Profile of A Trusted Partner

Customers should insist on explicit trust. Only by being trustworthy, transparent, and accountable can a vendor earn the right to be considered a TRUSTED PARTNER. A trusted partner weaves security into the very fabric of their business – securing their data, processes, products, services, and employees to deliver true pervasive security.

Trustworthy
- Manage, secure and protect customers data
- Follow a Secure Development Lifecycle (SDL)
- Meet global certification standards
- Secure the supply chain
- Work with third parties and open source communities to improve security
- Require ongoing employee security education

Transparent
- Provide equal and simultaneous access to security vulnerability information
- Clearly map the flows and explain the usage of customer data
- Publish all government requests for customer data
- Deliver timely and actionable breach notifications
- Enable customers to verify code and development artifacts in a dedicated, secure environment

Accountable
- 24/7 security incident response team
- Ethical and predictable response to security incidents
- Quick detection and remediation of product vulnerabilities
- Admit when mistakes are made and work to make things right
- Timely, actionable and simultaneous notification of bug fixes and security patches

Are you working with a trusted partner?
trust.cisco.com
What is Trust?

What does it take for a product to be trustworthy?

A **trustworthy system** is one that does what it is expected to do in a verifiable way. When making a buying decision, consider the building blocks of trustworthy systems:

### Secure Development Lifecycle

Security should be considered from the product design phase, not as an afterthought. A repeatable, measurable combination of tools, processes, and awareness training should be introduced in all development lifecycle phases and mandated to ensure defense-in-depth, provide a holistic approach to product resiliency, and establish a culture of security awareness.

### Verifiable Product Integrity

**Hardware-anchored secure boot**

At boot-up, a trusted product performs an automated check of software integrity that is anchored in hardware, ensuring that only genuine, unmodified software boots on that platform.

**Secure key storage**

Trustworthy products provide secure key storage that is anchored in hardware, allowing customers to store sensitive data encrypted in non-volatile memory.

**Image signing**

A product that is trustworthy utilizes digitally-signed software that ensures that it came from a trusted source.

**Trusted entropy**

A trusted product generates certifiable entropy for random number generation.

### Secures the Supply Chain at Every Stage

Vendors who produce trusted products implement a program that continually assesses, monitors, and improves the security of the supply chain throughout their entire lifecycle.

### Transparent and Proactive Incident Response

Trusted products are continually monitored by a dedicated, global team that manages the receipt, investigation, and public reporting of information about product security vulnerabilities. This team should provide equal and simultaneous access to security vulnerability information.

### Continuous Innovation

The engineering roadmap of trustworthy products is informed by the expertise the vendor has gained from defending their global enterprise. Product security standards are continually reviewed in order to address constantly evolving cyber threats.

### 3rd Party Validation

Products that are trustworthy meet rigorous global certifications and standards requirements.

---

Does Cisco produce secure products? You decide.

[trust.cisco.com](trust.cisco.com)