# Managing Risk to Your Network Infrastructure: A Matter of Trust

## Cisco trustworthy systems help ensure a signed, sealed, and verifiable network infrastructure

Cyber attacks targeting the network infrastructure have become increasingly sophisticated and damaging. Today's evolving threat landscape requires business leaders to approach security differently. In addition to deploying multilayered security solutions that provide defense in-depth, organizations must ensure security effectiveness and exercise ongoing security diligence. This requires organizations to evaluate their network security, identify its gaps, and proactively harden vulnerable systems. Organizations also need to update aging infrastructure to secure the network, protect data, and meet rising expectations of customers, shareholders, and regulators.

CISOs must not only deliver effective security that stops attackers at the network perimeter, they must also prevent attackers from subverting the switches, routers, and other network devices at the heart of the communications infrastructure. Why? Because by attacking and modifying the network infrastructure, sophisticated attackers can eavesdrop on sensitive communications, steal or manipulate data, and launch attacks against other parts of the network. If successful, these attacks can go undetected for days, weeks, or even months, and can inflict devastating damage on your organization.

# Contents



## But in today's threat environment, how can you know whether the network infrastructure is secure and resilient?

A secure, resilient network foundation starts with a trustworthy IT partner. This means designing and delivering trustworthy products, solutions, and services, as well as ensuring the security and resilience of your business operations. A security mindset and holistic approach to security throughout your operations is essential, as is consistently demonstrating your commitment to deliver the highest quality products and services to your customers.

## Security across the business

At Cisco, security is our top priority and we are committed to delivering trustworthy systems. 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.

Trustworthy systems refers to Cisco's commitment to develop solutions with multiple layers of security and to embed security across the full product lifecycle including design, sourcing, manufacturing, delivery, product support, and end-of-life. Trustworthy systems highlight Cisco's commitment to continually enhance the security and resilience of our solutions to protect against today's rapidly-evolving cyber threats. The breadth of this commitment provides multilayered protection from attacks that seek to compromise the integrity and trustworthiness of the network infrastructure.

This means Cisco embeds security into products and solutions across our networking portfolio. We have built that security into the design of switches, routers, wireless, and cloud solutions, as well as firewalls and other Cisco platforms. These added layers of protection reduce vulnerabilities and enhance product security. Trustworthy technologies run automated checks of hardware and software to verify that Cisco networking devices are genuine, unmodified, and operating as intended. By embedding security in core network devices, we make security more pervasive throughout the network so you can identify and remediate threats more quickly.

## A strong foundation

Below are the foundational elements of trustworthy systems at Cisco. We start with a mandatory secure development process that enhances product security and embeds it across our portfolio. We have built the Cisco Secure Development Lifecycle (SDL) on a foundation of security-focused polices and processes, such as:

- A comprehensive and evolving set of product security requirements
- Policies to help ensure the security of third-party software
- Secure design techniques, including threat modeling
- Secure coding practices, including the use of safe libraries
- Secure analysis to check for vulnerabilities and verify security effectiveness
- Vulnerability testing that verifies comprehensiveness of design by simulating common attacks

We further enhance the security of our products by embedding trustworthy technologies into many Cisco platforms. These technologies provide both boot and runtime protections, including:

- Image signing
- Secure boot
- Runtime defenses
- Device identity, crypto support, secure storage, and other capabilities in the Cisco Trust Anchor module

These added layers of security protect against counterfeit and software modification, help enable secure, encrypted communications, and allow network operators to verify the authenticity and integrity of Cisco network devices.

Trustworthy systems give CISOs a valuable tool for verifying the trustworthiness of the network, managing risk, demonstrating security diligence, and protecting the organization.

## The risks of aging infrastructure

But what about legacy systems? Along with helping to ensure that new infrastructures are secure and trustworthy, CISOs and CIOs need to address the risks of aging infrastructure proactively. Aging infrastructure is a widespread and growing risk exposing organizations to unnecessary and unacceptable risk. Ignoring an older, vulnerable infrastructure and hoping that your network won't get breached is not a strategy and doesn't meet the expectations of the board, shareholders, and regulators. Recent cyber attacks highlight one simple truth: If you choose to ignore an aging infrastructure, you do so at your own risk. Unpatched and older systems may not be capable of protecting against today's threats.

## The road ahead

There are a number of steps you can take to reduce risk and enhance the security and resilience of your network infrastructure. Fostering a security-aware culture across your entire organization is critical in shrinking the attack surface. All team members must understand their roles in reducing cyber risk and protecting the organization; security is everyone's responsibility, regardless of each person's role.

It's also essential to perform regular audits of existing systems to identify and mitigate vulnerabilities. You have to prioritize any new security risks discovered and put a mitigation plan in place. Follow basic security hygiene, like hardening systems and applying software patches in a timely manner. Replace any gray market, counterfeit, or end-of-support and end-of-life gear in the network with current-generation equipment as soon as possible to reduce risk and protect your organization, your customers, and your partners.

Don't put your business at risk by digitizing on an aging, fragile infrastructure. Look to Cisco as your trusted security partner. We offer an industry-leading portfolio of threat-centric security solutions and threat intelligence, plus security embedded throughout the network to reduce risk and help protect against today's threats. That's security. That's Cisco.

## Resources

Learn how Cisco Security Advisory Services can help you assess the risk profile of your organization.

Learn more about Cisco trustworthy systems.


C11-740047-00 01/18