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 business users and networks have changed. Users are demanding to use their personal smartphones, tablets, and other consumer devices to access the corporate network. Many of these users now reside outside the physical network, yet still require access to critical resources and applications using their personal consumer devices. This is not just true for employees. Contractors and partners also require access to resources and collaboration tools located inside the network, as well as business-critical services and applications that are 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 what is inside and what is 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 Framework

The Cisco SecureX strategy is a context-based, next-generation security approach that weaves together flexible and intelligent solutions, products, and services to enable and enforce consistent business policy throughout the distributed network. The Cisco SecureX strategy 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 solutions protect today's evolving networks by providing effective security for any user, using any device, from any location, at any time. This comprehensive security approach uses a higher-level policy language that understands the full context of a situation—the who, what, where, when and how of every connection—by providing organizations with end-to-end network intelligence from the local network using the Cisco AnyConnect™ Secure Mobility Client and Cisco TrustSec®, and near-real-time global threat information from Cisco Security Intelligence Operations (SIO). 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 Framework.

Continued on next page

Comprehensive Network Security Services

Cisco provides a comprehensive suite of highly integrated, market-leading security services to protect networks of all sizes. From Cisco ASA firewalls to Cisco IPS sensors, Cisco security solutions are available in a wide range of sizes and performance levels to fit networks and budgets of all sizes, while offering a consistent, proven level of security.

Cisco ASA protects corporate networks while providing users with secure access to data—anytime, anywhere, using any device. With more than 15 years of proven firewall leadership and over 1 million security appliances deployed throughout the world, Cisco ASA delivers a trusted level of security that protects some of the largest networks at some of the most security conscious companies in the world. Cisco ASA is available in an array of form factors, including standalone appliances, high-performance blades that integrate with existing Cisco network switches, and virtual instances to secure virtual and cloud environments.

Cisco IPS delivers advanced network awareness and threat protection up to Layer 7 to defend the data center, core, or edge. Unlike most IPS products which rely exclusively on signature firings, Cisco IPS solutions also use source reputation to mitigate identified attacks. With Cisco Global Correlation backed by Cisco SIO, Cisco IPS gains visibility into hundreds of additional security parameters, millions of rules, and 8 TB of threat telemetry per day from market-leading email, web, firewall, and IPS devices. Cisco IPS uses broad network context through every stage of analysis, including victim OS, evasion techniques, attack state across signatures, and an industry first: attacker identity and behavior. Cisco IPS is available in standalone appliances, high-performance blades and integrated software modules that integrate with Cisco ASA firewalls and ISR routers.

		
Cisco ASA 5500 Series Adaptive Security Appliance	Cisco ASA 5500-X Series Midrange Security Appliance	Cisco ASA CX Context-Aware Security
• 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	• Delivers broad and deep network security through cloud- and software-based integrated security services backed by Cisco SIO • Provides comprehensive antimalware capabilities, including three antivirus scanners, botnet traffic filter, and anti-spyware • Scales to meet the performance and budget requirements of a wide range of network applications • Offers the ability to enable additional security services quickly and easily, in response to changing needs	• Delivers end-to-end network intelligence by combining context from local traffic with in-depth global network context • Provides deep insights and the ability to develop security policies based on specific users, applications, and sites visited; and the type, location, and security posture of mobile devices • Enforces individual- and group-based policies that enable access to specific components of an application, while disabling others • Blocks port- and protocol-hopping applications for more effective security, while writing fewer policies

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.

Cisco Intrusion Prevention System

- 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

Cisco Integrated Services Router Generation 2

- 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

Cisco Security Manager

- 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

Application and Content Control

Cisco's email and web security solutions reduce costly downtime associated with email-based spam, viruses and other malware, web threats, and data loss, 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	Email and Web 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 security solutions stay ahead of the latest threats with continuous real-time threat intelligence feeds from Cisco Security Intelligence Operations (SIO). Cisco SIO is the world's largest cloud-based security and threat intelligence ecosystem, using almost a million live security data feeds from deployed Cisco email, web, firewall, and intrusion prevention system (IPS) solutions to generate nearly 8 million security updates per day.

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

After analysis, new security rules are created and dynamically delivered to 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

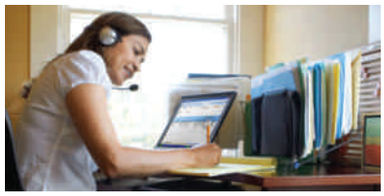
Cisco's security solutions for mobile workers and devices promote highly secure mobile connectivity with VPN, wireless security, cloud-based Internet protection, and remote workforce security solutions that extend network access safely and easily to a wide range of users and devices. Cisco Secure Mobility 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

- 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

Cisco Adaptive Wireless IPS Software

- 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



Cisco Virtual Office

- 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

Data centers are undergoing rapid evolution, and Cisco's security solutions are designed to protect high-value data center resources and servers, including virtualized environments, with high-performance threat protection, secure segmentation, and policy control.

			
Cisco ASA 5585-X Adaptive Security Appliance	Cisco Catalyst 6500 ASA Services Module	Cisco ASA 1000V Cloud Firewall	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	· Uses the proven ASA security platform to provide consistent, enterprise-class security for private and public clouds · Complements the zone-based security capabilities of the Cisco Virtual Security Gateway (VSG) to provide multi-tenant edge security, default gateway functionality, and protection against network-based attacks · A single instance spans multiple ESX hosts to provide deployment flexibility and enhanced cloud security appliance manageability · Uses VNMC as a multi-tenant manager for enhanced manageability of the security components of the cloud infrastructure · Enables role-based access privileges for more precise control	· 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 Unified Access

Cisco TrustSec® is an intelligent and scalable access control solution mitigating security risks across the entire network through comprehensive visibility, exceptional control and effective management It 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

- 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
- Enables IT to offer mobile business freedom by allowing users to easily self-provision their device
- Delivers the deepest, broadest, and most accurate device knowledge with network-based Device sensors and real-time endpoint scans to gain more relevant insight
- Protects data on mobile devices and help ensures compliance by partnering with multiple mobile device management (MDM) vendors

Cisco Secure Access Control System

- 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?

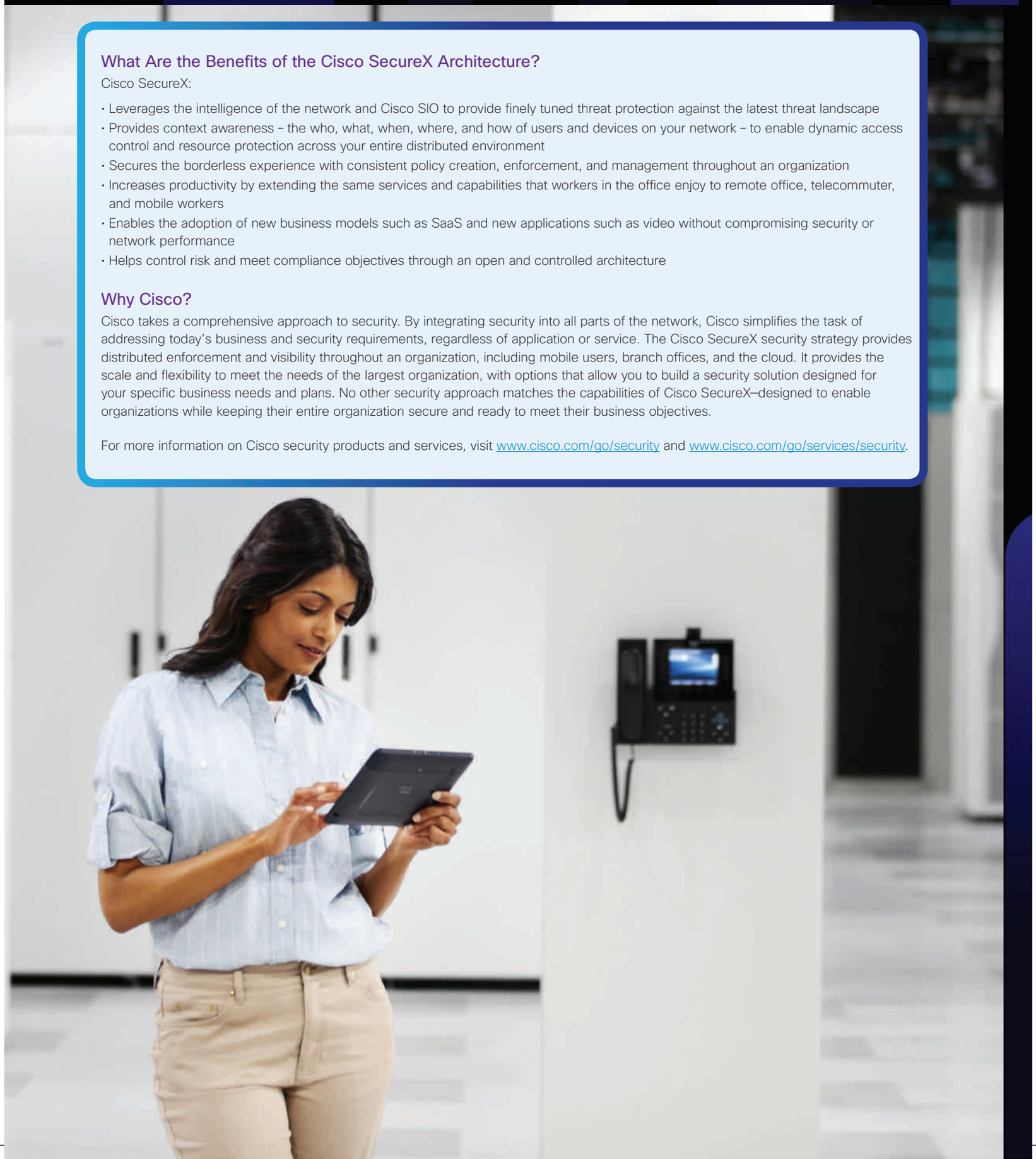
Cisco SecureX:

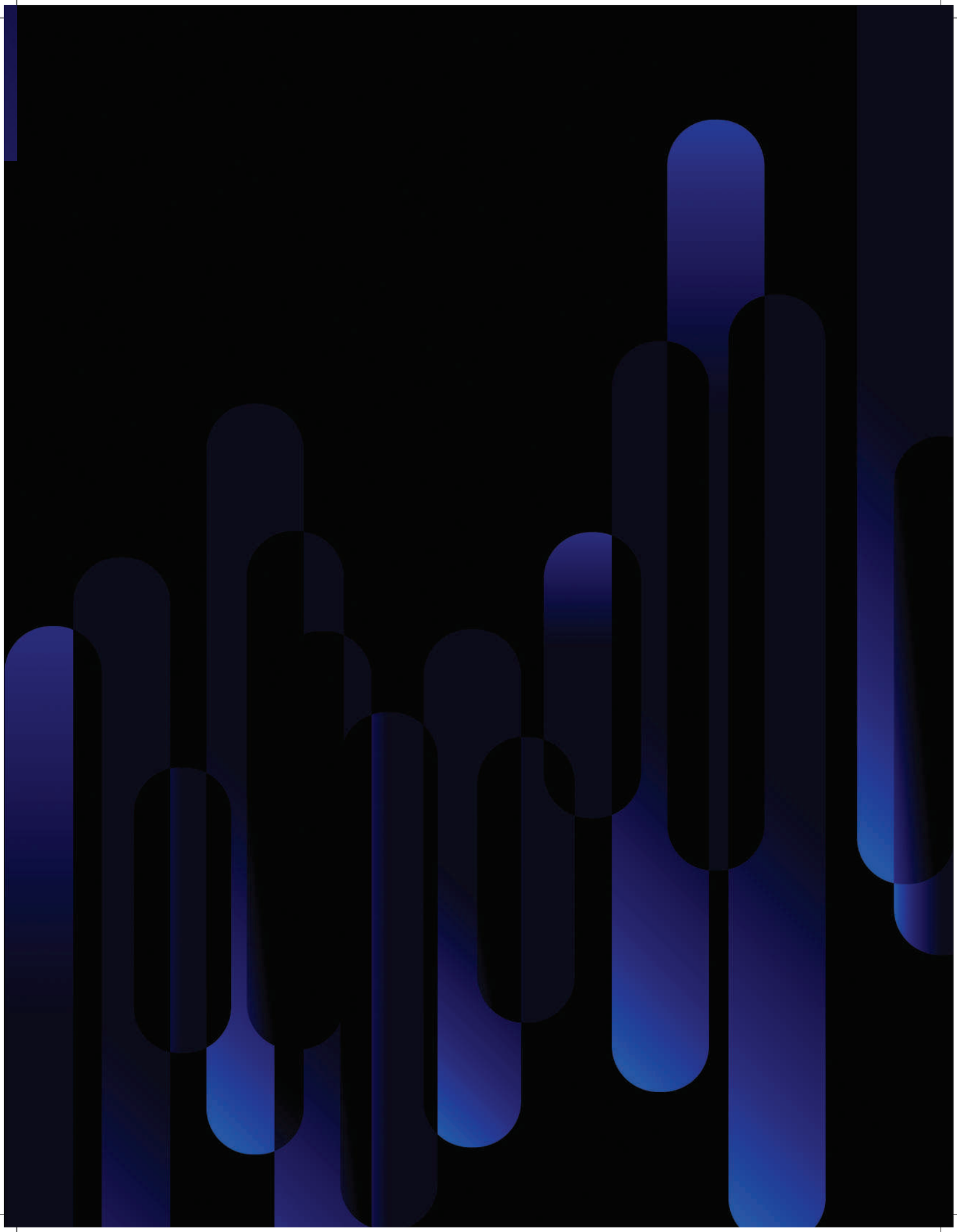
- Leverages the intelligence of the network and Cisco SIO to provide finely tuned threat protection against the latest threat landscape
- Provides context awareness – the who, what, when, where, and how of users and devices on your network – to enable dynamic access control and resource protection across your entire distributed environment
- Secures the borderless experience with consistent policy creation, enforcement, and management 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

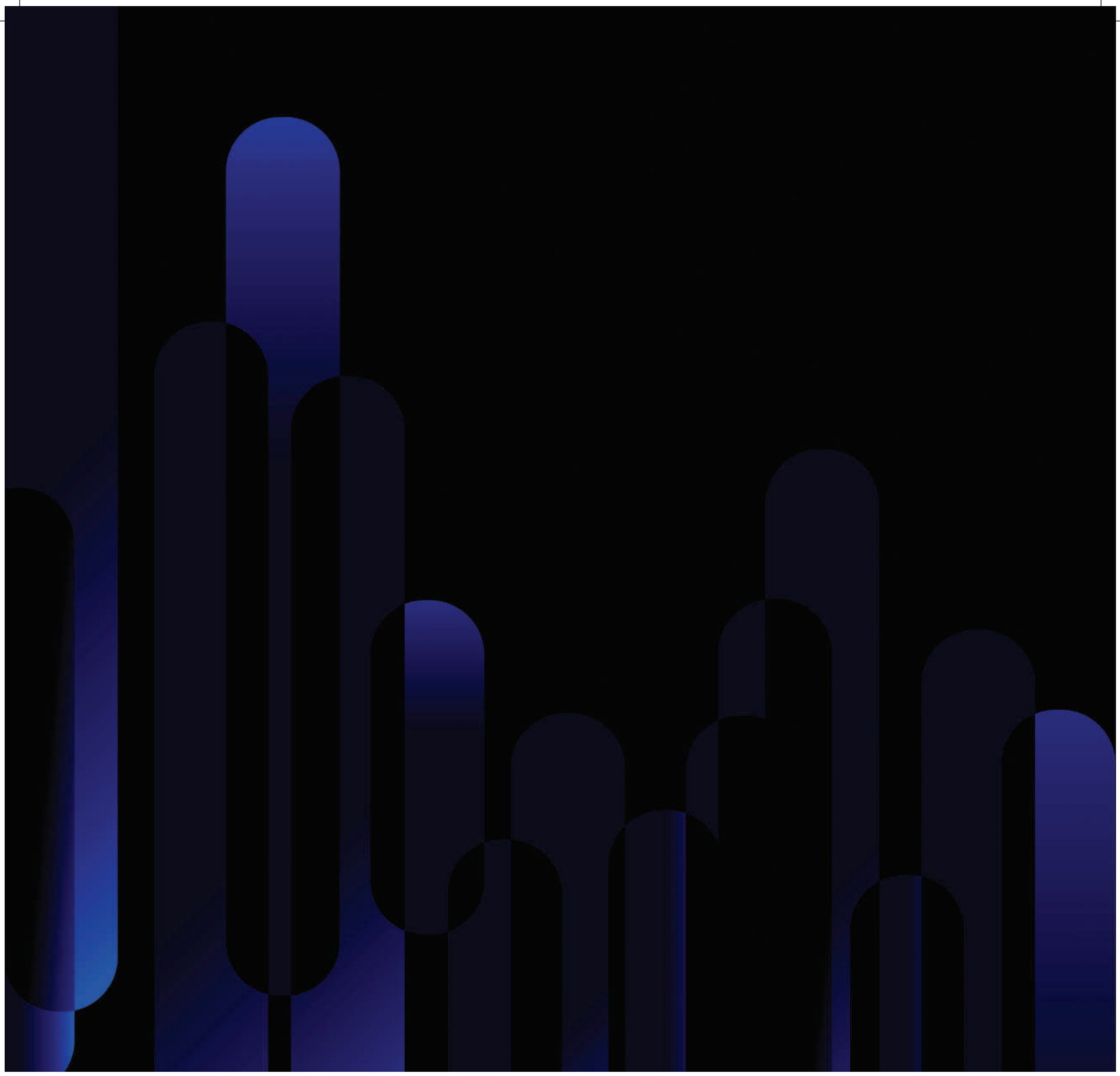
Why Cisco?

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 security strategy provides distributed enforcement and visibility throughout an organization, including mobile users, branch offices, and the cloud. It provides the scale and flexibility to meet the needs of the largest organization, with options that allow you to build a security solution designed for your specific business needs and plans. No other security approach matches the capabilities of 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 and www.cisco.com/go/services/security.







Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

C02-632589-04 03/12