



Why Service Providers Should Offer Security as a Value-Added Service to Consumers, SMBs, and Enterprises

Table of Contents

Introduction	3
Why SMBs and Enterprises Want to Outsource Their Security to Service Providers	4
Why Consumers Are Interested in Buying Security from Service Providers	6
Why Service Providers Should Offer Managed Security Services	7
Which Services Should a Service Provider Offer?	8
Conclusions	9

Why Service Providers Should Offer Security as a Value-Added Service to Consumers, SMBs, and Enterprises

Introduction

A revolution is taking place in telecommunications, with broadband technology at its heart. Unstoppable and welcome, broadband is spearheading the replacement of much of the world's telecommunications infrastructure with a new, high-speed, converged network across which data, voice, TV/video, and games will all flow unimpeded.

In many countries, convergence is already reality, with the rollout of new, high-speed multimedia networks now seeing wide-spread adoption. Having started primarily with the upgrading of the core networks of the large national telecommunications and service providers, high-speed convergence is now penetrating businesses of every size. Even more exciting is the rapid deployment of converged services to the residential/home user, where uptake of broadband cable or DSL quickly leads to the adoption of new telephony or other value-added services.

Unfortunately, increased network speeds, interconnectivity, and easier remote access have all made it easier for viruses and other forms of malware to circulate from one network node to the next, and from one business to another. Further, recent versions of malware not only threaten the integrity of business data, but also expose adversely affected networks—their data, their resources, and their bandwidth—to access by other individuals and organizations.

While PC and network security previously was seen as the responsibility of the individual or the administrator of the private LAN/WAN, attention is turning to the service providers that supply new network infrastructures and converged, high-speed network links. Not surprisingly, rightly or wrongly, some blame is being placed upon these telecommunications and service providers for seemingly allowing polluted, unchecked, and dangerous bandwidth to flow into homes and outsourced business networks under their control.

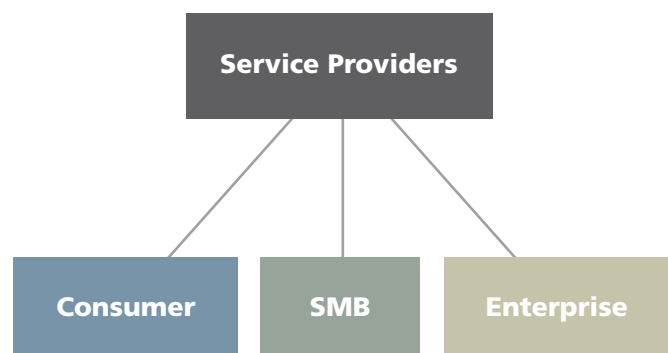
At the same time however, public awareness of new networking and communication security threats is increasing. Individuals and companies, while realizing

they must accept responsibility for securing their own bandwidth and network assets, are struggling to cope with the increasing number of vulnerabilities and threats they face. Enterprises, small businesses, and consumers do not have the expertise, funds, or rapid-response capabilities necessary to keep up with the latest countermeasures and techniques to effectively combat the problems caused by increasing number of vulnerabilities and security threats.

Historically, all roads led to Rome. Nowadays, in the networking world, all roads seem to lead to the service provider. The service provider is best positioned by its advantages of scale, network reach, and expertise to proactively protect the bandwidth and infrastructure it offers to customers, as well as the networks and assets they build around them. And if problems do occur and the customer turns to the service provider for help, guidance, or blame, the service provider is then given a unique opportunity to offer valued assistance that can not only strengthen the bond of trust between them, but can also create significant upsell opportunities for the service provider.

It would be impossible for service providers to achieve this all alone, but, by working together with global security partners who share a common vision, it becomes possible to jointly secure core networks and build managed security services that are in high demand and can generate profitable revenues from customers who either want to remain in control of their own infrastructure or outsource the management of their services to the service provider.

Service providers are uniquely placed to address three distinct markets:



This document examines the opportunity service providers have to work with a security vendor such as McAfee® to build and offer new managed network security services in response to the growing market need. It will focus on why businesses and consumers turn to service providers for help and outsourced security services, as well as why service providers are well-positioned to respond to the increasing demand for managed security services. It will also highlight the threat that faces those service providers who fail to provide security services to their customers, and who run the risk of losing their customers to new service provider partners who do.

Why SMBs and Enterprises Want to Outsource Their Security to Service Providers

Over the past few years, business executives have discovered that developing a security strategy that protects company information and essential business operations is vital to a business's long-term success.

Building security into the core strategy of any company is essential, since the threat viruses pose to profitability is now compounded by sophisticated new malware (e.g., Trojan horses, spyware, keyloggers, etc.) that threatens the integrity, ownership, and control of a company's confidential data and intellectual rights. Security breaches represent a significant risk for an organization.

Today's businesses face a virtually insurmountable task when attempting to secure their data against malware. In addition to providing the expertise to install basic security technologies such as anti-virus, firewall, and intrusion detection and prevention solutions, they also have to ensure ongoing network interoperability, that the latest security updates and patches are continuously downloaded and deployed, and that the network is continuously monitored and maintained, all against a backdrop of a growing list of hardware and software vulnerabilities.

In addition, they are tasked with staying on top of the latest technologies designed to protect them from the ever more sophisticated hacker attacks and dreaded "zero-day" viruses. Assigning resources to this task, especially when resources are limited, is often a luxury that many organizations cannot afford.

Not surprisingly, in an increasingly competitive marketplace, enterprises and small and medium-sized businesses (SMBs) no longer have the budget, skill sets, or IT-support capabilities to properly deal with this problem.

Unfortunately, even when resources are available, lack of effective action in the face of new threats can lead to a state of paralysis in which, unsure of how to proceed, businesses often take little or no action at all, thus leaving networks exposed to threats.

Such concerns were borne out in a recent Yankee Group survey [Yankee Group Q4 SMB IT Infrastructure survey] in which 61 percent of surveyed SMB and mid-market business owners identified security breaches as their top technology challenge, followed closely by 47 percent of respondents concerned with how to keep up with network security upgrades. Yet many of these businesses still took no action toward solving the challenges they had acknowledged. According to the research, 40 percent of respondents stated that they don't take action to secure themselves because of concerns that one upgrade would simply trigger another, and that 38 percent of respondents lacked IT staff or skills to cope with this. Finally, 32 percent stated that they simply did not have the time to do it.

Accepting their inability to respond effectively to another potential security threat, an increasing number of businesses are outsourcing security needs to service providers that are able to offer cost-effective solutions. This trend is forecasted to grow significantly over the next three years.

In the following table, we look at some of the factors that are driving businesses to adopt security services.

Drivers for Businesses to Adopt Security Services**Business Justification**

Business as usual	Organizations want their technology to run seamlessly. Any compromise is unacceptable. Any data loss or downtime of core business functions such as email and server-based applications can have a massive financial impact.
Decreased costs through subscription-based security services	<p>The financial strength of an organization can be increased by:</p> <ul style="list-style-type: none"> • Reducing upfront capital expenditure of trialling, purchasing, and implementing network security equipment and solutions • Converting ongoing operational expenditure for these security solutions to predictable, monthly subscription fees <p>This may also provide accounting efficiencies in the way costs are treated differently within the accounts.</p>
Increasing malware threats complicate deployment of point solutions	<p>Point products are expensive to roll out and maintain. As more and new forms of security threats are identified, new point product solutions are needed.</p> <p>Significant cost savings can be achieved by outsourcing to an expert who operates solutions shared securely between multiple customers, thus bringing down the cost per customer, and where economies of scale enable the expert to deploy cost-effective solutions based upon the latest technology.</p>
Disaster preparedness	Legal, regulatory, and business-driven service-level agreements (SLAs), along with a common-sense requirement for network redundancy and disaster recovery in the face of disruptions such as power blackouts, terrorist activity, and natural disasters, commonly lead businesses to outsource data back-up and recovery to service providers. Such planning must now include planning for the effect of security breaches and harmful malware activity, both in terms of preventing such activity and recovering from the aftereffects.
Regulations and compliance	Time-consuming and confusing industry regulations (e.g., Health Insurance Portability and Accountability Act, or HIPAA, and Sarbanes-Oxley) place an increasing burden on businesses, forcing them to divert resources and money to comply with regulations dealing with a variety of network and data considerations that are not part of the company's core business. To assure compliance and not detract resources from primary operations, businesses are including regulatory and compliance considerations when defining services which may be outsourced to an expert.
IT staff	<p>Organizations, particularly small and mid-sized ones, do not have access to full-time staff with expertise in every area of technology. When new security threats require new solutions to be implemented quickly, lack of resources can either result in a solution being implemented too slowly or not at all, often with serious consequences.</p> <p>Service providers offer an incredible value-add for organizations that have insufficient IT resources or expertise. Service providers can implement and provide ongoing support for these solutions with far less up-front and ongoing expenditures than any organization could accomplish on its own.</p>
Increased willingness of firms to outsource	As service providers hone technology and roll out new, cheaper, managed, subscription-based security services, the benefits to businesses, both financial and technological, are increasingly overcoming internal fears and objections to outsourcing security to a third party.

Why Consumers Are Interested in Buying Security from Service Providers

As broadband is more widely adopted by consumers, demand for anti-spyware and anti-adware products increases dramatically, since faster connectivity allows malware to more easily be downloaded transparently onto an end user’s PC. Whereas the effect of viruses can remain undiscovered, spyware and adware have obvious effects that provoke immediate concern and reaction from end users. Consumers, aware that the problem comes from the Internet, automatically turn to the source of their Internet connection—their service provider—for help, advice, and problem resolution. As spyware and adware becomes a more prevalent consumer issue, the burden that support calls will place on service providers is expected to increase.

Unless service providers implement solutions to block the spread of malware, or offer simple and cost-effective anti-malware solutions to customers, whether bundled with the basic broadband connection or as an optional value-

added service, this problem will only increase—negatively impacting the profitability of consumer broadband services.

As service providers offer customers increasingly complex products (Voice over IP, video-on-demand, data back-up, etc.), consumers will grow more frustrated and less capable or willing to maintain an understanding of what they have to do to secure their identities, their data, and their PCs.

Increasingly they will look to their service providers to do this. In response, consumer-targeted security solutions must be simple and almost transparent to the end user. In addition to the opportunity to generate new revenue streams, service providers will need to provide security services to customers to increase customer satisfaction and reduce customer churn. Otherwise, customers will seek out service providers that do offer the security solutions they require.

The key drivers for consumers buying security services from service providers are:

Drivers for Consumers to Adopt Security Services

Business Justification

Lack of technical expertise	To protect their broadband connections with basic security, consumers must install, manage, and ensure regular updating of anti-virus, personal firewall, anti-spam, content management, anti-spyware, anti-adware, and pop-up blocking solutions. Few consumers have the ability, time, or money to do this effectively.
Increasing dependence on the Internet	PDA’s, laptops, handhelds, remote employee, and business partner PCs are all integral to today’s businesses. End users, frustrated by lack of IT knowledge but with no choice but to use the technology, must turn to someone for help. This situation is made worse when the technology and hardware being used is also essential for home-business use, and where the lack of IT expertise of the employer effectively pushes responsibility for such devices to the end user or employee.
Cost of lost personal and professional productivity	Managed security services can help consumers prevent lost productivity and hardware outages due to malware.
Need for rapid response and resolution of problems	When consumers experience a hardware outage from a security breach, their requirements to get back up and running are often just as critical as corporate employees. They do not have access, however, to IT staff for rapid response and resolution. The service provider can be a great value to consumers in this way.
Threat protection and Internet protection	Service providers can help with threat protection, but they can also protect against other types of negative usage such as by restricting access to unauthorized sites and preventing sensitive information from unknowingly leaving end-user computers (i.e., transmission of personal data or information initiated by spyware programs).
Zero-day threats and lack of technology sophistication	Though a customer may already have survived a virus with no significant ill effects, fear of a new, unstoppable, disastrous virus erasing an end user’s data or disabling important hardware are increasingly present in consumers’ minds. End users are willing to pay to protect their systems, especially if they know the solution is powered by a large, trusted vendor with global expertise in security.
Limited budget	It can be costly for consumers to purchase multiple software packages to provide sufficient security. These can also be difficult for consumers to manage and maintain, particularly when one software package clashes with another. If service providers can provide this as a cost-effective, well-tested bundle, then consumers will be well-protected for less cost and fewer resources than by doing it themselves.

Why Service Providers Should Offer Managed Security Services

As providers of broadband connectivity, managed VPNs, access links, and a host of other complementary services, service providers already have a direct route to the very heart of their customers. As convergence becomes more popular, service providers who provision or manage the customer’s core network or access links will find themselves in an increasingly powerful position of trust, responsibility, and opportunity. Not to mention that customers will also

enjoy a significant comfort level with their service providers, which is the greatest hurdle for any vendor when trying to reach consumers.

Because service providers have already perfected the services model and the addition of ancillary services, satisfying customer demand by offering additional security services will be a natural progression.

Some reasons why service providers should offer managed security services on a larger scale are given below:

Drivers for Service Providers To Adopt or Enhance Managed Security Solutions

Business Justification

Deep network expertise and investment	Service providers already have tested, established relationships with their customers. With an existing infrastructure (network hardware and software, management, monitoring, end-user network visibility, billing, customer service), service providers can easily roll out additional services. Further, incremental penetration deeper into their account base prohibits other players from capturing market share from their customers.
Ability to leverage investment over large user base	Service providers are in a unique position to derive benefit from scale. They can deploy the latest technologies and solutions and recoup investments in a reasonable period of time, leveraging hardware and software to address multiple users.
Established business processes	Service providers already have scalable provisioning and billing relationships, which enables them to offer new subscription services using established processes. No other industry has such a strong recurring customer relationship, perfect for adding incremental services.
Installed customer base	The cost of customer acquisition for new services should be low, since service providers already have existing clients who might be interested in additional security services.
Single billing	By centralizing services by using a single vendor, customers can benefit from the service provider’s ability to collate multiple services onto a single monthly invoice.
Single point of contact	Not only can the service provider reduce operational expenditure by centralizing support for multiple services to a single help desk, but customers benefit from a single point of contact in the event of service problems.
Flexibility and expertise	Organizations with limited resources struggle to keep abreast of technology, threats, and countermeasures. Service providers are in a unique position to keep up with technology trends, establishing themselves as recognized security experts. Subsequently, they can spread the benefits of research and testing on the latest solutions across multiple customers, using their scale to react quickly to new developments and create flexible and economically viable solutions that customers would never otherwise be able to afford.
New sources of revenue and growth	Many services that service providers currently offer to their customers are regulated, and therefore suffer from downward-spiralling pricing as a result of increasing competition and regulatory pressures. Service providers are therefore driven to find new services to increase the annual return per user (ARPU).
Satisfy increased customer demand for outsourcing	Economic and business reasons for customers to outsource network, IT, and security services to service providers are increasing. Service providers that fail to recognize this trend, and are unable to respond to increasing customer demand, risk losing potential customers.
Implement the strategy and derive the benefit of convergence	<p>Many service providers have subsidized the cost of customer acquisition when signing up customers to new broadband or VPN services. The strategy has been to initially capture the customer on a new high-speed link, in preparation for the convergence of multiple, new, future value-added services onto that same, single access link.</p> <p>Not only are security services seen as one of the first of these services, but also, in order for customers to benefit from future converged services, the core network, assets, and bandwidth of the customer must be protected against new threats and vulnerabilities that will come with such services. Otherwise, network performance may be impacted in such a way as to make other new future services non-viable (i.e., spyware could introduce too much latency into a connection, making VoIP-based telephony services incoherent).</p> <p>While service providers will be able to derive new future revenue streams by offering additional incremental security services, failure to fully protect customer networks may threaten future implementation of such services.</p> <p>To ensure successful rollout of strategic value-added services, some service providers might consider subsidizing the cost of security services.</p>
Build a predictable incremental revenue stream	Managed security services can be offered on a subscription basis, providing predictable revenue streams that increase month-on-month, as the customer base grows. Many subscription-based services can also enjoy high renewal rates.
Customer lock-in to reduce churn	Security and trust is at the heart of any relationship. When service providers earn the trust of customers and win the right to provide managed security services, they enjoy a unique partnership in which the customer depends on the service provider for many core aspects of its business. This position of trust can lead to profitable, long-term partnerships. Security services can thus reduce potential customer churn and increase customer loyalty, protecting service providers from competitors.

Which Services Should a Service Provider Offer?

There is a broad range of services a service provider may create.

At their core, these security services should provide protection for the following:

- Network infrastructure (CPE, servers, routers, switches, gateways, signaling servers, PCs, telephones, handsets/PDAs)
- Assets associated with the network (data, voice, video, databases, business operations, and the ability to do business)
- Bandwidth (reducing unwanted and unauthorized traffic)
- Network availability (preventing and countering Denial-of-Service attacks)
- Personnel (preventing damage to personnel or individuals as a result of the theft of personal information, or protecting any life-critical systems that could be impacted by malware or a breach of security, such as power supplies and life-support systems in hospitals)
- Company integrity (preventing illegal or unauthorized communications leaving an organization, which could impact on a company's reputation or legal standing; protecting business partners by preventing malware being transmitted from one organization to another)
- Software and business applications (protecting the business software and applications that enable an organization to function in its chosen marketplace)

This would be done by service providers:

- Monitoring the potential threats to each of the above
- Monitoring a customer's exposure to each of the potential threats, advising the customer how to mitigate against such threats, and assisting the customer to decrease the customer's vulnerability and exposure to any such threat
- Assisting the customer to implement, or implementing on behalf of the customer, procedures to proactively protect the customer against specific threats
- Monitoring the network, assets, bandwidth, data, and data flow in real time to see specific threats or attack vectors to the above as they unfold, and implementing real-time countermeasures to counter or block any unauthorized or potentially damaging activity
- Providing remediation services to rectify the negative effect of any previous damage (e.g., cleaning infected files from viruses, restoring databases and data after service outage)
- Maintaining and monitoring a customer's equipment and software

In partnership with security companies that specialize in global security solutions, service providers can develop and roll out services that provide comprehensive protection to address these concerns.

A good example of such services are the service provider security protection suites offered by McAfee. These suites allow service providers to build security solutions for customers to protect business-critical data and applications, along with securing the Internet connection by minimizing the risk that data arriving from and going to the network may contain malware or can be used by attackers.

The McAfee service provider security protection suites contain all the necessary components for service providers to build powerful solutions that will protect their customers' businesses and assets:

- **Anti-malware** (anti-virus, anti-spam, anti-spyware/adware, URL filtering, detection and removal of potentially unwanted programs, desktop firewall, etc.) built on the McAfee anti-malware software-as-a-service solutions, which enable service providers to uniformly protect consumer, SMB, and enterprise PCs, desktops, and servers)
- **Mobile device security** built on the McAfee Mobile VirusScan® and Firewall products, which enable service providers to provide advanced VirusScan wireless protection, optimized for PDA devices such as handhelds and pocket PCs
- **Intrusion prevention** built on McAfee's family of network intrusion detection and prevention appliances can provide detection of network intrusion by malware or attackers, with real-time response to protect the network and its assets. An effective tool in helping customers comply with government and industry regulations (e.g., HIPAA, Sarbanes-Oxley)
- **Secure content management** built on the McAfee Secure Content Management solutions, which enable service providers to protect both the integrity of data in transmission to and from a customer, but also ensure that any malware hidden in the content of data is not allowed to penetrate a network or its appliances and assets. These solutions also protect stored data, network bandwidth, and network operations by dealing with the threats related to spam mail, Denial of Service attacks, and malware by preventing any negative impact on key network servers
- **Vulnerability management** built on the McAfee Foundstone® solution that protects network infrastructure by automatically discovering and classifying all known assets on a network; creating an inventory of hardware, software versions, and patch status; correlating this inventory against a list of all known vulnerabilities and

potential threats that could be targeted against them; and then cross-checking it against a strategically determined list that values each of the assets in the company according to business need or importance. In the face of potential information overkill, this solution would automatically prioritize and draw up a list of remedial actions that a customer (or the service provider) must work through in order to protect network assets from threats, followed by automated remediation tracking and progress reporting

Conclusions

As a result of the rollout of converged services and broadband networks, there is a growing demand for managed security services. Service providers that provide connectivity to consumers and businesses are positioning themselves to increase their position of trust with their customers. Using solutions from the McAfee security protection suites, service providers can proactively deploy value-added services that sanitize and protect a customer's network, assets, and business applications by automatically contending with network threats and malware either in-the-cloud, at the network edge, or within the network. In the creation of such services, it is anticipated that service providers will be able to leverage the brand value of a global security provider such as McAfee to drive and promote acceptance of these offerings within their customer base.