



Cisco Security—At-A-Glance

Cisco Security Technologies

Cisco offers the industry's most comprehensive, integrated systems approach to security, with the broadest portfolio of [hardware, software, enterprise management and service provider management platforms](#). The company considers network security a baseline architecture for all its technologies, from infrastructure, such as switching and routing, to advanced technologies, such as wireless and IP telephony.

Cisco's security solutions allow organizations to protect productivity gains, reduce overall operating costs and enable mission critical deployment of new and existing technologies.

Cisco Featured Security Partnerships

Network Admission Control (NAC) is a Cisco Systems sponsored industry initiative that uses the network infrastructure to enforce security policy compliance on all devices seeking to access network computing resources, thereby limiting damage from viruses and worms.

Using NAC, organizations can provide network access to endpoint devices such as PCs, PDAs, and servers that are verified to be fully compliant with established security policy. NAC can also identify noncompliant devices and deny them access, place them in a quarantined area, or give them restricted access to computing resources. NAC offers the following benefits:

- Comprehensive span of control
- Extension of existing technologies and standards
- Extension of existing network and antivirus investments

NAC is a multivendor collaboration between leading security providers. Current partners include Computer Associates, IBM, Kingsoft Co. Ltd., McAfee, Rising Tech Co., Symantec, New Boundary Technologies®, and Trend Micro. In addition, NAC works in collaboration with Microsoft's Network Access Protection (NAP) security architectures. More information can be found at: www.cisco.com/go/nac

Cisco Featured Security Acquisitions

Since 1993, Cisco has expanded its security portfolio by purchasing a number of companies, including:

Protego Networks, Inc.: Provides traditional security information management (SIM) functions, including security event / log capture, consolidation, centralization, correlation, prioritization, visualization, investigation, escalation, and compliance reporting. *12/2004*

Perfigo, Inc.: Leading developer of access control solutions that provide endpoint policy analysis, compliance, and access enforcement capabilities. *10/2004*

Twingo Systems, Inc.: Leading provider of desktop security solutions for Secure Socket Layer (SSL) Virtual Private Networks (VPNs). *03/2004*

Riverhead Networks, Inc.: Leading developer of security technology that protects against Distributed Denial of Service ("DDoS") attacks and other security threats in enterprise and service provider networks. Riverhead delivers an innovative solution that protects online operations from sophisticated attacks by detecting and blocking malicious traffic without impacting legitimate business transactions. *03/2004*

Okena, Inc.: Developer of software providing threat protection for desktop and server computing systems. *06/2003*

Psionic Software, Inc.: Developer of network security software that increases the efficiency of intrusion detection systems (IDS) by reducing false alarms by up to 95 percent. *10/2002*

Allegro Systems: Leading developer of Virtual Private Network (VPN) acceleration technologies designed to enhance the performance and functionality of secure networking platforms. *07/2001*

Altiga Networks: Market leader in integrated VPN solutions for remote access applications. *01/2000*

Compatible Systems Corp.: Leading developer of standards-based, reliable and scalable VPN solutions for service provider networks. *01/2000*

WheelGroup Corporation: A leader in intrusion detection and security scanning software products. *02/1998*

Global Internet Software Group: A pioneer in the Windows NT network security marketplace. *06/1997*

TGV Software, Inc.: Leading supplier of Internet software products for connecting disparate computer systems over local area, enterprise-wide and global computing networks. *01/1996*

Network Translation, Inc. (NTI): Networking manufacturer of cost-effective, low maintenance network address translation and Internet firewall hardware and software. *10/1995*

Cisco Featured Security Solutions

Cisco's Self Defending Network is Cisco's vision for an integrated network. Organizations can use their existing investments in routing, switching, wireless, and security platforms to deploy a Self-Defending Network that will help them identify, prevent, and adapt to both known and unknown security threats.

Adaptive Threat Defense (ADT) Further minimizes security risks by dynamically addressing threats at multiple layers, enabling tighter control of network traffic, endpoints, users, and applications. ADT also simplifies architectural designs and lowers operational costs. This innovative approach combines secure, multilayer intelligence, application protection, network-wide control and threat containment within high-performance solutions. ADT is a critical advancement in the Cisco Self-Defending Network security strategy that helps customers fortify their business systems.

Anti-X Defenses Prevent and respond to network threats through a combination of innovative traffic and content-oriented security services. Core security enforcement technologies include firewall, Intrusion Prevention System (IPS), anomaly detection and Distributed Denial of Service (DDoS) mitigation fused with application-inspection services such as network anti-virus, anti-spyware, and URL filtering. This convergence brings granular traffic inspection services to key network security enforcement points, thereby containing malicious traffic before it can be propagated across the network.

Application Security Solutions Provides advanced business application protection through the use of application-level access controls, application inspection, and enforcement of appropriate application-use policies, web-application control, and transaction privacy.

Network Control and Containment Network intelligence and the virtualization of security technologies provides the ability to layer sophisticated auditing and correlation capabilities to control and help protect any networked element or service such as Voice over IP (VoIP) with active management and mitigation capabilities.

The **SAFE Blueprint** provides a "defense-in-depth" approach to strong data privacy for organizations of all sizes by recommending ways to implement scalable, cost-effective, best-in-breed network security solutions. It recommends specific technologies and products to address key security threats across network topologies and components.