



Securing Your Business with Your Network: Security Made Simple



Today, businesses of every size are concerned about the safety of their company information. Customer credit card numbers, private accounting information, data on purchases, suppliers, and inventory—no one wants that kind of information getting out. But how can you set up your infrastructure to make sure it doesn't?

For a security system to be successful, it should:

- Protect against internal and external network attacks
- Ensure privacy of all communications, at any place and any time
- Control access to information by accurately identifying users and their systems
- Reduce any liability resulting from compliance requirements
- Take into account your company's culture and method of operations
- Maintain productivity by quickly deploying new solutions and protocols
- Deliver a fast return on investment (ROI) and use existing hardware and software wherever possible

Cisco® networking technologies lead the industry in protecting your company's confidentiality. In an intelligent Cisco Self-Defending Network, all aspects of your infrastructure—including applications, desktops, laptops, IP Phones, and servers, as well as network devices such as routers, switches, wireless access points, and appliances—have security features integrated into them to protect your organization from harm.

Understanding How Security Works

Complete business protection depends on using not just one security method, but a set of barriers that defend your business in a variety of ways. Even if one solution fails, others still stand, guarding your company and its data from a wide variety of network attacks.

With these multiple barricades integrated directly into the network, which supports all your other technologies, you automatically safeguard all your applications, appliances, and devices at once. This is the basic concept behind the Cisco Self-Defending Network. The strength of this solution is its flexibility: Whether your business expands or downsizes, adds new channels, updates hardware, or moves its location, the network still protects your entire infrastructure.

Cisco security offerings include:

- **Deploying firewalls**—Firewalls separate the secured corporate network from other unsecured networks, such as the Internet, by blocking unwanted traffic. They also monitor and control the traffic you want based on a “security policy” (a set of rules that define what traffic is permitted). Everyday applications such as e-mail, instant messaging, and Web browsers are protected against misuse.
- **Creating secured communications**—Virtual private networks (VPNs) encrypt information prior to being sent, authenticating users and protecting your information. For this reason, VPNs are essential for remote workers who use the Internet at home, or from Wi-Fi hotspots and hotels.



- **Preventing network intrusions and attacks**—Intrusion prevention systems (IPSs) scan the network for harmful or malicious behavior. They can even take corrective action against an attack, and alert network managers as well.
 - **Controlling Internet threats**—Advanced defenses protect content and users from viruses, spyware, and spam.
 - **Managing endpoint security**—Network Admission Control (NAC) protects your network by verifying each user before granting access to the user's data.
 - **Managing user access**—Authentication, Authorization and Accounting (AAA) services help verify network users, allow the right level of access, and guard against unauthorized use.
- IT managers can oversee the network from remote locations, with less travel and more productivity.
 - Your company requires less investment in security equipment.
 - Your firm is safer from losses due to potential litigation.
 - You have verified compliance to regulatory guidelines, including such common requirements as PCI credit card safety standards.
 - Network bandwidth is properly allocated according to usage, improving performance and responsiveness.

To help you take best advantage of all these tools, Cisco has designed a [Smart Business Roadmap](#) for small to medium-sized businesses. This Roadmap provides a structured path that maps business challenges and “pain points” to technology solutions to help evolve your business over time toward its optimal performance.

Better Cost Containment with Better Security

Cost containment is a top concern for businesses everywhere. By using a network-based security solution that can be easily deployed, integrated, and managed, businesses gain better control over their costs. Leveraging your Cisco investment in infrastructure and applications allows your business to reduce expense and minimize loss due to hacking or lost data. With the right level of security:

- The Internet can be used as an inexpensive medium for secure business communications and commerce.
- Data loss due to attacks, such as viruses and worms, are eliminated.

Improving Operational Efficiency

The Cisco Self-Defending Network allows you to integrate security into the operations of your company, as well as into the network. Your security system can detect and automatically respond to threats, preventing infected files or harmful activities from damaging your business. Your secured transactions can be extended to remote locations as well as suppliers, resellers, and partners. With integrated security:

- Employees, including mobile and teleworkers, are productive any time, anywhere, with secure access to company resources and tools.
- You can carry out business with a high degree of confidence in the integrity of your information.
- Sensitive customer and supplier information is kept confidential.
- Network downtime due to malicious activities is minimized.

- Employees are more productive because the network and critical business applications respond and perform faster.
- Business transactions are processed electronically and on time, and financial reports are available in real time.
- Supplier and compliance paperwork is submitted with minimum effort.
- Your company will achieve better efficiencies through online and electronic customer and supplier relationships.
- Workflow management is improved to maximize production.
- E-mail and instant messaging applications are guarded against misuse.

Rapid Customer Responsiveness

At the most basic level, improving customer responsiveness for your business involves:

- Making it easier to reach employees
- Offering employees many ways to stay connected and respond to customers
- Providing a reliable, up-to-date Website for customers
- Giving employees quick and secure access to customers' history

Network security is essential for your business to achieve this level of responsiveness, because it allows authorized employees and vendors to access company voice and data services over a secure network connection, wherever they may be located. This makes employees more productive in dealing with service requests and inquiries, because they can respond quickly to important e-mails, phone calls, and voice mails whether they are on the road, working from home, or at a customer site.

Also, having a professional and secured Website leaves a positive impression with customers, supporting the perception that your business is available to respond to their needs. Cisco security technology protects the Website so it is always ready to provide accurate information and securely receive customer orders.

With a secure Website:

- Customers get information quickly and easily.
- Customers gain a high degree of confidence that their sensitive data is kept secure.
- Customers perceive your company as competitive and up-to-date.
- Employees serve customer needs in the office, on the road, or telecommuting with full access to the voice and data network.
- Customers can purchase products and services easily and securely from the Website.
- Corporate customer-facing Websites are protected from hacking and misuse.

Your Next Step

Security is the number-one requested integrated service from businesses of every size. Based on the Smart Business Roadmap, Cisco provides industry-leading security solutions with intelligent, resilient, and adaptable functionalities to protect your data. Every aspect of the network is protected by integrated security features to completely guard your organization from threats.

To take advantage of Cisco security solutions for your company, please contact your local Cisco Security Specialized Partner. For additional information, please visit: www.cisco.com/en/US/netsol/ns339/networking_solutions_small_medium_sized_business_home.html



Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

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.

©2006 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCI, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0612R)