

# Cisco Security 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, iPads, the consumerization of IT, and the rise of social media in the workplace, combined with telecommuters, home offices, contractors, partners, extranets, 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

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. 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.





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 Cisco SecureX Architecture.

▶ Continued on next page

## Network Security



The Cisco network security infrastructure inherently detects and blocks penetration, 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).

			
<p><a href="#">Cisco ASA 5500 Series Adaptive Security Appliance</a></p>	<p><a href="#">Cisco Intrusion Prevention System</a></p>	<p><a href="#">Cisco Integrated Services Router Generation 2</a></p>	<p><a href="#">Cisco Virtual Security Gateway</a></p>
<ul style="list-style-type: none"> <li>• Combines firewall, VPN, and optional content security and intrusion prevention to distribute network security across your operations</li> <li>• Provides threat defense and highly secure communications services to stop attacks before they affect business continuity</li> <li>• Reduces deployment and operational costs while delivering comprehensive security for networks of all sizes</li> <li>• Supports a wide range of environments from small businesses to large enterprises</li> </ul>	<ul style="list-style-type: none"> <li>• Identifies, classifies, and stops malicious traffic, including worms, spyware, adware, viruses, and application abuse</li> <li>• Delivers high-performance, intelligent threat detection and protection over a range of deployment options</li> <li>• Uses global threat correlation with reputation filtering to prevent threats with confidence</li> <li>• Provides peace of mind with guarantees for coverage, response time, and effectiveness for Microsoft, Cisco, and critical enterprise application vulnerabilities<sup>1</sup></li> <li>• Promotes business continuity and helps businesses meet compliance needs</li> </ul>	<ul style="list-style-type: none"> <li>• Delivers suite of built-in capabilities, including firewall, intrusion prevention, VPN, and cloud-based web security</li> <li>• Promotes the integration of new network security features on existing routers</li> <li>• Provides additional protection without adding hardware and maximizes network security</li> <li>• Decreases ongoing support and manageability costs by reducing the total number of devices required</li> </ul>	<ul style="list-style-type: none"> <li>• Secures virtual network and multi-tenancy environments</li> <li>• Provides trusted multi-tenant access with granular, zone-based, and context-aware security policies</li> <li>• Supports dynamic provisioning of security policies and trust zones during virtual machine (VM) instantiation</li> <li>• Promotes mobility-transparent enforcement and monitoring</li> </ul>

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.

## Email and Web Security

Cisco email and web security solutions reduce the 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.

	
<a href="#">Cisco IronPort Email Security—Cloud, Hybrid, and On-Premises</a>	<a href="#">Cisco Web Security—Cloud and On Premises</a>
<ul style="list-style-type: none"><li>• Provides a multi-layered approach to fighting spam, viruses, and blended threats to protect organizations of all sizes</li><li>• Provides fully integrated outbound control through data loss prevention and encryption</li><li>• Reduces downtime, simplifies administration of corporate mail systems, and eases the technical support burden</li><li>• Offers comprehensive reporting and message tracking for administrative flexibility</li><li>• Provides flexible solutions to grow with your organization's needs</li></ul>	<ul style="list-style-type: none"><li>• Provides most effective defense against web-based malware: Cisco SIO, combining best-in-class web reputation and content analysis intelligence</li><li>• Delivers rich, flexible policy controls that are effective for Web 2.0 sites with dynamic content and embedded applications</li><li>• Provides rich reporting capabilities for flexible, unsurpassed visibility into web usage</li><li>• Offers choice of deployment options with industry leading ScanSafe and IronPort Web Security technology</li></ul>

## 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](http://www.cisco.com/go/sio).

## Secure Mobility

Cisco promotes 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.

		
<p>Cisco AnyConnect Secure Mobility Solution</p>	<p>Cisco Adaptive Wireless IPS Software</p>	<p>Cisco Virtual Office</p>
<ul style="list-style-type: none"> <li>• Provides an intelligent, smooth, and reliable connectivity experience</li> <li>• Ideal for companies that want to give users a choice of how, when, where, and on what device they access their information</li> <li>• Teams with ASA 5500 Series Adaptive Security Appliances at the headend to provide remote-access connectivity policy enforcement that is context-aware, comprehensive, and preemptive</li> <li>• Enforce web security and policy, even for off-VPN communications, with Cisco's premise-based IronPort Web Security Appliances or cloud-based ScanSafe</li> </ul>	<ul style="list-style-type: none"> <li>• Provides automated wireless vulnerability and performance monitoring to deliver visibility and control across the network</li> <li>• Maintains a constant awareness of the RF environment to meet the demands of the largest networks</li> <li>• Automatically monitors for wireless network anomalies and to identify unauthorized access and RF attacks</li> <li>• Collaborates with Cisco network security products to create a layered approach to wireless security</li> </ul>	<ul style="list-style-type: none"> <li>• Extends highly secure, rich, and manageable network services to employees working outside the traditional work environment</li> <li>• Cost-effectively scales to deployment requirements through standard or express versions</li> <li>• Includes remote site and headend systems, remote site aggregation, and services from Cisco and approved partners</li> <li>• Delivers an office-caliber experience to staff wherever they're located with full IP phone, wireless, data, and video services</li> </ul>

## Secure Access Control

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.

		
<p><a href="#">Cisco Identity Services Engine</a></p>	<p><a href="#">Cisco Secure Access Control System</a></p>	<p><a href="#">CiscoWorks LAN Management Solution</a></p>
<ul style="list-style-type: none"> <li>• Gathers information from users, devices, infrastructure, and network services to enforce consistent contextual-based business policies across the network</li> <li>• Provides visibility into who and what is on the network for advanced discovery and troubleshooting</li> <li>• Enforces security policy on all devices that attempt to gain access to the network</li> <li>• Combines authentication, authorization, and accounting (AAA), posture, profiling, and guest management</li> </ul>	<ul style="list-style-type: none"> <li>• Controls network access based on dynamic conditions and attributes through an easy-to-use management interface</li> <li>• Meets evolving access requirements with rule-based policies for flexibility and manageability</li> <li>• Simplifies management and increases compliance with integrated monitoring, reporting, and troubleshooting capabilities</li> <li>• Adopts an access policy that takes advantage of built-in integration capabilities and distributed deployment</li> </ul>	<ul style="list-style-type: none"> <li>• Simplifies the configuration, administration, monitoring, and troubleshooting of Cisco networks</li> <li>• Maximizes network security through integration with the TrustSec access control systems, as well as audits of network-level changes</li> <li>• Increases the overall availability of the network by quickly identifying and fixing network problems</li> </ul>

# Security Management

Cisco offers centralized operational tools to simplify and help you manage your entire network security deployment. In addition, Cisco has partnered with best-in-class technology vendors to deliver security information and event management (SIEM) systems that have been pre-tested and validated with Cisco security products. This variety of management options gives you the flexibility to choose the network security management solutions best suited to your environment and business needs.

		
<p><a href="#">Cisco IronPort Security Management Appliance</a></p>	<p><a href="#">Cisco Security Manager</a></p>	<p><a href="#">Validated SIEM Partnerships</a></p>
<ul style="list-style-type: none"> <li>• Simplifies security management across Cisco IronPort email and web security products</li> <li>• Delivers centralized reporting, message tracking, and spam quarantine for email security appliances</li> <li>• Provides centralized web policy management for web security appliances</li> <li>• Allows for delegated administration of web access policies and custom URL categories</li> </ul>	<ul style="list-style-type: none"> <li>• Facilitates the configuration and management of Cisco firewalls, VPNs, IPS sensors, and integrated security services</li> <li>• Ideal for controlling large or complex deployments of Cisco network and security devices</li> <li>• Supports role-based access control and an approval framework for proposing and integrating changes</li> <li>• Delivers flexible device management options, including policy-based management and methods for deploying configuration changes</li> </ul>	<ul style="list-style-type: none"> <li>• Third-party SIEM vendors that have been validated for use with Cisco security products enable you to address your unique security and reporting needs and gain assurance that the solutions work together</li> <li>• Solution guides with deployment recommendations and integration findings are included for overall management and for each technology partner's product to enable you to get up and running faster</li> </ul>

## 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 keeping 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](http://www.cisco.com/go/security) and [www.cisco.com/go/services/security](http://www.cisco.com/go/services/security).

