Cisco **SecureX**
Product Brochure

Security Matters More Than Ever

Traditional approaches to network security were designed for a single purpose: to protect resources inside the network from threats and malware coming from outside the network.

Today's businesses must consider smartphones, tablets, and consumerization of IT, combined with telecommuters, contractors, partners, and business-critical services hosted in the cloud. Security is more important than ever—and far more complex.

Businesses still need to defend themselves against network threats, protect valuable data and resources, and implement the necessary controls for regulatory compliance, but the line between inside and outside is not as clear. The opportunities for better and richer collaboration for anyone, anywhere, with any device are matched by the challenges presented to the IT and security professionals who are tasked with delivering secure, reliable, and seamless voice, video, and data.

Cisco SecureX Architecture

The Cisco SecureX Architecture™ is a next-generation security framework that brings together flexible solutions, products, and services to address and enforce consistent business policy throughout the distributed network. The Cisco SecureX Architecture blends global threat intelligence and contextual awareness to address unique security challenges—such as the increase in highly mobile users, the wide variety of network-enabled mobile devices, or the move to cloud-based infrastructures and services—by protecting information, applications, devices and users.

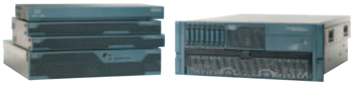
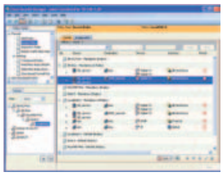
The Cisco SecureX Architecture protects today's borderless networks by providing effective security for any user, using any device, from any location, and at any time. This new security architecture uses a higher-level policy language that understands the full context of a situation—the who, what, where, when and how. With highly distributed security policy enforcement, security is pushed closer to where the end user is working, anywhere on the planet.

Explore the following Cisco® security solutions that are part of the Cisco SecureX Architecture.

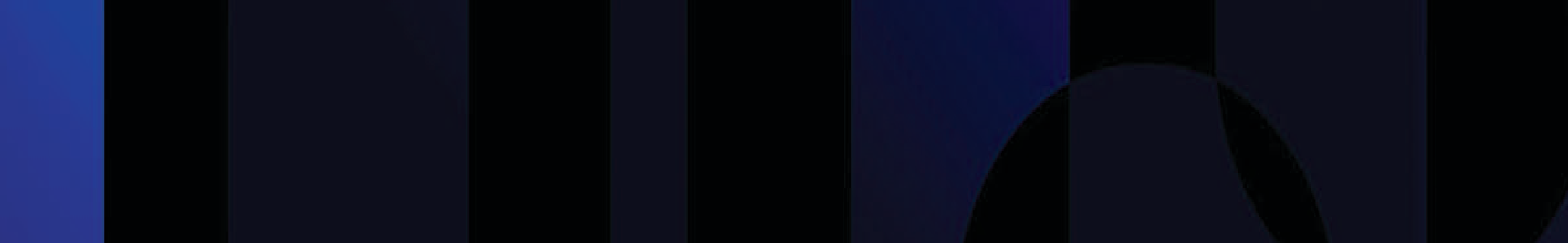
Continued on next page

Secure Network

Cisco secure network and branch detect and block attacks and exploits, preventing intruder access. With firewall and intrusion prevention in standalone and integrated deployment options, customers can better thwart attacks and meet compliance requirements, such as the Payment Card Industry Data Security Standard (PCI DSS).

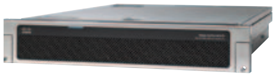
			
Cisco ASA 5500 Series Adaptive Security Appliance	Cisco Intrusion Prevention System	Cisco Integrated Services Router Generation 2	Cisco Security Manager
· Combines industry-leading firewall, VPN, and intrusion prevention in a unified platform · Provides comprehensive real-time threat protection and highly secure communications services to stop attacks before they affect business continuity · Reduces deployment and operational costs while delivering comprehensive security for networks of all sizes · Versatile, always-on remote access integrated with IPS and web security for highly secure mobility and enhanced productivity	· Identifies, classifies, and stops malicious traffic, including worms, spyware, adware, viruses, and application abuse · Delivers high-performance, intelligent threat detection and protection over a range of deployment options · Uses global threat correlation with reputation filtering to prevent threats with confidence · Provides peace of mind with guarantees for coverage, response time, and effectiveness for Microsoft, Cisco, and critical enterprise application vulnerabilities[1] · Promotes business continuity and helps businesses meet compliance needs	· Delivers suite of built-in capabilities, including firewall, intrusion prevention, VPN, and cloud-based web security · Promotes the integration of new network security features on existing routers · Provides additional protection without adding hardware and maximizes network security · Decreases ongoing support and manageability costs by reducing the total number of devices required	· Provides a comprehensive management solution for Cisco network and security devices · Enables consistent policy enforcement, quick troubleshooting of security events, and summarized reports across the deployment · Supports role-based access control and an approval framework for proposing and integrating changes · Integrates powerful capabilities, including policy, object, and event management; reporting; and troubleshooting

[1] Guaranteed coverage applies to the availability of signatures for eligible Cisco, Microsoft, and critical enterprise application vulnerabilities. Full service-level agreement details, including eligibility, remedies, terms, and conditions will be available from Cisco at release time, currently scheduled for the first half of 2011. For more information, please contact your Cisco reseller.



Secure Email and Web

Cisco secure email and web solutions reduce costly downtime associated with email-based spam, viruses, and web threats, and are available in a variety of form factors, including on-premise appliances, cloud services, and hybrid security deployments with centralized management.

		
Cisco IronPort Email Security–Cloud, Hybrid, and On-Premises	Cisco Web Security–Cloud and On Premises	IronPort Security Management Appliance
· Provides a multi-layered approach to fighting spam, viruses, and blended threats to protect organizations of all sizes · Provides fully integrated outbound control through data loss prevention and encryption · Reduces downtime, simplifies administration of corporate mail systems, and eases the technical support burden · Offers comprehensive reporting and message tracking for administrative flexibility · Provides flexible solutions to grow with your organization's needs	· Provides most effective defense against web-based malware: Cisco SIO, combining best-in-class web reputation and content analysis intelligence · Delivers rich, flexible policy controls that are effective for Web 2.0 sites with dynamic content and embedded applications · Provides rich reporting capabilities for flexible, unsurpassed visibility into web usage · Offers choice of deployment options with industry leading ScanSafe and IronPort Web Security technology	· Simplifies security management across Cisco IronPort email and web security products · Delivers centralized reporting, message tracking, and spam quarantine for email security appliances · Provides centralized web policy management for web security appliances · Allows for delegated administration of web access policies and custom URL categories

A Proactive Approach to Threats

Cisco's security products stay ahead of the latest threats using real-time threat intelligence from Cisco Security Intelligence Operations (SIO). Cisco SIO is the world's largest cloud-based security ecosystem, using almost a million live data feeds from deployed Cisco email, web, firewall, and intrusion prevention system (IPS) solutions.

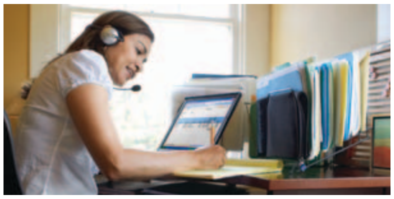
Cisco SIO weighs and processes the data, automatically categorizing threats and creating rules using more than 200 parameters. Security researchers also collect and supply information about security events that have the potential for widespread impact on networks, applications, and devices.

Rules are dynamically delivered to deploy Cisco security devices every three to five minutes. The Cisco SIO team also publishes security best practice recommendations and tactical guidance for thwarting threats.

For more information, visit www.cisco.com/go/sio.

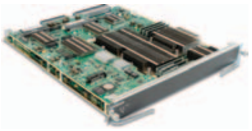
Secure Mobility

Cisco secure mobility solutions promote highly secure mobile connectivity with VPN, wireless security, and remote workforce security solutions that extend network access safely and easily to a wide range of users and devices. Cisco Secure Mobility solutions offer the most comprehensive and versatile connectivity options, endpoints, and platforms to meet your organization's changing and diverse mobility needs.

		
Cisco AnyConnect Secure Mobility Client	Cisco Adaptive Wireless IPS Software	Cisco Virtual Office
· Provides highly secure remote connectivity between the corporate network and a wide range of managed and unmanaged mobile devices · Enables users to securely access the network with their device of choice, regardless of their physical location · Can be used in conjunction with ASA security appliances, as well as ISRs and ASRs, for a comprehensive, highly secure connectivity solution · Integrates with existing networks to enable highly secure mobility in a wide range of environments	· Provides automated wireless vulnerability and performance monitoring to deliver visibility and control across the network · Maintains a constant awareness of the RF environment to meet the demands of the largest networks · Automatically monitors for wireless network anomalies and to identify unauthorized access and RF attacks · Collaborates with Cisco network security products to create a layered approach to wireless security	· Extends highly secure, rich, and manageable network services to employees working outside the traditional work environment · Cost-effectively scales to deployment requirements · Includes remote site and headend systems, remote site aggregation, and services from Cisco and approved partners · Delivers an office-caliber experience to staff wherever they're located with full IP phone, wireless, data, and video services

Secure Data Center

Cisco secure data center solutions protect high-value data center resources and servers with high-performance threat protection, secure segmentation, and policy control.

		
Cisco ASA 5585-X Adaptive Security Appliance	Cisco Catalyst 6500 ASA Services Module	Cisco Virtual Security Gateway (VSG)
· Combines a proven firewall with comprehensive IPS and high-performance VPN – Delivers 8 times the performance density of competitive firewalls by supporting the highest VPN session counts, twice as many connections per second, and 4 times the connection capacity of competitive firewalls—all in a compact 2RU footprint – Integrates IPS with Global Correlation for a solution that is twice as effective as legacy IPS and includes Cisco guaranteed coverage · Supports context-aware firewall capabilities for deeper insight, more effective security, and improved operational efficiency	· Delivers an integrated security solution that combines full-featured switching with best-in-class security · Places security directly into the data center backbone by integrating with Cisco Catalyst 6500 Series Switches · Provides up to 16 Gbps multiprotocol throughput, 300,000 connections per second, and 10 million concurrent sessions · Supports up to four modules in a single chassis, for up to 64 Gbps throughput per chassis	• Integrates with Cisco Nexus 1000V virtual switch and hypervisors • Delivers security policy enforcement and visibility at a virtual machine level • Logically isolates applications in virtual data centers and multi-tenant environments • Enforces separation of duties between security and server administrators

Secure Access

Cisco TrustSec® provides secure access to your networks and network resources through policy-based access control, identity-aware networking, and data integrity and confidentiality services. Cisco TrustSec allows you to improve compliance, strengthen security, and increase operational efficiency. It is available as an appliance-based overlay solution or as an integrated 802.1X infrastructure-based service that extends access enforcement throughout the network.

Cisco Identity Services Engine	Cisco Secure Access Control System
· Gathers information from users, devices, infrastructure, and network services to enforce consistent contextual-based business policies across the network · Provides visibility into who and what is on the network for advanced discovery and troubleshooting · Enforces security policy on all devices that attempt to gain access to the network · Combines authentication, authorization, and accounting (AAA), posture, profiling, and guest management	· Controls network access based on dynamic conditions and attributes through an easy-to-use management interface · Meets evolving access requirements with rule-based policies for flexibility and manageability · Simplifies management and increases compliance with integrated monitoring, reporting, and troubleshooting capabilities · Adopts an access policy that takes advantage of built-in integration capabilities and distributed deployment

What Are the Benefits of the Cisco SecureX Architecture?

Cisco SecureX:

- Addresses any organization's needs with the industry's richest and most innovative security profile
- Dynamically discovers and protects against next generation of threats with unique context aware threat protection and security intelligence
- Secures the borderless experience with consistent policy enforcement throughout an organization
- Increases productivity by extending the same services and capabilities that workers in the office enjoy to remote office, telecommuter, and mobile workers
- Enables the adoption of new business models such as SaaS and new applications such as video without compromising security or network performance
- Helps control risk and meet compliance objectives through an open and controlled architecture

Why Cisco?

Cisco takes a comprehensive approach to security. By integrating security into all parts of the network, Cisco simplifies the task of addressing today's business and security requirements, regardless of application or service. The Cisco SecureX Architecture provides distributed enforcement and visibility throughout an organization, including mobile users and the network's reach into the cloud. It provides the scale and flexibility to meet the needs of the largest organization, with options for optimal deployment. No other security approach matches the capabilities of the Cisco SecureX–designed to enable organizations while keepring their entire organization secure and ready to meet their business objectives.

For more information on Cisco security products and services, visit www.cisco.com/go/security and www.cisco.com/go/services/security.