Trustworthy Solutions FAQ

Overview

Q **What are trustworthy solutions?**

A 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 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 solutions?**

A Trustworthy solutions 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 solutions 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) enhances product security, reduces design vulnerabilities, and promotes the implementation of our 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 the Trustworthy Solutions Glossary of Terms, C67-741099-00.

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.

Which Cisco solutions have trustworthy technologies?

A

Trustworthy technologies are designed into many Cisco solutions including enterprise switching, routing, wireless, data center, security, servers, and collaboration. As we launch new solutions and update existing ones, Cisco continues to enhance their security and resilience.

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

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, supply 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 solutions di erentiate Cisco?

Cisco is committed to continually enhancing the security and resilience of our solutions. 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 solutions?

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