Cisco Self-Defending Network: Combining Best-of-Breed Products and Services with a Systems Approach

A new generation of interactive business communication and collaboration technologies provides tremendous productivity and flexibility gains for organizations of all kinds. But this unprecedented connectivity also unleashes new, complex security risks, including:

- **Increased exposure to security threats**—Ubiquitous access to Web-enabled applications and services enables users to work from anywhere, anytime—but also places businesses at risk anywhere, anytime.
- **An eroding network perimeter**—The traditional network barriers that separated trusted from untrusted and "inside" from "outside" are now disappearing. As more applications become directly accessible to remote users and systems, the concept of the network perimeter becomes increasingly vague and more difficult to protect.
- **Evolving threats**—Information attacks of the past were largely an issue of cyber-vandalism, with hackers primarily looking for fame. Today's attacks are a profit-driven business, often controlled by organized crime. The modern attacker uses a patient, "stealth" approach to eventually achieve a successful attack. In addition, modern attackers often avoid technology defenses, using spam, phishing attacks, and fraudulent Web links to target an organization's weakest link: human beings.

As security risks have evolved, so have organizations' approaches to them. Where information security was once a technology issue, today it is a business issue—representing a more significant cost and operational challenge, but a fundamental business enabler as well. More and more organizations are implementing formal programs to reduce IT risk, especially security and compliance risks. As regulatory compliance becomes a core requirement for organizations in more industries, businesses must develop new capabilities for controlling the kinds of information traversing their network, how that information is used, and who can access it. Organizations not only face the challenge of becoming compliant, but of staying compliant as the network continuously evolves with business needs.

"When we build a security environment that is flexible, manageable, and layered, we can handle any new challenges that may appear. Our Cisco solution definitely gives us this capability."
—Al Grapoli, network manager, State of Oregon

Organizations are wrestling with information security demands that span many overarching business challenges such as complying with regulatory requirements, preventing data loss, and blocking malware. The problem is that dealing with these types of challenges requires a true security solution—not just security products. To prevent data loss alone, for example, businesses need a combination of strong perimeter defenses, malware defenses, identity services, endpoint security, policy enforcement mechanisms, and security monitoring tools, as well as a strong plan

for making them all work in concert. No single security product can provide all of these capabilities. So, today's businesses need security solutions that combine multiple best-of-breed products and approaches into a single, autonomous defense system. They need a truly holistic security solutions approach to network defense.

The Cisco Self-Defending Network: Best-of-Breed Security in a Systems Approach

In the past, many businesses thought they had to make a choice when it came to security: They could use best-of-breed products that were effective against specific types of emerging threats but did not fully integrate into a pervasive defense system. Or, they could take a systems approach that assimilated point products that were "good enough" into an intelligent system architecture. For modern businesses, however, neither option is enough. To meet today's security challenges, businesses need both best-of-breed product capabilities and the ability to plan, design, integrate, and operate those capabilities as an overarching, autonomous system. Only one security vendor can provide such a solution: Cisco®.

The Cisco Self-Defending Network combines best-of-breed point technologies to address emerging threats, a systems approach built on Cisco's industry-leading product portfolio to autonomously respond to pervasive threats, and Cisco's differentiating security services portfolio to help make the solutions approach a reality. This unique, comprehensive approach to information security is helping businesses around the globe reduce IT security and compliance risk, enforce business policies, and protect critical assets, while lowering administrative burden and reducing total cost of ownership.

> **"We chose a Cisco security solution because of Cisco's strategy and architectural approach. They look beyond the network 'plumbing' and enable us to focus on delivering the applications and services that we need."**
> **—Ray Smith, director of information services, Mississippi State Board for Community and Junior Colleges**

Cisco offers the broadest and deepest product and services portfolios in the industry, with channel partners that are empowered to design and implement solutions customized to the unique requirements of any business. Building on a history of security innovation, Cisco provides a powerful suite of best-of-breed security products, including market-leading firewall, virtual private networking (VPN), and intrusion prevention system (IPS) technologies. These products have earned the praise of industry analysts and achieved numerous awards, and are used by organizations around the world to address the most challenging business and security needs. Likewise, Cisco security services enable organizations to follow a lifecycle methodology to design, implement, operate, and optimize secure networks that are resilient and reliable, and align technology investment with business strategy.

An Evolving Vision of Autonomous Security

The Cisco Self-Defending Network strategy was initially built upon a network foundation—embedding core firewall, VPN, and IPS security technologies within the fabric of the network itself. As business practices and security risks continue to evolve, however, the Cisco Self-Defending Network is evolving as well. Today, the Cisco Self-Defending Network builds on industry-leading network and endpoint defenses to incorporate innovative application security, content security, policy enforcement, identity management, and security monitoring technologies. By integrating

best-of-breed product capabilities in all of these areas into a systems approach to information security, Cisco can provide a comprehensive solution for meeting today's security challenges.

The Cisco Self-Defending Network encompasses:

- **Network and endpoint security—**The Cisco Self-Defending Network integrates firewall, VPN, IPS, and other security services into network devices and endpoints to create an integrated, adaptive, and collaborative defense system.
- **Content security**—Cisco product and security innovations extend network defenses beyond the traditional network perimeter to protect data in motion, incorporating e-mail, Web interactions, instant messaging systems, and other applications that require content inspection and control.
- **Application security**—A Cisco Self-Defending Network extends protection to applications and data, providing XML and HTML inspection capabilities and fine-grained application control.
- **System management and control**—Today's Cisco Self-Defending Network integrates sophisticated policy, identity, and reputation services with powerful enforcement capabilities. These technologies unify disparate network, endpoint, content, and application security services, and provide businesses with unprecedented visibility and control.

The comprehensive Cisco Self-Defending Network strategy not only provides organizations with the state-of-the-art product capabilities they need to defend against the most serious emerging threats, but also provides a system that can continually adapt to the changing security landscape and autonomously respond to pervasive threats. And, it provides a range of services to help plan, deploy, operate, and optimize the secure system. Over the life of the network, collaboration among best-of-breed Cisco security products continually improves to provide better protection and reduce the time and effort required to achieve security objectives. Ultimately, these capabilities allow businesses to protect critical assets, enforce business policies, and reduce security compliance and IT risk, with less administrative burden and a lower total cost of ownership.

Self-Defending Network Foundation: Network and Endpoint Security

The core strategy of the Cisco Self-Defending Network is to make network security integrated into the network, adaptive to new threats, and collaborative across multiple capabilities and devices. Since the 1990s, Cisco has continually evolved its product portfolio under this guiding philosophy. Today's Cisco network security solutions are:

- **Integrated**—Market-leading Cisco products such as Cisco ASA 5500 Series Adaptive Security Appliances, Cisco Integrated Services Routers, and Cisco Catalyst® 6500 Series Switches embed a robust suite of security services into the network. Cisco provides security options using Cisco IOS® Software security features; modules in Cisco routers, switches, and adaptive security appliances; dedicated Cisco security appliances; or a combination of technologies. Today, more than 1.4 million Cisco routers and more than 3 million switches used by companies around the world provide integrated security.
- **Adaptive**—Cisco security products augment traditional signature-based detection technologies with behavioral-based capabilities. Cisco Security Agent, for example, monitors endpoint operating systems to detect suspicious behavior, allowing it to respond to both known and unknown "day-zero" threats. Technologies such as Cisco Guard Distributed Denial of Service (DDoS) Mitigation, Cisco Anomaly Guard, and Cisco NetFlow Event

Management products provide sophisticated capabilities to detect and dynamically respond to abnormal events such as DDoS attacks.

- **Collaborative**—Cisco's commitment to collaboration among diverse network components helps organizations implement more pervasive protection and simplify security management. For example, if Cisco Security Agent detects suspicious activity on a host PC, it can communicate with the Cisco Security Monitoring, Analysis, and Response System (MARS). Cisco Security MARS then collaborates with the Cisco network IPS solution to closely monitor traffic flows to and from that endpoint and cut off any potential attack. To enhance policy enforcement, Cisco Security Manager allows organizations to configure policies through a centralized interface and push changes out across the entire environment. Cisco Unified Communications and wireless technologies are designed to draw on multiple components of these solutions to enforce security.

These capabilities provide unparalleled network and endpoint protection, but they also serve as a powerful foundation for fulfilling the vision of the Self-Defending Network. With integrated, adaptive, and collaborative network and endpoint technologies, Cisco can:

- Transparently embed security services into the network
- Empower security teams to manage network security more efficiently, with fewer touch points
- Scale performance and services to customer needs
- Align security technology controls with business risk
- Deliver pervasive identity services
- Provide robust endpoint posture and policy assessment capabilities
- Improve business policy enforcement and compliance
- Provide strong protection against data leakage and loss

Cisco's commitment to building integrated, adaptive, and collaborative systems for network security has proven invaluable to organizations around the globe. To date, Cisco has shipped more than 1.5 million security appliances, more than 3 million switches with integrated security, and more than 500,000 Cisco Integrated Services Router security bundles. Indeed, Cisco's powerful combination of best-of-breed product capabilities, broad services portfolio, and an integrated systems approach has made Cisco the worldwide market leader in network security.

Protection Beyond the Perimeter: Content Security for Data in Motion

New forms of communication and collaboration such as e-mail, Web applications, and instant messaging allow employees to work more collaboratively and flexibly than ever before. But these applications also present compelling targets for criminals seeking to launch and propagate malware attacks. Modern communications tools also create new challenges and costs for businesses, such as coping with spam, which continues to grow at an alarming rate every year.

“It’s about protecting your company, its assets, and its employees. Protecting our network is fundamental, but protecting all the data that is stored and transmitted across that network is just as important. We put a lot of time and effort into finding solutions that would fulfill our vision for comprehensive data security and we believe in Cisco’s Self-Defending Network solution strategy as a way to bring that vision to life.”

—Chris Whitesock, information security manager, Coastal Federal Credit Union

To address these emerging threats and provide protection beyond the network perimeter, Cisco offers a portfolio of best-of-breed content security technologies. Cisco content security tools include Cisco ASA 5500 Series content security technologies; Cisco IOS Software content filtering and voice security technologies; and industry-leading Web and e-mail security technologies from IronPort, now a Cisco company. These technologies incorporate innovative content security strategies such as:

- **Treating all threats as “day-zero”attacks—**Cisco content security solutions are designed to analyze an unlimited number of variants, rather than seeking out a small set of targets. Using behavior- and reputation-based analysis, these technologies can identify attacks that share functions, even if they don’t share a specific attack signature.
- **Providing scalability to address myriad attacks**—Modern attacks are extremely diverse, ranging from simple e-mail fraud to sophisticated, multivector threats such as the NIMDA worm, which can infect and propagate across thousands of hosts using multiple means. Cisco content security technologies are designed to recognize all attacks as unique threats, regardless of scale.
- **Providing tools to manage multiple techniques and sources of attack**—Cyber-criminals may target everything from office applications to collaboration software to e-mail, employing a variety of self-propagating and user-propagating techniques. Cisco content security solutions provide strong protection regardless of attack source, transmission medium, or propagation method.

Drawing on these powerful Cisco content security capabilities, organizations can:

- Protect against Web-based security threats such as phishing attacks, URL outbreaks, and botnets
- More easily meet regulatory compliance requirements for secure voice and data communications
- Reduce the expense of securing small offices, branch offices, and telecommuter environments
- Enforce corporate Web and content usage policies more efficiently and effectively
- Eliminate the vast majority of spam before it reaches mail servers and impedes employee productivity and network bandwidth

Cisco and IronPort have been early leaders in content security and have a rich history of innovation in this area. Cisco was the first network technology provider to support content security in the network switching and routing fabric, and IronPort was the first to integrate data loss prevention capabilities for data in motion. IronPort has also pioneered multiple innovations in e-mail encryption and Web and application security. Today, Cisco is the market leader in e-mail security, with Cisco/IronPort solutions providing visibility into 25 percent of global e-mail traffic.

Protecting Business Applications and Data: Application Security

As business use of XML applications, Web services, and service-oriented architectures continues to grow, organizations need new tools for securing these applications—both from malicious external threats and from mistakes or abuse by legitimate users. In fact, Cisco research indicates that while the number of newly discovered operating system vulnerabilities has declined over the past several years, the number of application vulnerabilities has increased by double-digit percentages annually.

The Cisco Self-Defending Network includes best-of-breed application security technologies to provide:

- Layer-7 application protection for vulnerabilities in office and Web applications, Web servers, and application servers
- Role-based authorization for accessing applications
- Identity services that extend from the network to applications
- XML traffic validation and inspection
- Enhanced deep-packet inspection to identify application protocols

At the core of Cisco's application security strategy is the Cisco ACE Web Application Firewall. The technology provides comprehensive HTML and XML Web application traffic inspection to prevent application hacking, secure both custom and packaged applications, and address the full range of Web application threats. These capabilities protect organizations from attacks such as identity theft, data theft, application disruption, and targeted attacks, while simplifying compliance with regulatory requirements such as Payment Card Industry (PCI) data security standards. Ultimately, they allow businesses to take full advantage of modern Web communication and collaboration applications while protecting critical assets and reducing compliance and IT risk.

Improving System Management and Control: Identity, Policy, and Reputation

Even the strongest network and endpoint security, application security, and content security technologies cannot, on their own, address the full range of security challenges that modern organizations face. To provide comprehensive malware protection, prevent data leakage, and help ensure regulatory compliance across the enterprise, businesses need an intelligent overarching system management and control framework. They need tools to monitor the behavior of users and devices across the environment, provide end-to-end identity services, and enforce corporate policies.

The Cisco Self-Defending Network includes a comprehensive suite of operational control and monitoring services to provide total security system management. Cisco Security Manager, for example, provides best-of-breed policy management tools to centrally configure and enforce corporate policies across the enterprise. Cisco Security MARS provides sophisticated security monitoring and threat analysis to help organizations correlate security event information across

even the largest, most complex environments, and dynamically identify and respond to threats. When combined in a Cisco Self-Defending Network, these technologies allow businesses to:

- Automate many security functions to optimize resources and dramatically reduce the administrative burden
- Align monitoring and policy services into a single, enterprisewide system
- Employ reputation-based and behavior-based information across multiple security services to more rapidly and effectively respond to threats
- Maintain a comprehensive view of the environment to simplify regulatory compliance and IT risk management

Ultimately, these technologies help organizations manage network monitoring, identity, and policy services much more efficiently, and provide unparalleled operational control.

"Understanding which users do what and where, on networks and on applications, is a key component of the compliance strategy of virtually every enterprise. Doing so requires implementing a security architecture based on the roles and identities of users. In our recent benchmark on security and information protection, enterprise IT executives cited Cisco as the top strategic security vendor relied on to help with these and other security initiatives."

—Andreas M. Antonopoulos, Analyst Nemertes Research

Cisco Security Services and Support

Cisco Security Services enable organizations to follow a lifecycle methodology to design, implement, operate, and optimize secure networks that are resilient and reliable, and align technology investment with business strategy. Businesses today are increasingly mobile, extended, and operating in collaboration with partners, vendors, and customers. In this environment, they must manage risk by protecting data at rest and in motion, maintaining regulatory compliance, and protecting themselves from both internal and external threats. Cisco provides a comprehensive suite of security services to help organizations meet these challenges. These services derive from Cisco's proven strength in designing, implementing, and managing many of the world's largest converged networks.

Cisco Security Center

Cisco Security Center, at http://www.cisco.com/security, offers powerful, timely intelligence to assist organizations in proactively addressing potential security threats before they affect the business. Cisco Security Center provides:

- Event-based, early warning security intelligence
- Comprehensive alert analysis and mitigation solutions powered by Cisco Security IntelliShield

- Real-time e-mail threat, virus, and spam tracking and trending
- Easy access to comprehensive security best practice guidance
- Security Intelligence RSS feeds

Cisco Channel Partners

The Cisco Security Specialization Program recognizes Cisco channel partners that have developed the skills required to sell, design, install, and support Cisco network security solutions for customers. As Internet business solutions are adopted, Cisco Security Specialized Partners can meet the growing demand for critical security implementations and support services.

Cisco Training Services: Cisco Security Certifications

Using best-in-class training and exams, Cisco security certifications validate the skills and competencies of security professionals. The Cisco CCSP® certification validates the advanced knowledge and skills required to secure Cisco networks. With a CCSP, a network professional demonstrates the skills required to secure and manage network infrastructures to protect productivity and reduce costs. Cisco security courseware also meets the 4011 training standard. This standard is intended for information systems security (INFOSEC) professionals responsible for the security oversight or management of critical networks.

Security-Focused Authorized Cisco Learning Partners

Many authorized Cisco Learning Partners worldwide focus on Cisco security training, offering courses, remote labs, self-study materials, and other resources on the latest security technologies. These include advanced Cisco adaptive security appliances, Cisco secure intrusion detection systems, and end-to-end security implementation. A Learning Locator, course information, exam dates, and a detailed list of security-focused partners are available at http://www.cisco.com/go/training.

Building Real-World Solutions for Today's Business Challenges

Modern applications and communications tools are providing businesses with unprecedented efficiencies and flexibility, but they also carry a cost: continually expanding IT risk. Fortunately, while information security threats have never been more challenging, the tools at an enterprise's disposal to address those threats have never been more powerful. By combining best-of-breed security products with a systems approach, the Cisco Self-Defending Network provides all the capabilities businesses need to defend against malware, halt data loss, and streamline regulatory compliance. These advanced, autonomous solutions are not just conceptual. They are being used in real-world networks around the world every day, helping millions of businesses meet their security challenges, lower operational costs, and better manage IT risk.

For More Information

To find out more about the Cisco Self-Defending Network, visit http://www.cisco.com/go/sdn.

For more information on Cisco security products, visit http://www.cisco.com/go/security.

For more information on Cisco Security Services, visit http://www.cisco.com/go/services/security.

To view detailed network designs for security solutions, visit the Cisco Design Zone at http://www.cisco.com/go/designzone.

For more information and detailed network designs for PCI compliance, visit http://www.cisco.com/go/pci.

To find the latest information about emerging security threats, visit Cisco Security Center at http://www.cisco.com/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.**

Printed in USA C02-466111-00 04/08