

## Providing Managed Network Security Services FAQ Integrated Security Solutions from Cisco Systems

Q. What are managed security services?

A. Managed security services can range from services as basic as providing a firewall solution for a small company to comprehensive security lifecycle management for global enterprises. Service providers often tailor solutions that can be comprised of multiple capabilities including firewall management, virtual private networks (VPNs), intrusion detection solutions, virus scanning, Web site security assessments, 24x7 monitoring, applet scanning, content inspection, and URL blocking.

Q. What is the market size?

A. Even though overall IT spending is down, global security spending is up across every market segment and business size. Because companies of all sizes depend on their networks for vital daily operations, security has become a priority. And because the complexity of ensuring data and network security is rising, many companies—especially small and medium-sized businesses (SMBs)—do not have the expertise or resources to implement and manage solutions themselves.

For these reasons, outsourcing is expected to become a large source of revenue for service providers during the next few years.

The Yankee Group estimates that managed security service provider revenues will reach to almost US\$2.6 billion by 2005. (*Managed Security Services in Mid-2002: Alive, Kicking, and Evolving*, July 2002)

- According to the Gartner Group, security monitoring and management revenue will grow at a CAGR of 35 percent. About half of managed security installations are paid for up front with an average monthly recurring charge of US\$23,000. (Gartner Group, 2001)
- Large enterprises will likely continue to either manage their own security or work with large system integrators. (Gartner Group, 2001)
- Outsourced managed services are being adopted faster than security consulting and solution implementation services. (The Yankee Group, 2001)

Q. Which industries are good opportunities?

A. Market segments that will turn to outsourcing first include Financial Services, Manufacturing, Government, Healthcare, Utilities, and Communications. In addition, companies that rely on broadband communications tend to require more comprehensive security services.

- SMBs that currently use DSL or leased lines are more likely to plan security purchases over the next 12 months. SMBs that plan such purchases project higher IT budgets to cover the costs of such investments than SMBs with no plans to purchase security products.



- Financial, insurance, medical, and real estate markets represent good opportunities and plan to purchase security services because of requirements for data confidentiality. In some cases, the need for security is mandated by law; for example, the Health Insurance Portability and Accountability Act (HIPAA) of 1996 requires end-to-end encryption of data traveling between medical locations, thus encouraging the use of customer premises-based VPNs in that vertical.
- Financial, insurance, medical, real estate, and professional services also have a greater-than-average proportion of mobile workers, business travelers, and telecommuters who require secure access to home networks.

Q. Which companies represent the best opportunities?

A. The fastest growth is occurring among small companies. According to Infonetics (2002), this market will grow from approximately 25 percent of companies adopting managed security solutions in 2001 to almost 75 percent by 2006. Medium-sized companies' adoption rates will grow from about 20 percent to almost 45 percent by 2006.

Q. What managed services do customers need?

A. Small and medium-sized businesses want to be able to focus on their core competencies instead of having to dedicate staff to becoming experts in deploying and managing network security. They also want ensured reliability. According to Infonetics, the five most in-demand solutions for small and medium-sized businesses are:

- Virus scanning
- Firewall
- Authentication
- Encryption
- Network-based intrusion detection services
- Interest is also growing in VPN solutions

As the market for managed security services grows, however, businesses will increasingly combine multiple services for greater protection against threats. For example, a company may want virus scanning, firewall, and site-to-site VPN set-up and monitoring in one service.

The Yankee Group predicts rapid growth in managed intrusion detection services and also an increasing amount of revenue from security protection solutions that can be bundled with managed firewall solutions (*Managed Security Services in Mid-2002: Alive, Kicking, and Evolving, July 2002*).

Q. How are managed security services being priced?

A. According to the Yankee Group, (2001) average monthly charges for various services are:

Managed firewall	\$2000
High availability firewall	1800
URL scanning	300
Anti-virus	300
Intrusion detection	2500
Scanning service	500
IP VPN	500
Security Intelligence	2000



Q. What are the benefits to customers?

A. Small and medium-sized businesses have much to gain by outsourcing security solutions to trusted service providers. They can:

- *Ensure end-to-end secure solutions*—by outsourcing, companies can tailor services to meet specific security needs. They aren't limited to standalone point solutions that only cover portions of their information infrastructure.
- *Minimize security gaps*—protect network systems and data from intentional or accidental damage.
- *Gain flexibility and scalability*—often, the cost of expanding coverage or adding capabilities is cost-prohibitive for small and medium-sized businesses. Often it is far more cost-effective to outsource for specialized expertise than try to divert internal resources and do it themselves.
- *Better protect information assets while improving productivity*—service providers have the infrastructure, monitoring systems, and staff to deliver reliable security services. This frees the small business to focus on what it does best and improves its productivity.

Q. What is the Cisco integrated security solution comprised of?

A. Cisco integrated security solutions are based on secure, multiservice platforms for all market segments. Each Cisco solution enables VPN, quality of service (QoS), firewall, and intrusion detection features in addition to high-performance routing capabilities. Several platforms also enable secure voice and video capabilities with high QoS.

Specifically, Cisco is announcing:

- Enhancements to Cisco IOS<sup>®</sup> software
- New security routers for SMB, telecommuting, and CPE environments
- New VPN routers for integrating secure IP services
- New VPN modules for enhancing existing Cisco 2600, 3600, and 3700 routing platforms
- Catalyst 6500 VPN and Firewall Systems with integrated IP services

Q. Why are managed security services a good business opportunity?

A. As a service provider, the managed security services market represents a good opportunity for many reasons. The market need is growing rapidly, especially among customers who already subscribe to broadband services. Other advantages include:

*Low-cost, Fast Market Entry*

It costs much less to roll out new security services on top of existing infrastructure and using platforms that are already being managed. Cisco platforms already deployed can be easily upgraded, in some cases, or merely enabled, in others, to launch new revenue-generating value-added services. Time to market is also faster because it is not necessary to install new equipment in every POP, train technicians on new platforms, or build a new support infrastructure.



### *Market Advantage*

Cisco has the major market share among enterprise businesses, in some cases as high as 80 percent. These Cisco customers are already “pre-sold” on the value of choosing Cisco. When looking for a service provider, seeing the Cisco Powered Network designation gives enterprise customers a high comfort level because it means high quality, reliability, familiarity, and all the benefits of end-to-end networking. Cisco security solutions allow service providers to leverage a platform and brand that customers know and trust (Cisco IOS software) to perform multiple functions across their network infrastructure.

### *Annuity Factor*

Managed security services add value to existing customer installations, adding monthly revenue for service providers that increases profitability and reduces total cost of ownership for equipment deployed. Customers who gain the added value of security to their current services are more likely to remain loyal customers, longer.

### *Customizability for Market Penetration*

Cisco managed security solutions allow service providers to tailor and differentiate security services that meet each business customer’s needs. Now they can offer a fully integrated product solution with the flexibility to meet the unique needs of any network to maximize market penetration.

Q. How has Cisco IOS software been enhanced?

A. Cisco IOS software has been enhanced by adding advanced security features and additional resiliency. The advanced security features added to Cisco IOS software include:

- IDS Signature Enhancement—Cisco IOS software now supports 42 new intrusion detection signatures, both atomic and compound
- Up to 500 percent improvement in firewall and IDS performance
- New, Dynamic Multipoint VPN capabilities provide on-demand meshing in data or voice/video/data VPNs
- New software supports the latest Advanced Encryption Standard (AES)

Resiliency is improved as well to ensure that critical business applications are not lethally affected by security breaches. Sub-second stateful IP Security (IPSec) failover protects applications while dial back-up features on the new Cisco 830 Series routers ensure high VPN uptime for small offices and telecommuters.

Q. Which CPE routing platforms include the new security features?

A. New Cisco routers include advanced capabilities that are normally only found on large, high-end routing platforms. These capabilities ensure secure network services all the way to the edge of the network, enabling even the smallest businesses to take advantage of advanced IP services delivered by leading service providers.

### *Cisco SOHO 90 Series*

Cisco Small Office Home Office (SOHO) 90 routers deliver outstanding routing performance and support dual Ethernet connections. They include an integrated firewall, a four-port 10/100 switch, IPSec VPN capabilities, out-of-band management, and dial backup. The SOHO 97 additionally is optimized for ADSL broadband connectivity.



### *Cisco 830 Series*

Cisco 830 series routers deliver the same features as the SOHO 90 series plus integrated intrusion detection with URL filtering, hardware-accelerated VPN capabilities, and QoS for voice and video traffic. The Cisco 837 is also optimized for ADSL broadband connectivity.

Q. What about deploying integrated security features on already-installed CPE routers?

A. Cisco has also introduced new acceleration modules for Cisco 2600, 3600, and 3700 series branch routers. These modules can increase VPN throughput by five to ten times while decreasing CPU utilization by half. Support for the new AES encryption standard is also integrated in addition to Layer 3 compression. Acceleration modules can increase bandwidth at branch offices, enable businesses to take advantage of new managed services, and enhance the value of already-deployed access routers.

Q. How does this affect Catalyst switching platforms?

A. Versatile Cisco 6500 Catalyst switches can now be expanded with a range of high-capacity modules that include VPN and security features. A new firewall service module can support 100,000 connections per second with a throughput capacity of 5 Gbps. The Cisco Catalyst 6500 chassis can support up to four modules for a total throughput capacity of 20 Gbps. The module also supports stateful failover for increased resiliency. A new VPN service module will support up to 8000 simultaneous tunnels and encrypted throughput of 1.9 Gbps. Now, businesses can further leverage their investment in Catalyst switching equipment to improve security and integrate with managed security and VPN services.

Q. When are the new routers and Cisco IOS software enhancements available?

A. Cisco integrated security solutions are available today.

For more information about Cisco Integrated Security Solutions, visit: [www.cisco.com/go/security](http://www.cisco.com/go/security)



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.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
www.cisco.com  
Tel: +65 317 7777  
Fax: +65 317 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 Web site at [www.cisco.com/go/offices](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia  
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

All contents are Copyright © 1992-2002, Cisco Systems, Inc. All rights reserved. CCIP, the Cisco Arrow logo, the Cisco Powered Network mark, the Cisco Systems Verified logo, Cisco Unity, Follow Me Browsing, FormShare, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ logo, iQ Net Readiness Scorecard, Networking Academy, ScriptShare, SMARTnet, TransPath, and Voice LAN are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That's Possible, The Fastest Way to Increase Your Internet Quotient, and iQuick Study are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherSwitch, Fast Step, GigaStack, Internet Quotient, IOS, IP/TV, LightStream, MGX, MICA, the Networkers logo, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, RateMUX, Registrar, SlideCast, StrataView Plus, Stratum, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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.  
(0208R) KW/LW3840 1102