Built-in Security Protection from Cyberattacks

Benefit

- Security in Cisco® networking devices helps protect against modern cyberattacks
- Cisco secure development lifecycle and security technologies built into products provide assurance that Cisco hardware and software are genuine and unmodified
- Enhanced platform integrity, security, and resilience provide confidence that the data coming from your Cisco network can be trusted

Security Is Critical in a Hyperconnected World

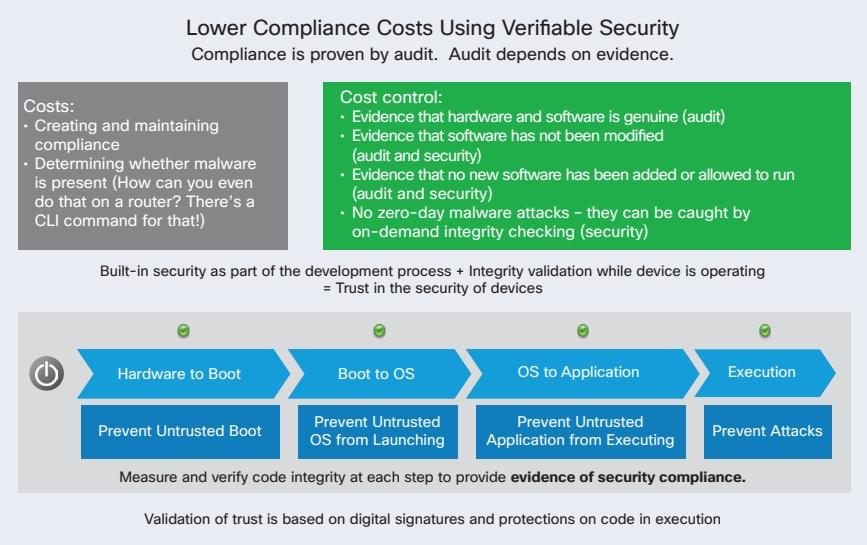
Cyber threats are a top concern for organizations today. Attacks are increasingly frequent, sophisticated, and damaging. Hardly a week passes without the disclosure of another devastating data breach or ransomware attack.

In an increasingly interconnected and digitized world, the security of networks is critical. Secure, resilient networks enable business productivity and growth while protecting critical data and assets.

Disappearance of the Network Perimeter

As attacks have changed, so too has network security. In the past, networks had a well-defined perimeter. If you could protect your data center, your remote offices, and a few endpoints, you could protect your data and your organization. But today, cloud, mobility, and the Internet of Things (IoT) are behind a huge increase in the number of endpoints and the volume of data on the network. This has dramatically increased the attack surface and made the security and trustworthiness of the network increasingly important.

Your data is no longer protected by a well-defined network perimeter. Now it's everywhere–in the cloud, on mobile devices, or within the networks of your customers, suppliers, and partners.



Attacks Against the Network Infrastructure

Attacks have changed dramatically in recent years as the financial motivations for cybercrime continue to grow and the damage to organizations skyrockets. Attacks in the past were often perpetrated by disgruntled hackers. But today's most damaging attacks are the work of highly-motivated organized crime syndicates and nation states that are financially-motivated, technically sophisticated, and intent on stealing anything that can be sold for profit or can be used for competitive advantage.

The types of cyberattacks have also changed dramatically over the last decade. While attacks in the past were focused mainly on disrupting network availability and access, attackers today seek to subvert the normal operation of network devices due to their privileged position in the IT infrastructure. By controlling a switch or router, for example, an attacker can gain a privileged position in the network to exfiltrate data and launch attacks against the rest of the network.

Malware Sophistication

Advanced malware designed to run on a device stealthily in privileged mode while monitoring and exfiltrating information from the operating system is a major concern. Industry experts estimate that, on average, malware often remains undetected for up to six months before being discovered and remediated, leaving organizations vulnerable to theft of IP and other sensitive data, propagation of malware across the network, and worse. Sophisticated malware can also attempt to hide its presence by modifying the command output of network devices that would normally alert the network administrator to the presence of the malware. And malware can even be remotely programmed from a command-and-control (C&C) server. This scenario, in which a system that has been compromised with malware appears to be operating normally, with integrity, but is actually transmitting false and misleading data, is known as the lying endpoint. These types of attacks require organizations to be able to verify the security and resilience of their network infrastructure and the integrity of data coming from the network.

Cisco's Approach to Security and Trust

These technology and business trends are forcing organizations to rethink their approach to security. Rather than relying on perimeter defenses alone, security must be pervasive. It should be built into all elements of the network infrastructure and embedded throughout organizational policies and practices. Organizations need the ability to verify that the devices in their infrastructure can be trusted.

At Cisco, security is our top priority. To protect against today's cyber threats, we take a holistic approach to security that includes building security into every facet of our business. We've committed to ongoing investment, innovation, and industry leadership in the rapidly-evolving security market. In addition to offering industry-leading security products and services, Cisco is building in security and trust across our solutions portfolio. That includes switches, routers, servers, and cloud solutions.

Our approach is much more than just adding security as an afterthought to existing products. It's about embedding security into the DNA of our products during the design phase. The result is that security is a primary design consideration, deeply integrated into the underlying architecture.

This built-in security provides platform integrity, facilitates secure communications, guards against counterfeit products and tampering, gives customers confidence that their Cisco® products are genuine and unmodified, and helps ensure that the data coming from your Cisco infrastructure can be trusted. These features have positive compliance implications for our customers. For example, validation of a digital signature on the Cisco IOS® Software installed on a platform is evidence that an auditor can use to state that the software on that platform is genuine and unmodified. This validation is done when a platform is started up and can be done against the running Cisco IOS copy on customer demand with a simple command-line interface (CLI) command.

Trusted Platform, Trusted Data

The data coming from your network devices provides valuable insights into the flow of data on the network, and it can be used to identify anomalous and suspicious traffic. Network administrators need to have confidence that the data coming from the network is secure, uncorrupted, and trustworthy.

This requires platform integrity and assurance that the network hardware and software are genuine, unmodified, and trustworthy. Cisco is building foundational security into our networking solutions to help ensure that data coming from your Cisco network can be a trusted.

Cisco builds security into our solutions using both secure development practices and by designing security technologies into the architecture of our products. These include the use of a mandatory Secure Development Lifecycle (SDL), safe coding libraries, digitally signed software, Cisco Secure Boot, and run-time defenses like Address Space Layout Randomization (ASLR).

Table 1 provides an overview of the processes and technologies that Cisco uses to enhance the security, resilience, and integrity of our solutions. These processes and technologies help ensure that Cisco hardware and software are genuine and unmodified. Administrators should ensure their hardware and software support these features to ensure that the integrity of the device is fully protected and the data coming from devices can be trusted.

Table 1. Security Processes and Technologies for Cisco Hardware and Software

Security Feature	Protections Provided & Customer Benefits
Cisco Secure Development Lifecycle (SDL)	Cisco Secure Development Lifecycle (SDL) is a mandatory process designed to mitigate the risk of vulnerabilities and increase product security and resiliency.
Digitally signed software images (image signing)	Cryptographically signed images help ensure that the firmware, BIOS, and other software are authentic and unmodified.
Cisco Secure Boot and hardware trust anchors	Cisco Secure Boot can ensure that the first code executed on Cisco hardware platforms is authentic and unmodified, establishing a root of trust and preventing your network devices from executing tainted network software.
Value chain security	Cisco's Value Chain Security program focuses on counterfeit products, tainted products, and misuse of intellectual property. Our Value Chain Security program helps ensures that devices delivered with the Cisco Systems name are authentic and unmodified.

Security Feature	Protections Provided & Customer Benefits
Run-time defenses	Run-time defenses such as Address Space Layout Randomization (ASLR) and Executable Space Protection (X-Space) increase system resilience by randomizing software, making it more difficult for an attacker to exploit vulnerabilities.
Cisco IOS run-time memory integrity verification	Network administrators can also verify the integrity of the run-time memory of Cisco IOS Software. Verifying its integrity is particularly relevant in detecting in-memory tampering.

Next Steps

Cisco is committed to ongoing innovation and leadership to address a rapidly-evolving cybersecurity threat landscape. As new products are developed and existing products are updated, Cisco will continue to embed built-in security into additional platforms.

As you refresh your network infrastructure to reduce vulnerabilities, improve resiliency, and position your organization to benefit from digitization, ask your Cisco account manager or partner about Cisco's holistic approach to security and the security built into many of our platforms. And explore the products and services Cisco offers to help you analyze your infrastructure, understand cyber risk, identify and mitigate vulnerabilities, and ensure that your network is built on a foundation of secure, resilient, and trustworthy products.

For More Information

For more information about the Cisco platforms available today with built-in security, see the Trust Anchor Technologies Implementation Report.

Visit the Cisco Trust and Transparency Center for more information.

Download a copy of "Trustworthy IT Business Partners for Dummies"

C45-737110-01 07/16