

Managed Security Services



Executive Summary

As corporations of all sizes embrace e-business strategies, they have become increasingly concerned about the security implications of the Internet. The deployment and management of security and virtual private network (VPN) solutions requires a highly skilled technical staff and sufficient time to implement a focused and disciplined approach. In today's fast-paced world of information technology (IT), these solutions can be precious or nonexistent resources. Consequently, many organizations are exploring outsourcing solutions for all or part of their security infrastructure.

Fortunately, an increasing number of service providers are offering managed security services to enterprise customers. Services based on Cisco Systems solutions include managed firewall, managed VPN (network based and premises based), and managed intrusion detection. For recent examples of commercially available services, refer to <http://www.cisco.com/go/managedsecurity>.

Cisco is the leader in enterprise networking, and providers recognize that Cisco security solutions offer them a competitive differential advantage. Managed services based on Cisco technologies allow end customers to migrate to new deployment models, while preserving their confidence with trusted solution sets. This is especially important as many enterprises increase their dependency on managed services and move from the pilot phase to broad deployment. Cisco branded solutions are uniquely positioned to offer a competitive selling advantage to providers who standardize on them.

Today, established providers are deploying second- or third-generation solutions. In addition, a new breed of managed service providers has emerged. Specializing in one or more service delivery areas, managed service providers (MSPs) might offer leading-edge options for business end customers or traditional service providers who bundle or private label the services for resale to their installed bases.

Cisco Systems recognizes that service providers need more than point products. As a result of the sweeping introduction of services hitting the market, new programs have been established to augment existing programs and to help managed service providers meet customer demand and successfully deploy solutions in today's rapidly changing environment.

In general, participation in these programs offers the following benefits:

- Enhanced credibility with enterprise customers through affiliation with Cisco
- Expanded customer penetration by leveraging Cisco installed base
- Comarketing resources



The benefits to enterprises that procure services through affiliated partners include:

- Confidence that outsourcing partners are using industry-standard technology
- Quick and easy deployment of security services
- Lower infrastructure investment

Managed Security Services Market

The managed security and VPN market is constantly evolving. As new products and service providers enter the market, business customers have an increasing number of options.

The many compelling reasons for corporations to consider managed security services include the following key benefits:

The Top 10 Reasons Companies Outsource	
<p>#1 <i>Improve company focus</i>—Companies can focus on broader business issues while outside experts assume operational details</p> <p>#2 <i>Access to world-class capabilities</i>—By the nature of their specializations, outsourcing providers bring extensive capabilities to meet the needs of their customers</p> <p>#3 <i>Accelerate reengineering benefits</i>—Companies immediately realize the anticipated benefits of reengineering by having an outside organization – one that has already reengineered to world-class standards – take over the process</p> <p>#4 <i>Share risks</i>—Outsourcing providers make investments on behalf of their many clients, not on behalf of just one company</p> <p>#5 <i>Free resources for other purposes</i>—Organizations can redirect resources from noncore activities to activities that have greater customer-service return</p>	<p>S T R A T E G I C</p> <p>Long Term</p>
<p>#6 <i>Make capital funds available</i>—Outsourcing reduces the need to invest capital funds in noncore business functions</p> <p>#7 <i>Cash infusion</i>—When outsourcing, assets are often transferred from the customer to the provider. Equipment, facilities, vehicles, and licenses used in current operations are sold to the vendor</p> <p>#8 <i>Reduce and control operating costs</i>—Access to the outside provider's lower cost structure, the result of a greater economy of scale, is one of the most compelling tactical reasons for outsourcing.</p> <p>#9 <i>Resources not available internally</i>—Outsourcing is a viable alternative to building the needed capability from scratch</p> <p>#10 <i>Function is difficult to manage</i>—Assuming the company understands the requirements, outsourcing can address difficult-to-manage functions</p>	<p>Short Term</p> <p>T A C T I C A L</p>

Source: The Outsourcing Institute



Business Opportunity for Managed Security Services

Many analysts believe that managed security and VPN is one of the hottest areas in networking today. This section highlights some of the general market predictions in this area.

In 2000, the Yankee Group had this to say:

“Managed security services is projected to be one of the fastest-growing information sector markets over the next several years. Logically, the pre-implementation market can be broken out according to the type of service offering. Some firms offer preimplementation managed services, such as penetration testing, vulnerability assessment scanning and Internet and perimeter security evaluations. Other firms implement technological solutions and services based on initial assessments. Still others offer ongoing monitoring and management of products after their implementation. Many service providers offer various combinations of the three services or partner with other providers outside of their core competencies.”

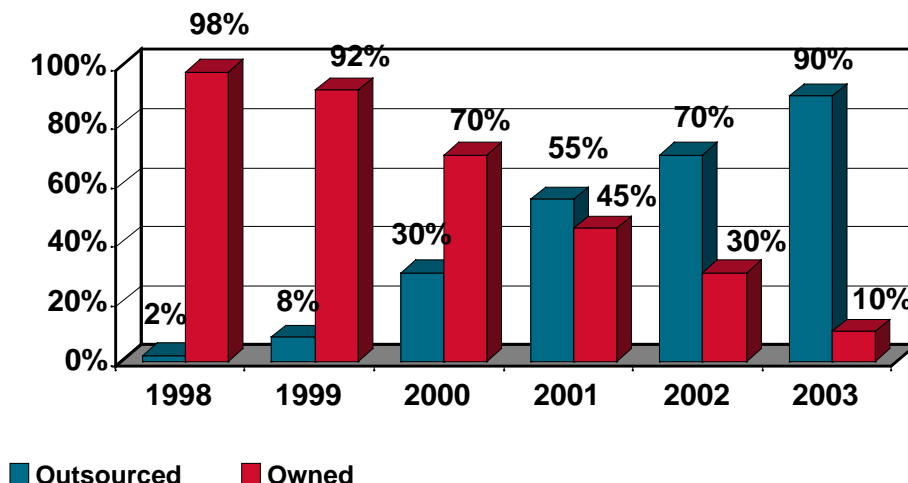
In the January 2001 issue of *Information Security Magazine*, Edmund Dejesus said, “The managed security services market is growing fast for both large and small enterprises. The market for the former is (and will remain) larger than that for the latter. According to The Yankee Group, the large enterprise market is expected to grow from US\$268 million in 2000 to nearly US\$1.2 billion in 2005.

One explanation for this rapid growth is that more and more Fortune 1000 firms with established security programs are outsourcing firewall or VPN management to free up technical resources for more complex or security-sensitive projects, such as Web access control, security policy management, directory services or public-key infrastructure (PKI).

While overall managed services revenue for small- to medium-sized businesses is less than that for large enterprises, growth projections are just as strong—from a little under US\$50 million in 2000 to US\$637 million in 2005, according to The Yankee Group.”

Business Opportunity for Managed VPNs

Businesses of all types deploy VPNs today. Over time, Cisco expects that incremental capacity and new installations will be deployed as managed services. In 1999, Cahners In-Stat predicted the trend toward outsourced services illustrated in the following chart:



A year later, the trend, if not the absolute percentages, seems to hold true. According to IDC, "Our 2000 WAN Manager Survey results for IP VPN services show very interesting and significant changes over last year's results. IP VPNs are more common, more accepted, and more often ordered through a carrier than an in-house solution, which was very prevalent in 1999. IP VPNs have entered the mainstream of WAN options." IP VPN Services: A Demand-Side View, IDC, December 2000

The available market for these services is compelling. "The IP virtual private network (VPN) services market for U.S.-based carriers will grow rapidly, from US\$1.28 billion in 2000 to almost US\$10 billion in 2005, for a compound annual growth rate (CAGR) of 51 percent in that time period. This rate of growth makes IP VPNs one of the fastest-growing segments of the IP telecommunications market." IP VPN Services: U.S. Market Forecast and Analysis, 2000-2005, IDC December 2000

Vendor Selection—Success Breeds Success

Only Cisco offers the complete range of product solutions for delivering managed security services. Enterprises that manage their own security infrastructure place their trust in Cisco. Consequently, Cisco is a market share leader in firewall, VPN, and intrusion detection.

In many cases, these Cisco customers represent the target accounts for service providers that offer managed security services. Providers that offer Cisco-based services will enjoy greater market acceptance and sales penetration.

"Cisco maintains its lead with 79% market share in the Total VPN market."

Infonetics Research, November 2000

"Cisco expands its lead as market leader in VPN gateways by increasing to 30% of the market." *Synergy Research Group, November 2000*

"Cisco solidifies its lead in the VPN router segment with 92% market share."

Infonetics Research, November 2000

In the firewall market, "Cisco widens its lead with 47% of the total worldwide market share in Q3CY00." *Infonetics Research, November 2000*

"As they continue to expand IDS into their core networking products, Cisco will be one of the primary players in the networking IDS segment."

IDC December 2000

Cisco Solutions for Managed Security Services

As corporations continually expand their mission-critical networks with new intranet, extranet, and e-commerce applications, network security technologies are becoming increasingly vital in preventing corruption and intrusion, and eliminating network security vulnerabilities. Without the proper safeguards in place, organizations could experience major security breaches, resulting in serious damages or losses. With the heightened importance of network security, more companies are looking to service providers for easy and reliable access to advanced security technologies and expertise, and to offload management functions so that they can focus on their core competencies.

Cisco provides a comprehensive suite of network security solutions, allowing service providers to meet the security requirements of any customer.

Managed VPN

IP VPN is rapidly becoming the foundation for the delivery of new world services. Along with well-known services such as access VPN, intranet VPN (site-to-site), and extranet VPN, providers today are offering value-added IP-based applications atop their VPN transport networks. Two unique and complementary VPN technologies, IP security (IPsec) and Multiprotocol Label Switching (MPLS) enable providers to deliver VPN services. Service providers can choose one or the other, or both of these technologies, based on customer demand and network design requirements.

For more information on Cisco VPN solutions, visit: <http://www.cisco.com/go/vpn>

For more information on Cisco VPN products, visit: http://www.cisco.com/warp/public/44/jump/vpn_devices.shtml

Managed Firewall

The Internet's growth has resulted in increased security risks to corporate and government networks. Existing solutions such as proxy-based firewalls that run at the application level have many limitations, including slow performance, the need for high-end, costly, general-purpose platforms running a UNIX operating system, and the security risks inherent in using an open system such as UNIX. The Cisco PIX[®] Series Firewall overcomes these limitations with its unique combination of high performance and strong security, backed by the Cisco worldwide 7x24 service and support organization.

Managed service providers might also offer router-based services using the Cisco IOS[®] Firewall. This add-on module to Cisco IOS Software is available for a wide range of Cisco routers and switches. It enables advanced firewall capabilities and intrusion detection and authentication, allowing service providers to bolster IOS router functionality with advanced security services.

For more information on Cisco PIX Firewall, visit: <http://www.cisco.com/warp/public/cc/pd/fw/sqfw500/>

Managed Intrusion Detection

The Cisco Intrusion Detection System (IDS) market-leading products detect unauthorized activity traversing the network, respond to such activity, and send alarms back to a management console. An array of Cisco IDS components is available to match any managed customer environment or service provider infrastructure.

For more information on Cisco IDS, visit: <http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz>

The Importance of Ecosystems

Ecosystem partnerships allow Cisco to offer comprehensive solutions to its customers. This philosophy extends to service partners and technology partners. Ecosystem partners benefit by taking advantage of the market reach of Cisco and its immense installed base.

For more information on Cisco ecosystems, visit:

<http://www.cisco.com/warp/public/779/servpro/programs/ecosystem/>

<http://www.cisco.com/warp/public/779/largeent/partner/esap/>

Programs for Managed Service Providers

Two marketing programs are highlighted here. As extensions of well-established programs with a proven track record of success, they are the latest additions in the Cisco drive towards excellence in ecosystem development.

Cisco Powered Network Managed Security

The popular Cisco Powered Network program is being extended to offer managed security services from qualified and knowledgeable service providers. This new service category complements the existing and well-established VPN services category in the program. The new designation highlights Cisco Powered Network service providers that offer managed security services based on the Cisco industry-leading VPN firewall and intrusion detection products.

For more information on the Cisco Powered Network Program, VPN, and Managed Security Services, visit

<http://www.cisco.com/go/cpn>

Cisco AVVID Partner Program

The Security and VPN Solutions category under the recently announced Cisco AVVID (Architecture for Voice, Video and Integrated Data) Partner Program is of particular interest to providers who deliver managed security and VPN services.

The Security and VPN Solutions category has two components: The Service component is for providers who offer managed services, and the Product component is for third-party vendors who offer complementary solutions to the Cisco portfolio. These products are appropriate for enterprises that are deploying their own security infrastructure, or service providers who are delivering managed security and VPN offerings.

Security Services

The Security Services umbrella provides eight offerings to assist enterprises in fortifying their networks:

- Design and Implementation Services
- Policy and Procedures Services
- Vulnerability Assessment Services
- Business Impact and Risk Assessment Services
- Application and Code Review Services
- Competitive Counter-Intelligence Services
- Outsourced Monitoring and Management Services
- Incident Response Services

The Outsourced Security Monitoring and Management Services category is particularly designed to help partners provide best-in-class managed security services to enterprise end customers.

Partners in the Outsourced Security Monitoring and Management category might offer services such as alarm and incident tracking. Others might provide complete turnkey services for deployment, management, and maintenance of customers' security and VPN infrastructures.

Security and VPN Solutions (products)

Cisco AVVID partners who provide third-party products help Cisco deliver comprehensive security solutions. This program provides interoperability and integration validation as deemed appropriate.

The product categories for Security and VPN Solutions are:

- Identity solutions—including authentication, authorization, and PKI solutions such as smart cards, hard and soft tokens, authentication servers, and certificate authority servers
- Application Security solutions—which include server and host protection applications
- Perimeter Security solutions—including URL filtering and e-mail and virus-scanning applications

- Security Monitoring and Management solutions—including products that support syslog analysis, event analysis, reporting, and secure remote administration
- Secure Connectivity solutions—including products such as VPN client software and wireless VPN products

For more information on the Security and VPN Solutions of the Cisco AVVID Partner Program, refer to <http://www.cisco.com/go/securitypartners>

Additional Resources—The VPN and Security Business Unit (VSEC)

In early 2000, Cisco formed a business unit for developing and marketing a strategic portfolio of security products. These products include the Cisco PIX Firewall, Cisco 7100 VPN Router, and Cisco VPN 3000 Series Concentrator.

A service provider marketing team was established to assist all types of providers in designing and deploying managed security services. This assistance can be especially useful while pursuing entry into one of the established programs.

Service providers and technology partners can contact this team for the following services:

- Guidance on security products manufactured by VSEC or affiliated products in the security and VPN area
- Navigation of related resources and programs at Cisco Systems

For more information, send e-mail to managedsecurity@cisco.com. A field marketing representative will review your inquiry and reply promptly.

For more information on the topics discussed in this data sheet, visit: <http://www.cisco.com/go/managedsecurity/>

Conclusion

Corporations of all sizes are concerned with the challenges of managing a security and VPN infrastructure. Many organizations are looking for outsourced solutions.

Cisco is embracing managed security services as a way to add value to its service provider partners and their enterprise end customers. Commercial services for managed firewall, VPN, and intrusion detection are becoming readily available worldwide.

Providers that offer these services can be traditional carriers, tier 1 ISPs, competitive local exchange carriers (CLECs), regional providers, specialty players, or the new breed of managed service providers. Cisco is adapting to the evolving service delivery requirements of each of these constituencies by offering a broad range of programs.



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 Europe
11, Rue Camille Desmoulins
92782 Issy Les Moulineaux
Cedex 9
France
www.cisco.com
Tel: 33 1 58 04 60 00
Fax: 33 1 58 04 61 00

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 Australia, Pty., Ltd
Level 17, 99 Walker Street
North Sydney
NSW 2059 Australia
www.cisco.com
Tel: +61 2 8448 7100
Fax: +61 2 9957 4350

Cisco Systems has more than 190 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco.com Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China • Colombia • Costa Rica • Croatia • Czech Republic • Denmark • Dubai, UAE
Finland • France • Germany • Greece • Hong Kong • 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 © 2001 Cisco Systems, Inc. All rights reserved. PIX is a trademark, and Cisco, Cisco IOS, Cisco Systems, and the Cisco Systems logo are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries. All other brands, names, or 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. (0102R)