



The Managed Security Services Opportunity

Executive Summary

Security is a sophisticated challenge for businesses and consumers alike. The increasing number of vulnerabilities and threats to communication systems is driving the rapid evolution of security technologies (see Exhibit 1). However, most enterprises and consumers do not have the expertise, funds or rapid response capabilities necessary to deal effectively with these problems. Businesses need highly specialized, knowledgeable and trained staff to properly deploy and manage their security solutions. Consumers are also encountering an increasingly wide range of security threats and attacks against their PCs and mobile and handheld devices. By building and deploying managed security services, service providers will enable their customers to focus on their core business and let experts take care of their networks, systems and devices.

Exhibit 1

Security Incidents Continue to Affect Businesses of All Sizes

Source: Yankee Group, 2006

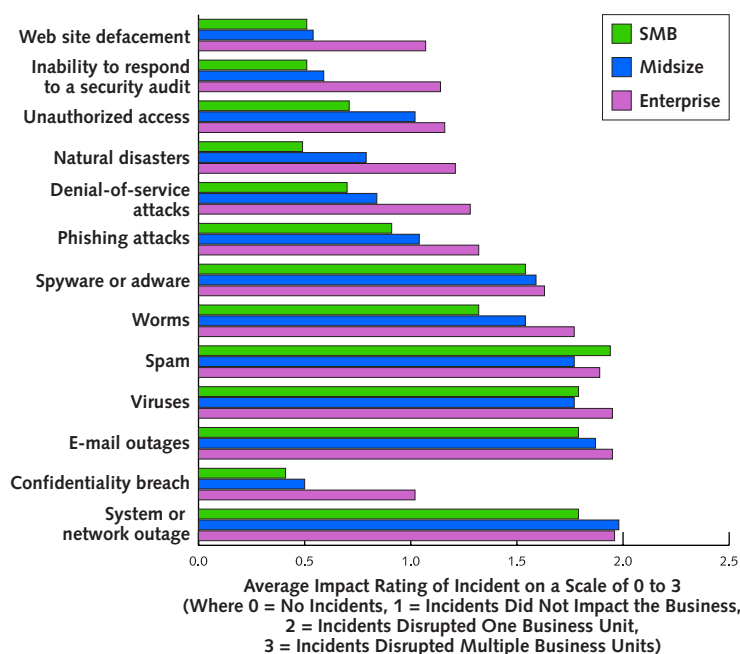


Table of Contents

I. Introduction	2
II. Market Overview	2
MSS Segment Overview	3
III. How Demand Is Driving the MSS Market	4
Enterprise and SMB Drivers of Managed Security	5
Consumer Drivers of Managed Security	5
IV. Market Impact from the Supply Side	6
V. Conclusions	7
Recommendations	7

I. Introduction

Enterprises and consumers face an enormous task in securing their data. Many enterprises, small and medium businesses (SMBs) and consumers do not have the expertise, funds or rapid response capabilities necessary to deal effectively with this problem. Not only must they have the expertise to install their anti-virus, firewall and intrusion detection and prevention solutions among others, but they have to make them interoperate, maintain patches and updates, and monitor these solutions. Additionally, the growing use of mobile devices and services for business and personal uses is introducing new threats and solutions to consider. End users must stay on top of the latest technologies designed to protect them in different areas of their network and endpoints, and implement them to their fullest capacity.

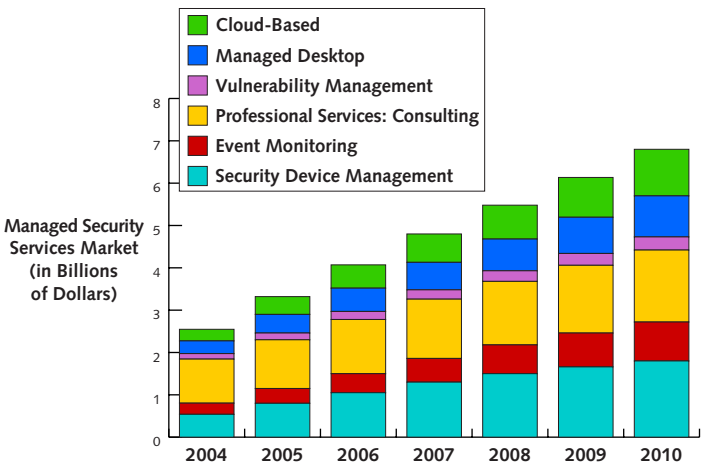
Logically, service providers are well positioned to address these challenges in the marketplace because of their ability to quickly roll out solutions and leverage their existing relationships with corporations and consumers. The challenge for service providers is to build services that are in high demand to generate profitable revenue yet flexible enough to meet the broad array of customer needs. In this Report, Yankee Group analyzes the supply- and demand-side drivers of the managed security services (MSS) market.

II. Market Overview

As security threats continue to evolve and become more sophisticated, businesses and consumers find themselves losing the battle against security breaches. Because service providers have an established services model including various ancillary services and an installed customer base, offering security services is a natural fit. Yankee Group estimates the 2006 managed security services market is approximately \$4 billion, including consulting and professional services revenue (see Exhibit 2). We expect the market to have a compound annual growth rate (CAGR) of 14% from 2006 through 2010.

Exhibit 2
Managed Security Services Market Forecast

Source: Yankee Group, 2006



MSS Segment Overview

The managed security services market consists of the following main segments:

- **Managed perimeter devices** are a core element of an outsourcing deal. They are frequently the first security functions that customers outsource. Firewalls continue as the majority of devices under management while IDS, IPS, VPN, perimeter anti-virus, authentication tokens and URL filtering are available as optional services. In 2006, we expect managed IDS and IPS to gain in popularity as customers look to reduce labor-intensive functions. Pure-play managed security device services are growing at a 15% rate by revenue. The aggregate number of devices under management grew 50% in 2005.
- **Managed messaging security** addresses a critical component of a business: the protection of a company's e-mail platform. With the growing prevalence of spam, e-mail-spread viruses, worms and phishing, the need for complete solutions that address these and any future threats is rapidly increasing and a security breach could cause catastrophic impact to a business.
- **Managing desktop security** is still an area of pain and expense for businesses. Several trends point to above-average growth in this segment during the next 5 years:
 - **The technology available to combat malware has multiplied.** Anti-virus is no longer enough; personnel firewalls, anti-spyware and perhaps host intrusion prevention are also needed.
 - **The technology for reaching and managing thousands of nodes is also vastly improved.** For example, better patch and configuration management and new standards for network access zoning can enforce policies for endpoints.
- **Vulnerability management services** are perhaps the most at-risk segment of the MSS landscape given technology trends. The need to scan both external and internal devices is strong and driving growth in database and web scanning markets. Technical and organizational challenges exist with the scanning of internal systems. Internal systems cannot be scanned without customer-premises equipment (CPE). Conversely, at the perimeter, scanning software is commoditized and the process for providers largely automated. As a standalone product or service, vulnerability scanning is at risk.
- **Cloud-based security services** include e-mail filtering services, non-premises firewall, IDS, IPS and denial-of-service (DoS) attack services. Yankee Group defines a cloud-based service as a service that does not require premises equipment but also leverages a provider's shared infrastructure. Service providers can leverage the shared infrastructure to greatly improve and enhance the security service delivered. Benefits to the customer include the reduced need for CPE devices and improved QoS/performance at the application and network levels. Cloud-based services offer the best protection against distributed DoS attacks, which are the most prevalent internet-originated type of attack.
- **Mobile security** is still a rather new area of focus in the marketplace although mobile security for the enterprise market is slightly more advanced than for the consumer. Currently many corporations and providers treat mobile devices as any other endpoint device, hence folding security management into the broader security management solution for the business. Moving forward, this approach may no longer be sufficient to protect a corporation's or consumer's content and data. In the longer term, this segment will become an increasingly focused area of security and growth for service providers.
- **Monitoring and intelligence services** are common additions to service contracts that initially included only managed devices. Providers are adding value to existing customers by integrating these services into bundled offers for managed and monitored devices. The trends in security driven by regulatory needs have also placed significant emphasis on monitoring and reporting. This segment will continue to grow even after the managed devices segment has petered out because the need for monitoring will remain a strong driver and differentiator.

- **Professional services** have long been a core need for enterprises in the security arena. Service providers are adding value for existing customers by offering professional services for free as part of the initial setup of a managed service. For example, professional services are commonly offered as part of a managed device contract. For example, the provider will conduct an initial review of existing firewall rules and make recommendations.

The trends in security driven by regulatory needs also have placed significant emphasis on risk assessment, auditing and security of internal applications and databases. To meet the increasing regulatory requirements, businesses must turn to consultants for guidance. Through consulting and professional services offerings, service providers can aid customers in achieving regulatory compliance.

Security is a rapidly developing area of technology. The breadth of services capable of being offered as a managed security service continues to increase as well. By purchasing from external service providers, buyers can gain quicker access to additional features and apply them more consistently at scale.

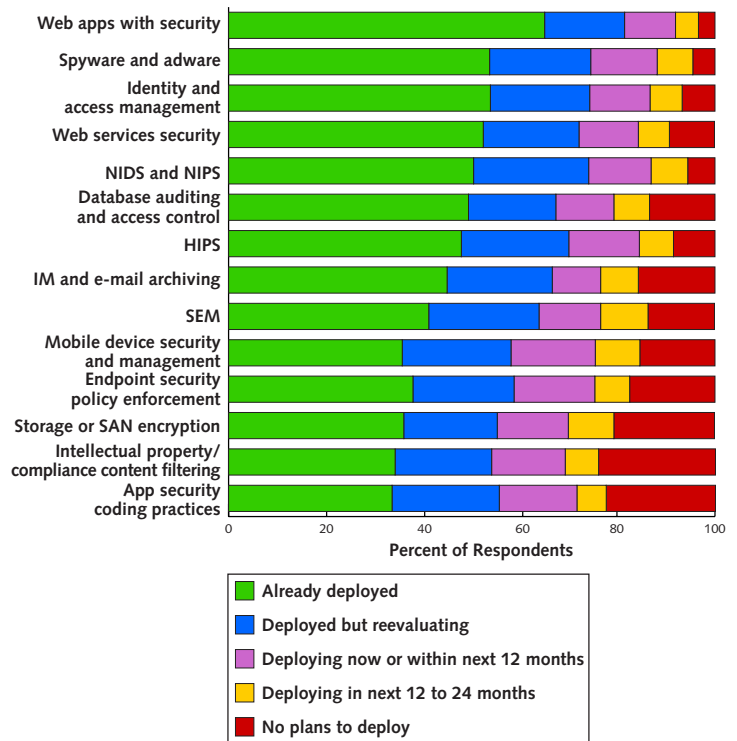
III. How Demand Is Driving the MSS Market

Security breaches are a big problem for organizations. When a business loses control of confidential records or is forced to shut down unexpectedly, the impact on profits, shareholder equity, partners and employee productivity can be catastrophic. Adopting a strong security strategy that safeguards essential business operations and information is critical to a business' long-term success. System, network and e-mail outages are some of the most disruptive to businesses. To combat these threats, enterprises are deploying an increasing number of security products and services (see Exhibit 3), but many are still skeptical of the impact of these offerings.

Companies have installed multiple layers of network security perimeter defenses, including firewalls, VPNs, IDSs and anti-virus software. These additional layers can make management of the security that much more difficult and add to an enterprise's operational costs. However, the Achilles' heel for nearly every enterprise remains the potentially exploitable vulnerabilities that these measures do not address. Unpatched, outdated and misconfigured software are the choice targets of hackers. A continuous assessment of external and internal network and application infrastructures is necessary to identify vulnerabilities and mitigate them in a timely manner. This has all been very expensive and not proven successful in mitigating vulnerabilities.

Exhibit 3
Enterprises Continue to Deploy Security Solutions

Source: Yankee Group 2005 Security Leaders and Laggards Survey



Enterprise and SMB Drivers of Managed Security

Corporations are aggressively increasing their outsourcing of security services and will increasingly turn to managed security service providers (MSSPs). Their challenge is to create the end-to-end coverage necessary to effectively secure the corporation. Three main drivers are pushing enterprises and businesses to external service providers for help in managing security threats:

- Increasing distribution of IT assets across geographically dispersed operations
- Increasing sophistication and proliferation of security threats
- Lack of adequate training to tackle the problem internally

Many of the key drivers for selecting a service or service provider remain the same for *Fortune 500* companies and individual consumers. Simplifying or improving processes and daily life typically are at the top of the list. Potential customers ask outsourcers whether they will accomplish at least one of these three things:

- Will managed services reduce the time that the organization spends on tactical security issues, allowing it to focus on more strategic areas of the business?
- Will the security of my environment be better and more secure as a result of my service provider managing it?
- Will the use of a managed security service reduce my overall costs associated with achieving a secure environment?

By purchasing managed security services, enterprises can gain valuable help on several fronts. Security outsourcing can reduce stress for a besieged IT staff, fill in competency voids, aid in regulatory compliance and give enterprises a third-party view of how secure their organizations really are. Transparency on both sides allowing fluid communications is key to maximizing the effectiveness of a managed service and delivering benefits to the business and provider while paving the way for expanding the customer/provider relationship. With on average 20% of their IT budgets going to security, businesses need to be confident that their money is really protecting their business.

Many large businesses have acquired a heterogeneous environment, which makes economic scaling of consistent security across the environment impossible. Security to a corporation goes beyond traditional point solutions and is becoming increasingly about comprehensive offerings centered on security architecture, governance and flexibility. We also expect, over the next 3 years, to see acceleration in the market demand because of wireless adoption. Providing security to untethered devices and the mobile environment will be a key area for developing and extending services.

To meet the evolving needs of business customers, as a result of regulatory drivers, mobility drivers and business drivers, MSSPs will need to offer services that are much more robust. Offerings must help businesses reduce and manage risk, keep pace with change and improve IT management effectiveness.

Consumer Drivers of Managed Security

Selling to the consumer market requires a different value proposition than when targeting businesses. Technology and internet-based communications (VoIP), services (on-demand digital music and video) and connectivity (Wi-Fi, VPN) are strong areas of interest for consumers and their interest will only increase. As the consumer market for information technology grows aggressively, consumers are, on average, less technically capable of managing their own security and more in need of external expert services to manage their environments.

Like businesses, consumers are facing a wide range of security threats and attacks against their PCs and mobile and handheld devices. Yankee Group estimates there will be 49.7 million US residential broadband households and 109.2 million residential broadband users by the end of 2006. For broadband service providers, now is the time to begin integrating applications and services into high-speed offerings. Younger broadband users are looking for broadband content. If broadband service providers (BSPs) do not offer entertainment applications and services (music, video, interactive gaming), these users will go elsewhere—thereby disintermediating BSPs and accelerating commoditization of high-speed internet access.

Although the public has not focused on mobile security as much as broadband or wireline security, the focus on and desire for security solutions by mobile consumers is expected to grow over the coming years. Yankee Group estimates there will be more than 177 million consumer mobile users in North America by the end of 2006 with an estimated 699 million consumer mobile users in EMEA. As these users continue to increase their dependence on mobile devices, secure content management will become a priority and service providers need to have valuable solutions to offer their customers or risk increasing customer churn.

The need for a real-time response to new threats and for solutions that address threats before entering the consumer’s environment is increasingly driving consumers to their service providers for relief. For many consumers, the only point of continuous contact with a technology provider is their service provider, especially their broadband service provider. We expect this trend to continue to gain momentum. Service providers must continue to increase their service offerings to reduce churn and drive customer satisfaction.

IV. Market Impact from the Supply Side

During the next 3 years, managed security service providers will experience acceleration in market demand. To capitalize on this demand, providers need to offer their customers value-added services that can stop the latest security threats before they affect the network, computing infrastructure or mobile devices.

Businesses increasingly recognize the complexity of security threats and—therefore—the value of managed services. For example, in the Yankee Group 2005 Security Leaders and Laggards Survey of 500 businesses, managed services attracted an increasing level of interest and penetration across many areas of security.

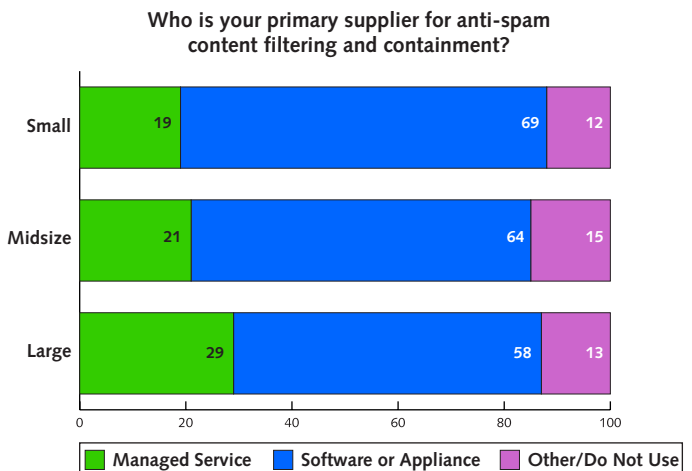
Exhibit 4 illustrates the type of supplier businesses turn to for anti-spam content filtering and containment by size of business. Additionally, when we aggregate the survey data, managed vendors take two of the top five slots in terms of primary supplier—demonstrating that managed services show increased traction.

Service providers in the managed security space need to maintain margins in the face of increasing competition, coupled with the maturation of some security technology. As providers standardize approaches to address security threats, differentiation will move toward effectiveness and efficiency of delivery. Clear communication using portals, well-defined service agreements and business processes will give customers greater visibility into the effectiveness of managed security service providers. This provides the customer with a clear understanding of the service’s return on investment, and the risk and cost reduction achieved through a managed service.

Service providers should look to partner with clear leaders in the security space as they develop and enhance their managed security solutions. Service providers bring to the table an installed customer base that will appeal to many pure security vendors. Managed security contracts typically don’t last more than 1 to 3 years. Therefore, providers need to focus on achieving the things that are most important to customers—single billing, single point of contact, flexible service options and higher levels of customer service—whether they are providing the services directly or through partnerships.

Exhibit 4
Supplier Preferences for Anti-Spam, Content Filtering and Containment by Business Segment

Source: Yankee Group 2005 Security Leaders and Laggards Survey



V. Conclusions

The demand for managed security services is only increasing. For too long, large and midsize businesses as well as consumers could not afford the cost of sophisticated security solutions. Consequently, end users were forced into one of the two leading alternatives: internal management or no action. By adopting managed security services, corporations will free up financial resources for investment into additional managed services.

Service providers in this space need to maintain margins in the face of increasing competition coupled with the maturation of security technology. With more standardized approaches for addressing security threats, differentiation is moving toward effectiveness and efficiency of delivery. Some security threats are changing rapidly and the industry is addressing those challenges with software and services. The best opportunities for provider differentiation are in rapidly evolving areas of threat mitigation. MSSPs aiming to establish thought leadership and differentiation must develop a robust software and professional services strategy.

Recommendations

- **Provide a robust security solution now.** The cost of downtime, regulatory noncompliance and information loss is higher than ever and the cost of implementing a managed security service has aggressively dropped in recent years. Given these shifting cost dynamics, enterprises need to implement managed security services that were once relevant for only the most sensitive cases.
- **Include a security component in consumer bundles.** Secure content and privacy protection are growing increasingly important to consumers. Service providers must be able to address these concerns through both mobility and broadband product bundles.
- **Partner to provide security and telecommunications services.** Companies benefit from service providers that offer both managed security services and telecommunication services. These partners can assist in the design of complex security solutions at lower price points.
- **Highlight the advantages of managed security services in your marketing material.** Business needs and security solutions are changing rapidly. Positioning skill sets and services to meet rapidly changing business requirements will likely be futile. Highlight how contracting with a managed security service provider enables businesses to be flexible and scalable to change with the times.
- **Evaluate the true total cost of security for businesses.** Businesses that have purchased S-BPO solutions, such as REPS and vulnerability management solutions, should reevaluate the TCO of providing these services internally. If internal analysis finds duplicated outsourced services efforts, then the enterprise should invest in extending its existing BPO engagements and look for additional value-added services from outsourcers.
- **Be clear about all complex professional services as part of managed service engagements.** It's critical to openly discuss the professional services engagement and define parameters such as length of project, pricing and pricing adjustments, and what customers will and won't receive after the completed implementation. Define the risks and benefits to the enterprise.
- **Deliver services as promised.** The level of service enterprises are purchasing is generally higher than what enterprises can deliver with their own in-house staff. But providers should not assume that will be readily apparent. Verify that technical capabilities and resources to deliver services exist and find reference customers who can attest publicly to SLA adherence. For example, if an organization's IT staff requires a provider to patch 90% of systems within 5 business days, the provider must show that it is delivering on that promise.
- **Present yourself as a security partner, not a security staff replacement.** Yankee Group believes that security should be a core competency for all enterprise IT departments. We recommend that enterprises work with MSSPs to complement internal staff so the latter can focus on core business areas that need heightened security or are under stricter regulatory watch.

Yankee Group

Yankee Group has research and sales staff located in North America, Europe, the Middle East, Africa, Latin America and Asia-Pacific. For more information, please contact one of the sales offices listed below.

Corporate Headquarters

31 St. James Avenue
BOSTON, MASSACHUSETTS 02116-4114
T 617.956.5000
F 617.956.5005
info@yankeegroup.com

EMEA

55 Russell Square
LONDON WC1B 4HP
UNITED KINGDOM
T 44.20.7307.1050
F 44.20.7323.3747
euroinfo@yankeegroup.com

North America

200-260 Terence Matthews Crescent
OTTAWA, ONTARIO K2M 2C7
CANADA
T 613.591.0087
F 613.591.0035
canadainfo@yankeegroup.com

Decision Services

Yankee Group Decision Service annual memberships offer clients access to research and one-to-one expert guidance.

Decision Services represent our best value for clients. The services help our members understand industry, regulatory, competitive and market-demand influences, as well as opportunities and risks to their current strategies.

Membership includes an invaluable in-person strategy session with Yankee Group analysts, direct access to a team of analysts, research reports, forecasts, DecisionNotes and regular Online Decision Forums on relevant topics.

We offer Decision Services on almost 30 selected topics in Telecommunications; Wireless/Mobile Communications; Consumers, Media & Entertainment; and Information Technology Hardware, Software & Services.

Decision Instruments

Yankee Group offers a full portfolio of technology and market forecasts, trackers, surveys, and total cost of ownership (TCO), return on investment (ROI), selection and migration tools. Decision instruments provide our clients the data required to compare, evaluate or justify strategic and tactical decisions—a hands-on perspective of yesterday, today and tomorrow—shaped and delivered through original research, in-depth market knowledge and the unparalleled insight of a Yankee Group analyst.

Trackers

Trackers enable accurate, up-to-date tactical comparison and strategic analysis of industry-specific metrics. This detailed and highly segmented tool provides discrete proprietary and performance data, as well as blended metrics interpreted and normalized by Yankee Group analysts.

Surveys

Surveys take the pulse of current attitudes, preferences and practices across the marketplace, including supply, delivery and demand. These powerful tools enable clients to understand their target customers, technology demand and shifting market dynamics.

Forecasts

Forecasts provide a basis for sound business planning. These market indicators are a distillation of continuing Yankee Group research, interpreted by our analysts and delivered from the pragmatic stance our clients have trusted for decades.

Signature Events

Yankee Group's signature events provide a real-time opportunity to connect with the technologies, companies and visionaries that are transforming Telecommunications; Wireless/Mobile Communications; Consumers, Media & Entertainment; and Information Technology Hardware, Software & Services.

Our exclusive interactive forums are the ideal setting for Yankee Group analysts and other industry leaders to discuss and define the future of conversable technologies, business models and strategies.

Consulting Services

Yankee Group's integrated model blends quantitative research, qualitative analysis and consulting. This approach maximizes the value of our solution and the return on our clients' consulting investment.

Each consulting project defines and follows research objectives, methodology, desired deliverables and project schedule. Many Yankee Group clients combine Decision Service memberships with a custom-consulting project, enabling them to augment our ongoing research with proprietary studies.

Thousands of clients across the globe have engaged Yankee Group for consulting services in order to hone their corporate strategies and maximize overall return.

www.yankeegroup.com

Yankee Group believes the statements contained in this publication are based on accurate and reliable information. However, because our information is provided from various sources, including third parties, we cannot warrant that this publication is complete and error-free. Yankee Group disclaims all implied warranties, including, without limitation, warranties of merchantability or fitness for a particular purpose. Yankee Group shall have no liability for any direct, incidental, special, or consequential damages or lost profits. This publication was prepared by Yankee Group for use by our clients.