q **What kinds of cyber attacks?**

A We’re referring to sophisticated attacks that seek to compromise the integrity and trustworthiness of the network infrastructure by modifying the hardware or software of network devices, which can make to possible for an attacker to obtain privileged information from the network platform. If a network device is directly compromised, it provides a powerful point of command and control of the network infrastructure, potentially resulting in a breach that severely impacts the enterprise.

Q **Does “network devices” mean security products like firewalls?**

A It includes, but goes beyond, traditional security products like firewalls. Because network switches, routers, wireless products, cloud solutions, and other platforms can also be attacked, Cisco is embedding security capabilities across its solutions portfolio.

Why would attackers want to attack the network infrastructure?

A

By controlling switches and routers, sophisticated attackers can:

- Eavesdrop on sensitive communications
- Steal or manipulate data
- Launch attacks against other parts of the network

These threats can go undetected for months or even years and can inflict devastating damage on an organization.

Is there any evidence that attacks targeting the network infrastructure are actually occurring?

A

Yes. SYNful Knock was a 2015 exploit intended to modify Cisco IOS® software. In 2016, the United States Computer Emergency Readiness Team (US-CERT) issued technical advisory TA16-250A, which concluded that:

> "For several years now, vulnerable network devices have been the attack-vector of choice and one of the most effective techniques for sophisticated hackers and advanced threat actors. In this environment, there has never been a greater need to improve network infrastructure security."
>
> See the blog for more information on the evolution of malware targeting network devices.

Securing the network infrastructure

How does Cisco enhance the security and resilience of its products?

A

The Cisco Secure Development Lifecycle (SDL) process enhances product security, reduces design vulnerabilities, and allows for implementation of a consistent security policy across product lines.

Cisco further enhances product security by designing trustworthy technologies into many of our platforms.

Trustworthy technologies

What are some of these trustworthy technologies and how do they protect the network?

A

Key trustworthy technologies include image signing, secure boot, runtime defenses, and the Cisco Trust Anchor module. Trustworthy technologies protect against counterfeit hardware and software modification; help enable secure, encrypted communications; help enable Plug-and-Play (PnP) and Zero-Touch Deployment (ZTD); and provide verification that Cisco network devices are operating as intended. See Table 1.

Are the trustworthy technologies mentioned above available in all Cisco products?

A

No. Cisco product teams design security technologies into their products based on the use case of the device. These capabilities are available in many Cisco routing, switching, wireless, and security products today, and we are designing them into additional platforms. We constantly review and adapt Cisco product security requirements as the threat landscape evolves. Cisco is committed to advanced security research and continues to innovate and develop new trustworthy technologies, which we implement as they become available.

How does Cisco embed these security-focused processes and technologies across its solutions portfolio?

A

Cisco has a dedicated team of engineers and security managers who work with Cisco product development teams to embed security across Cisco product lines.

What are the most trustworthy Cisco platforms?

A

For a list of them, see the Trust Anchor Product Support data sheet.

Does Cisco Secure Boot have to be deployed by an administrator?

A

No, Cisco Secure Boot is active by default and cannot be disabled.

What else does Cisco do to enhance product security?

In addition to embedding security into our products, we make ongoing investments in advanced security research, value chain security, and an industry-leading Product Security Incident Response Team (PSIRT), our vulnerability management and reporting organization.

Does Cisco allow government agencies or third parties to install backdoors in its products?

We categorically prohibit backdoors. We refuse to deliberately weaken our products. And we promote measures that support trustworthiness, transparency, and accountability. To read more on this topic, see the blog from Cisco Chief Security and Trust Officer John Stewart.

Do trustworthy systems differentiate Cisco?

The overall scope of the Cisco commitment to continually enhancing 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's leadership. Cisco uses the security expertise that we've gained defending our own global network infrastructure to continually enhance the security of our business and our solutions.

Where can I learn more about Cisco trustworthy systems?

You can find more resources focusing on our commitment to security and trust at the Trust Center (https://trust.cisco.com).

Table 1 – 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
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 • Effectively mitigate persistent attacks

Table 1 – Glossary of Terms

Feature	Description	Benefits
Secure boot	Cisco Secure Boot helps to ensure the first code executed on Cisco hardware platforms is authentic and unmodified. Secure boot anchors the microloader in immutable 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
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
Trust Anchor module	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

Table 1 – Glossary of Terms

Feature	Description	Benefits
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
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
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