



OVERVIEW

MANAGED SECURITY SERVICES FOR SMALL, MIDSIZE, AND ENTERPRISE ORGANIZATIONS

EXECUTIVE SUMMARY

Network security breaches can affect an organization on many levels, from productivity losses to costly downtime, from operational disruptions to unprotected proprietary data. Businesses do not have to engage in e-commerce or e-business transactions to find themselves at risk from an Internet transmission. Internal networks, data and file sharing, e-mail communications, mobile or offsite workers, and worldwide access amount to a network with multiple points of vulnerability. Few organizations have the resources for 24-hour monitoring or the ability to keep informed of the latest network security technologies; those that do may spend more time and money than necessary to support their security operations.

Effective business security is available, however, whether you choose to manage network security operations internally or to out-task to a service provider. This overview explains the basics of network security; the options for small, midsize, and enterprise organizations; business requirements; and some examples of security solutions.

Finding the right security solution for your organization begins with assessing and prioritizing your specific requirements, as well as becoming informed about your alternatives and some of the common decision points. This overview provides a starting place. To learn more, go to Cisco.com or contact a Cisco Systems® representative or Cisco® Powered Network provider.

MARKET OVERVIEW

In the networked business environment, security is not only critical, it has taken on a level of complexity that has affected organizations of all sizes worldwide. Network security today includes constant monitoring and management of both internal and external network operations, from the desktop to e-business transactions to global communications and file sharing. In order to retain their competitive agility and time-to-market responsiveness, businesses find they must maintain a level of openness and connectivity with vendors, partners, customers, and/or employees working remotely. This increased need for external connectivity places network infrastructures at greater risk than ever before. Small businesses can no longer rely only on standard off-the-shelf virus programs to provide sufficient security, while large enterprises experience vulnerability along an infrastructure extended to local, regional, or global offices.

Although the demands of securing daily workflow, transactions, and data have increased substantially, businesses may be reluctant to out-task network security functions, fearing that loss of control over security will put them at greater risk. However, reliable service providers can create a comprehensive security offering that meets the needs of organizations large and small, while building in features that give businesses the control and peace of mind they require. Service providers may manage some or all of their customers' network security functions, helping organizations to take advantage of sophisticated technologies, dedicated manpower, and 24-hour watchfulness, as well as routine maintenance and management of disaster operations.

Security is no longer optional in today's business market and out-tasking is one solution for reducing risk and expenditure, while concentrating on essential business functions and enhancing productivity.

SERVICES DESCRIPTION

Managed security is the out-tasked management and monitoring of network and customer premise security devices, systems, and processes according to a business' security policy. Managed security services include all the provisioning, installation, maintenance, monitoring,

operations, and administrative functions associated with managing a secured network environment. The primary benefit is 24-hour service that improves network security posture and lowers security costs.

Securing a business may encompass hardware and software implementation, management, and monitoring, depending on a particular organization's current infrastructure and requirements.

Services may include:

- *Managed firewalls*—Firewalls protect internal and external network borders by restricting the types of network protocols and traffic allowed across the network border. Firewall appliances, which the service provider manages remotely, include dedicated hardware and software platforms located on your business premises.
- *Managed intrusion detection systems (IDSs)*—Intrusion detection determines when inappropriate access to your network, systems, services, applications, or data has occurred or is underway. Intrusion detection services rely on network-based or host-based monitors, and often match monitored traffic or activity against profiles of known attacks.
- *Managed IP-VPNs*—VPNs are secure, end-to-end, private network connections over third-party networks, such as the Internet or extranets.
- *Managed antivirus protection*—This service most often involves checking for viruses at the gateway or firewall as well as in e-mail messages and attachments, and in file transfers. Automatic updates may be included in the service provision.
- *Managed endpoint threat protection*—This service detects and prevents anomalies from occurring on endpoint devices, such as desktops and servers.
- *Managed authentication*—Authentication monitors and directs processes and technologies to verify the identity of a user attempting to gain access to systems or applications.
- *Managed content filtering*—Filtering is used to isolate and block content deemed inappropriate by internal policies or regulatory policies.
- *Vulnerability assessment*—Involves security risk assessments, network scanning, and probing to reveal network, operating system, or application vulnerabilities in Internet-facing systems.

BUSINESS REQUIREMENTS

If you are considering out-tasking some or all of your network security functions, or widening the array of security services your business currently receives from a service provider, you are part of a trend. Analysts predict a surge in out-tasked security, with the most significant increases in VPN and firewall services.

Out-tasking security does not have to mean relinquishing control over critical business processes. A managed service provider can work with you to help ensure that you maintain control of workflow in your organization. Businesses with in-house IT expertise can determine where control is desirable, and where managed service provider support can free time and resources to devote to widespread infrastructure management and strategic business initiatives.

What primary factors are causing businesses to out-task security and rely on the experience, economies of scale, and advanced technology of a service provider? Businesses today are motivated by the following:

- *Increased security threats*—High-profile feats of hackers and intruders have heightened awareness of network security breaches and security risks. Managed security service providers have the manpower for 24-hour monitoring of the changing security landscape.
- *"Day Zero" damage*—Rapidly spreading attacks occur too fast for reactive products to halt them immediately. Managed security service providers have automated security systems with warning mechanisms and proactive capabilities.
- *Growing use of Internet and remote access*—As businesses increase their investment in the Internet, intranets, extranets, and remote access connectivity, they concurrently increase their exposure to network security threats. Managed security service providers can secure the full range of business connectivity options.

- *Dynamic technology*—Managed security service providers can acquire and keep pace with the latest network security technology. Small and midsize businesses often do not have these in-house capabilities, while enterprises can reduce the cycle of continually investing in new security technologies and training.
- *Growing complexity of e-business models*—Complex e-business models require complex network security solutions. Businesses are finding initial investment costs high for implementing security in house and costly maintenance requirements for adapting existing solutions. Out-tasking security services is one potential avenue for controlling and reducing IT costs.
- *Lack of customer confidence*—Business customers and partners understand the risks, and they are raising network security concerns. Managed security offerings can bolster perceived security of business extranets.
- *Regulatory issues*—Regulatory agencies have begun to require industries to improve network security postures by specific timeframes. Examples include the e-signature law, which makes online contracts with electronic signatures as binding as hard-copy versions, requiring comprehensive authentication capabilities; the Safe Harbor Agreement for compliance with data privacy requirements in the European Union; and the Health Insurance Portability and Accountability Act (HIPAA) for healthcare organizations. Managed security service providers have experience meeting regulatory requirements.

Whether these factors directly affect your business, you may gain the same benefits as other organizations that choose managed security services. These benefits include:

- *Reliability*—The most important benefit of network security is reliability—businesses in today’s marketplace cannot afford to take chances with their security coverage. A managed security service provider’s reputation depends on delivering reliability day in and day out. Organizations require the 24-hour support and state-of-the-art expertise provided by out-tasking security services.
- *Focus*—Out-tasking security services allows an organization to focus its workforce, infrastructure, and IT resources on core business capabilities and strategic initiatives, while using the expertise and advanced technologies of a reliable managed service provider.
- *Lower costs through economies of scale*—Out-tasking security products and software, which can be costly and complicated to implement and manage, can decrease the total cost of network ownership. For this reason, managed security providers can deliver the latest technologies and expertise to their customers at a lower cost.
- *Faster deployment*—Managed security service providers are in the business of implementing network security solutions quickly and efficiently.
- *Reduced IT costs*—Managed security service providers can cut expenditures by offering financial and network performance guarantees through service-level agreements (SLAs).

CASE STUDY

Providing Network Security to a Global Nutritional Health Company

When a premier global nutritional health company needed enhanced security, its leaders decided to out-task, and selected a service provider that operates its services over a network built end to end with Cisco equipment—and thus displays the Cisco Powered Network mark. The solution included a multisite IDS pilot that helped in the evaluation of IDS implementation and usage throughout its worldwide enterprise network. The company benefited from the service provider’s use of efficient, cost-effective, open-source technology. With the help of a reliable service provider, the nutritional health company obtained crucial information about its security network at a reasonable cost, without risking its core business resources.

Decision Tree

When evaluating the role of managed security services in your organization, you will want to assess your current and projected requirements. At a minimum, your assessment should include your:

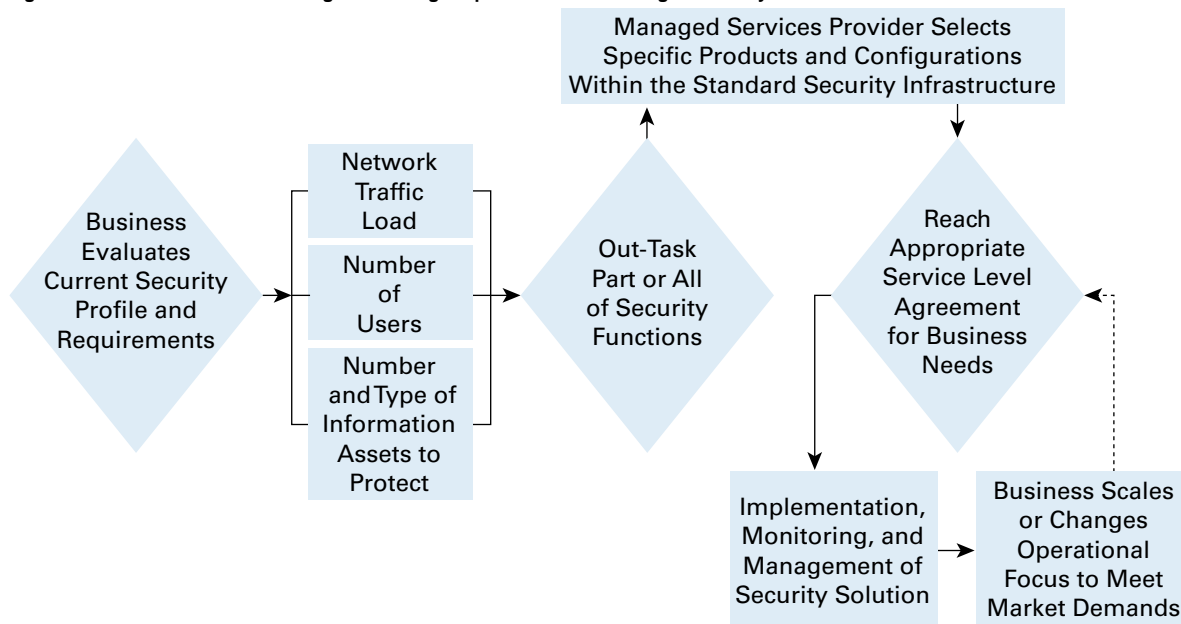
- *Organizational structure*—Evaluate the types of offices and network infrastructure that your organization possesses. Consider your headquarters, branch, and remote offices—locally, nationally, and globally—LAN, MAN, or WAN networks; and mobile and offsite workforce, and the number of workers supported.
- *Network access and availability*—Inventory your bandwidth, application, and usage requirements for both internal and remote workers.
- *Information assets*—List your computer and server hardware, applications, and critical data.
- *Industry requirement*—Assess the industry-specific needs of your organization. For example, financial institutions and banks often incur greater network security risks.

The material presented in Table 1 and in Figure 1 can provide a starting place for discussion about your specific business needs with a managed service provider.

Table 1 Assessing Your Network Security Profile

Small Business	Midsize Business	Enterprise Business
<ul style="list-style-type: none"> • Low complexity • Low traffic volume • Few types of information assets to protect (for example, servers, databases, applications) • Minimal amount of risk associated with each asset 	<ul style="list-style-type: none"> • Medium complexity • May host dozens of servers, multivendor hardware and software platforms, and multiple applications • Several different types of information assets • Varying levels of risk associated with each asset 	<ul style="list-style-type: none"> • High complexity • High bandwidth requirements • Many types of information assets • Maximum risk associated with company assets • Large number of remote locations and teleworkers • Varying levels of security that depend on a business division or workgroup

Figure 1 Decision Tree for Evaluating Networking Requirements and Managed Security Services



Searching for the right managed security service provider to meet your security requirements can begin with assessing and prioritizing your business objectives. Table 2 shows a checklist of potential business objectives and the benefits you may realize.

Table 2 Assessing Your Managed Service Provider

	Objective	Benefit	•
1.	Access to network security expertise and the latest technological security advances	<ul style="list-style-type: none"> • Service provider expertise • Service provider best practices 	
2.	Excellent customer service	<ul style="list-style-type: none"> • 24-hour monitoring • Real-time incident reporting • Administrative control • Onsite support • Reliable service backed by SLA • Responsive support staff 	
3.	Compatibility with existing equipment	<ul style="list-style-type: none"> • Interoperability with existing security controls, and with legacy LAN and WAN environments 	
4.	Protection of broadband Internet connection	<ul style="list-style-type: none"> • Protection of Internet-based VPN • Secure Internet access solution, bundled broadband connectivity, Web hosting 	
5.	Comprehensive managed security offerings	<ul style="list-style-type: none"> • May include consulting, implementation, management, and training services 	
6.	Consulting services	<ul style="list-style-type: none"> • Specialized knowledge of security functions 	
7.	Processes and procedures to manage threats and incidents effectively and quickly	<ul style="list-style-type: none"> • Specified response times for handling incidents • Real-time reports detailing incidents and threats 	
8.	Flexible, individual offerings and security service bundles	<ul style="list-style-type: none"> • Ability to expand out-tasked services as trust in managed service provider grows • Control over select security functions to maximize workflow, if needed • Cost-effective, end-to-end security solutions 	

Whatever your business size, managed security services can facilitate the implementation of your business strategy, as shown in Table 3.

Table 3 Out-Tasking Strategies

	Business Strategy	Managed Security Services
Enterprise business	Enhance current security operations to effectively mitigate potential security risks and attacks	<ul style="list-style-type: none"> • Managed firewalls • Managed intrusion detection services • Consulting on overall security policy and architecture
	Protect information flowing in and out of organization	<ul style="list-style-type: none"> • Authentication • Encryption • Public key infrastructure (PKI) • VPNs
	Proactively safeguard network	<ul style="list-style-type: none"> • Policies and technologies in place to secure network against current and future threats • Content security solutions (e-mail and Web scanning) • Intrusion detection • Vulnerability analysis
Small to midsize business	Extending Internet usage as a way of replacing or expanding existing WAN connectivity	<ul style="list-style-type: none"> • Managed firewalls • Virus scanning • Managed intrusion detection services

Financial Analysis

Providing continual network monitoring and protection by relying solely on in-house resources can burden resource allocations and budgets for organizations of all sizes. Out-tasking network security services to a managed security service provider can result in significant savings in ongoing management, as well as in implementation and training costs. It also enables in-house personnel to focus on core business competencies.

Consider, for example, the cost savings and benefits of out-tasking two high-priority network security services: intrusion detection and firewall services.

Organization: Enterprise with four IDS servers

Cost Savings: 75 percent in monthly recurring costs by out-tasking managed IDS services

Benefits: The reduced expenditure resulted in an increase in network reliability and monitoring, along with the flexibility to reallocate IT staff to strategic projects. In addition, the organization lowered implementation and training costs.

Organization: Enterprise with 9 sites and 2500 users

Cost Savings: 65 percent in monthly recurring costs by out-tasking managed firewall services

Benefits: Again, the reduced expenditure resulted in an increase in network reliability and monitoring, along with the flexibility to reallocate IT staff to strategic projects. In addition, the organization lowered implementation and training costs.

Ask your Cisco Powered Network managed service provider to help you calculate managed services security return on investment (ROI) with the Cisco ROI calculator.

CISCO POWERED NETWORK PROGRAM

Cisco Systems is the leader in enterprise networking, and small, midsize, and large businesses can enjoy the same reliability, scalability, and flexibility of network services by looking for the Cisco Powered Network designation when they choose to out-task these capabilities. Service providers with the Cisco Powered Network designation are committed to using end-to-end Cisco equipment in their networks and meet high standards of operational excellence and customer service and support. More service providers are offering their business customers managed security services based on Cisco solutions that include managed firewall, network- and premises-based VPNs, and managed IDSs.

Businesses have turned to service providers with the Cisco Powered Network designation to supply reliable, industry-leading out-tasked services that help enable advanced applications based on Cisco end-to-end network equipment and technology.

More than 375 of the most successful service providers around the world are members of the Cisco Powered Network program. Located in more than 56 countries, these program members offer a wide range of services—featuring networks built with Cisco products and solutions—for their small, midsize, and large business customers.

Service providers with the Cisco Powered Network designation are committed to using end-to-end Cisco equipment in their networks and meet high standards of operational excellence and customer service and support.

FOR MORE INFORMATION

To learn more about Cisco Systems solutions for business security, visit: <http://www.cisco.com> and <http://www.cisco.com/go/security>.

Please visit <http://www.cisco.com/go/managedservices> for information on other managed services, including:

- VPN services
- Business voice services
- Metro Ethernet services

CISCO SYSTEMS



Corporate 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: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
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

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

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or 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. (0402R)

DM/LW6137 04/04