Cisco Trustworthy Systems

Challenge

Global service provider, enterprise, and government networks today rely on the unimpeded operation of complex computing and communications networks. The integrity of your data and IT infrastructure is foundational to maintaining these networks and user trust. With the evolution to anywhere, anytime access to personal data, users expect the same level of access and security on every network. The threat landscape is also changing, with adversaries becoming more aggressive. Protecting networks from attacks by malevolent actors and from counterfeit and tampered products becomes even more critical. Collaborating with a trustworthy vendor who can help mitigate these actions is essential for every organization.

Hallmarks of Trustworthy Systems

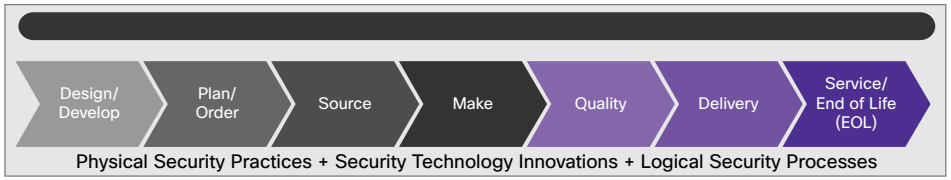
- Trustworthy vendors strive to assure that a product is designed, developed, manufactured, sold, and serviced as documented.
- Trustworthy vendors take steps to secure their manufacturing and distribution supply chains against counterfeiting and tampering, and to prevent the installation of unauthorized features such as "back doors."
- Trustworthy products incorporate state-of-the-art, built-in security features and functions rather than adding them on as overlays to "ethically neutral" hardware and software. Such features include a secure development lifecycle, encrypted internal communications, use and access controls, and policy management controls.
- Trustworthy products comply with industry and government security standards relevant to customer business requirements.
- Perhaps most important, trustworthy vendors are transparent about their policies, processes, and technologies they use across their product lines. They stand behind trustworthy products and systems and are always ready to enhance features, functionality, supply chain integrity, and business practices as both the products and threat models evolve.

How Cisco Addresses Trustworthy Systems

Cisco® trustworthy systems use industry best practices to help ensure full development lifecycle integrity and end-to-end security. This architected approach incorporates supply chain security and Cisco trustworthy systems technology.

Cisco manages the entire supply chain by deploying a set of interlocking practices, procedures, technologies, and implementation checkpoints to embed physical and logical security at each step of the supply chain. Three foundational elements are employed: security technology innovation, physical security practices, and logical security processes. This lifecycle management approach (Figure 1) strives to make sure that Cisco products resist the malicious modification of technology, products, and security measures, even when the supply chain is disrupted or intellectual property is misused.

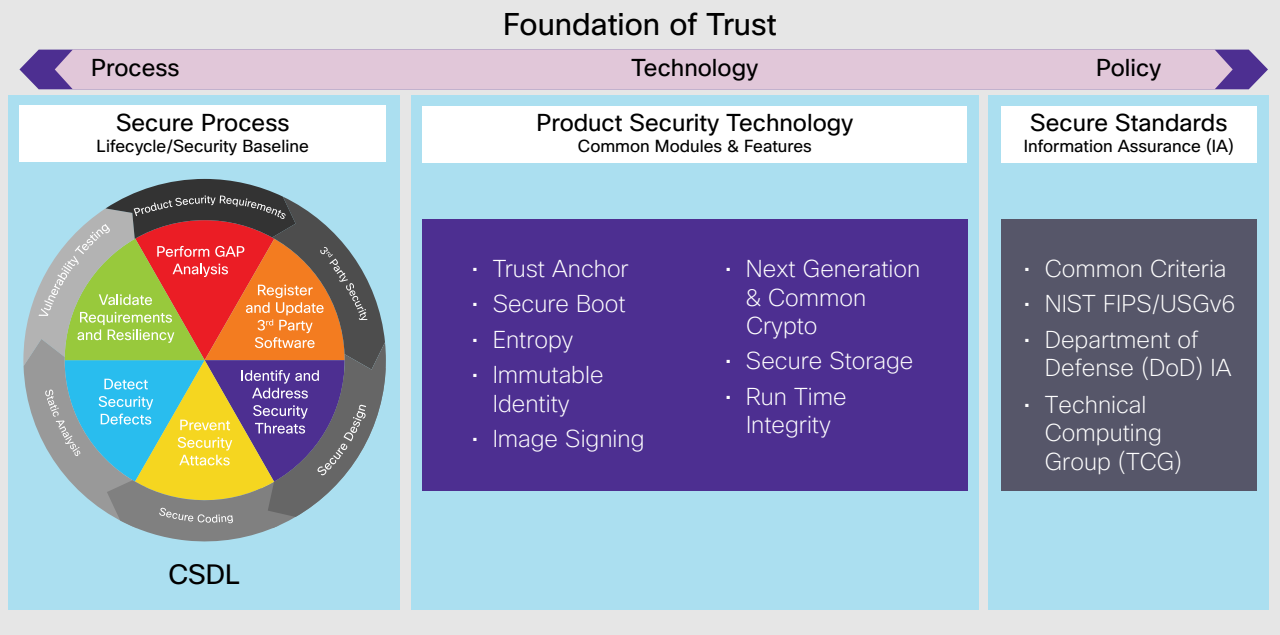
Figure 1. Supply Chain Lifecycle



Cisco trustworthy system initiatives generate innovative security technologies to help ensure that Cisco continues to be recognized as a trusted networking vendor. Our three primary initiatives (Figure 2) include:

- **Cisco secure development lifecycle:** Part of the Cisco product development methodology, the secure development lifecycle provides a repeatable and measurable process designed to mitigate the risk of vulnerabilities and increase product resiliency.
- **Cisco product security technologies:** These technologies work together to provide product assurance and protect customer networks. Cisco trust anchor technology can enable the authentication of hardware and software and acts as a "hardware anchor" for highly secure storage and identity. Next-generation encryption capabilities simultaneously satisfy security requirements while using scalable cryptographic algorithms.
- **Certifications:** Cisco has dedicated resources throughout the certification process. We work closely with government and standards bodies that define and rely on these certifications to increase the value and lower the cost of certifications worldwide.

Figure 2. Cisco Trustworthy Systems Technologies



Why Choose Cisco

The network forms the foundation of your defense against the threat landscape. Trustworthy systems establish the base of assurance for an architected secured network, and this trust must be earned on a continuous basis. Cisco offers continued innovation to enhance resiliency in a network. We provide visibility and transparency while partnering with our customers to prepare for any and all threats. With best-in-class, highly secure development practices and end-to-end security lifecycle, Cisco is committed to implementing state-of-the-art technologies in our products to allow for comprehensive customer assurance.