

IBM Internet Security Systems
Ahead of the threat.™



Managed Security Services Deliver Protection on Demand

**Information Security that Works for You,
Instead of Putting You to Work.**

Contents	
1	<i>Managed Security Services Deliver Protection on Demand</i>
2	<i>Who: As in, who needs it?</i>
2	<i>What: What are Managed Security Services offering protection on demand?</i>
6	<i>When: When do you need Managed Security Services with Protection on Demand?</i>
6	<i>Where: Where do you need Managed Security Services with Protection on Demand?</i>
7	<i>Why: Why do you need Managed Security Services with Protection on Demand?</i>
7	<i>How: How do you get Managed Security Services with Protection on Demand?</i>
9	<i>Conclusion</i>

Managed Security Services Deliver Protection on Demand – Information security that works for you, instead of putting you to work

Today's business climate is demanding and fast-paced. Thanks to advances in technology, a company's level of responsiveness, flexibility and performance can mean the difference between success and failure when it comes to protection. Businesses rely on technology for a competitive edge, an innovative means to serve customers and partners, an efficient way to manage business processes, and much more. Where does information security fit into the business and technology equation? Security absolutely includes technology components, but it also affects business process and vice versa. Information security can be viewed as one component of an overall IT strategy, but in a sense, it also protects and enables the IT infrastructure. Is information security foundational to IT strategy, or is it an overlay? The answer remains ambiguous. Every business is different and each will take a varied approach to security. Hence, we face myriad security technology and the troubling complexity of finding and managing an enterprise security solution.

Consider the results of a recent CIO survey¹:

- Only 11 percent of executives felt more vulnerable to security breaches from last year.
- Only 25 percent of CIOs rated preventing breaches, controlling user access to data and systems, and assessing risk as top priorities.
- More than half rated managing the complexity of security as their number one challenge.

While executives may not feel at risk, and the major worm outbreaks seem to have subsided, Internet threats are on the rise with cyber crime taking a more sinister, sophisticated approach. Professional criminals have replaced glory-seeking hackers as the primary threat. Responsible executives don't question the need for security – especially in the age of increasing regulatory compliance. Understandably, the question facing most businesses regarding security is how to reduce the complexity, prevent threats and prove due diligence all without breaking the bank or taking man-hours away from critical initiatives. A managed services approach to security aims to solve these problems for business large and small by affording the features and benefits of protection on demand.

Protection on Demand capabilities integrate managed services, technology and security intelligence with existing business processes, so that enterprises prevent attacks and misuse, address key stakeholder demands, and meet environmental changes – when and how they require. Unlike other technologies and applications that operate within one small or broad functional range, security has to cross multiple boundaries and systems. It has to protect all of the technology and information businesses already have in place as well as any new demands placed on the business. Additionally, lack of time and resources emphasize the need for security to integrate with existing workflow, ticketing and reporting systems to create greater efficiency and ultimately help reduce costs.

The demands on security require a protection on demand approach from managed security services: it's the Who, What, When, Where, Why and How of security. When used properly, managed security services are designed to optimize resources, reduce operational costs, improve flexibility and responsiveness, and address regulatory requirements. In essence, managed security services should work for you, not the other way around.

Who: As in, who needs it?

Security threats and weaknesses know no vertical industry boundaries. Software vulnerabilities exist in all systems and attacks don't discriminate between small and large companies. So far, the complexity of security technology has relegated much of it to the enterprise level only, as the big guys are the only ones with enough manpower to install, manage and monitor bulky security solutions. Managed security services offering protection on demand can be applied for the largest enterprises, as well as small businesses and companies in between. Managed services also help satisfy security needs across industries, from government to retail to manufacturing.

What: What are Managed Security Services offering protection on demand?

Managed security services with protection on demand capabilities are designed to deliver protection to organizations of all sizes, helping them to proactively respond to Internet threats while integrating security with key business processes. IBM's innovative managed security services approach blends market leading services, technologies, and security intelligence into a single solution that can be utilized when, where and how you need it. The result is a cost-effective solution that should enable you to optimize resources, improve flexibility and responsiveness, and address regulatory requirements.

One of the keys to understanding managed security services with protection on demand capabilities is to see them in contrast with the current approach to security involving multiple technologies, management systems, manpower and manual integration. To achieve the benefits of managed security services with protection on demand, a business would have to manage the following components:

- Security technology – anti-virus, firewall, VPN, intrusion detection and prevention for networks, servers and desktops, anomaly detection and virus prevention
- Vulnerability assessment technology – software and appliances to scan networks, servers and desktops for potential risks
- Centralized management system – software or appliance to monitor and manage security technologies (a vendor's solution usually only works with its own products)
- Security Event and Log Management (SELM) system – unlike the log analysis tools built into individual appliances or applications, SELMs are costly systems that work across multiple classes of devices (firewalls, intrusion detection systems, intrusion prevention systems, etc.) from multiple vendors
- Event Analysis – a huge undertaking, this requires human security expertise to normalize, aggregate, correlate, archive, escalate and remediate security events (most SELMs today have limited or no ability to do this)
- Primary security intelligence – applied to all the security event and vulnerability information in order to prioritize risk and protection
- Workflow and ticketing integration – as threat and vulnerability data is continually collected, assessed and prioritized, it must also drive corrective actions and reporting in workflow and ticketing systems
- Security experts – while most security technology is automated, security experts are still required for the level of security protection on demand affords.

Most companies find it impossible to purchase, install, monitor and manage such a comprehensive and expensive security solution. And in fact, many companies don't need all of the bells and whistles security technology has to offer. When it comes to security, most executives simply want to answer the question, "Am I more secure today than I was a year ago?" The managed services approach can provide the answer without the management hassle.

The components of managed security services with protection on demand are simple, and encompass many of the technologies and capabilities listed above minus the complexity. Managed services are combined with security technology, expert systems and security intelligence to form a solution that businesses do not need to purchase, manage or maintain – unless they choose to do so.

Security is not a one time event; it is an anytime imperative. With a managed security services approach to protection on demand, security can help drive IT productivity by improving system availability and reducing risk. By making protection more proactive, managed services are designed to transform the way organizations approach security, while aligning security technology to address evolving business requirements more strategically.

Managed Security Services with Protection on Demand Offer Flexibility

Delivering protection on demand through managed security services offers organizations the flexibility to choose what type of security service and/or technology they need at any time. Traditionally, security solutions have been purchased on an “all or nothing” basis. With managed services, businesses select the security technologies they need, when they need them. Then companies choose how they want the technology managed – outsourced, in-house or a combination of both. Companies can switch from in-house to outsourced management at any time – during overnight hours, in the event of a threat or when internal resources are needed to focus elsewhere. They only pay for what they use – a novel concept in information security.

Businesses can also use managed services to secure particular aspects of their business. For example, a business might want to secure the VoIP platform implementation. With managed security services, the VoIP devices can be managed so that the VoIP traffic is monitored and analyzed, which should automatically prevent most threats.

Vulnerability management also becomes much simpler with a services-based approach. Instead of the patch-and-panic cycle many businesses engage in, managed services are designed to enable vulnerability scanning at any time, at whatever location – all according to individual business needs. For example, a retail chain may want to perform scans for all locations overnight to avoid traffic slow-down during business hours. With managed security services, the retailer can schedule scans at the most appropriate times. Scanning becomes automatic and seamless, with integrated ticketing and workflow for remediation, bringing security and IT maintenance activities in line.

In the event of an acquisition, businesses using managed security services can temporarily entrust the security of the newly-acquired company assets to a trusted provider while a long-term solution is developed. If a business fails an audit and wants to produce detailed security reporting to demonstrate due diligence, it can rely on managed services until further notice. Consider the expense, time and resources saved with this approach.

Managed Security Services with Protection on Demand Improve Responsiveness

Businesses can make security a proactive scenario using managed security services that deliver protection on demand, helping stop threats before impact. Managed security services are designed for companies to apply security technology where it is most needed to address business requirements. Managed services offer responsiveness that makes security an integrated part of overarching business processes, not a separate business process of its own.

If a security event occurs, businesses can take action when, where and how they choose, rather than being locked into to a rigid “one-size-fits-all” protocol. Managed services make security adaptable to changes in the threat landscape, shifting business priorities and new business processes.

As updates to security technologies or new security technologies become available, managed security services enables companies to quickly apply those technologies as they see fit. Increasing speed-to-protection provides businesses with the security they require to protect business processes.

Managed Security Services with Protection on Demand Enhance Performance

Measuring security performance has been a tricky prospect in the past. If information security does its job right, then nothing happens. However, it's hard to use “nothing” as a measure for success. The real question businesses face regarding security is whether they are more secure than they were the year before? And if so, how can they quantify that in terms of reduced risk and compliance, and overall value to the organization?

Businesses also want to know if the cost of ownership for security solutions makes sense. With managed security services, businesses have a consolidated view of business security posture – there is only one place to go (a security portal) for all the information you need. Managed security services provide numerous customized reporting options to effectively demonstrate that progress has been made regarding vulnerability management, security policy maintenance, and event and log archival for meeting compliance requirements and investigative purposes.

Comprehensive reporting helps companies prove the business value of their security investment and answer the critical question, “Are we more secure today than we were last year?”

Security event information is only valuable if businesses can use it to take corrective action. With a consolidated view of security posture, businesses now have the flexibility to report on the number of remediation tasks assigned and completed, the number of vulnerabilities reduced, the cost-savings associated with cleaner traffic and more efficient use of bandwidth, and much more.

Regulatory compliance can be linked to security performance as well. The information needed for annual audits – vulnerability management, security log files, etc. – is captured and maintained in a forensically-sound manner. To ease auditing and investigation, the information can be accessed from a single portal for convenience and efficiency.

When: When do you need Managed Security Services with Protection on Demand?

Managed security services that deliver protection on demand capabilities are designed to fit individual business in whatever timeframe is required. For example, a business that normally manages its own IPS devices may choose to transfer those devices to a managed service in the event of a worm outbreak. Just as easily, the management of IPS devices can be returned to the company once the outbreak is over.

At any time, organizations can opt for a do-it-yourself, outsourced or combination-of-both approach. Managed security services also offer security and business process advantages in the event of new government regulations, an acquisition or changes in the business such as new systems or the addition of a new business unit.

Because it helps make security more proactive, managed security services provide the benefits of protection on demand, helping to enhance the way businesses operate, and align security with evolving business requirements like never before. Managed security services are available at any time, but their advantages become clearer whenever businesses experience a change that would normally cause them to re-assess, re-prioritize and re-configure security technology. In such instances, managed security services are designed to work fluidly in a changing IT environment – hence the benefits of protection on demand.

Where: Where do you need Managed Security Services with Protection on Demand?

Managed security services can be applied wherever businesses want to protect information assets. Whether globally, at corporate headquarters or only for remote locations, the choice depends on whatever makes business sense. Companies don't have to start big. Instead, they can selectively test services by starting with outsourced protection at a particular location or for a certain segment of the IT infrastructure, while still managing other aspects of their security internally. Whether starting with a single data center or the entire IT infrastructure, organizations will have access to all the protection on demand capabilities – advanced analysis and correlation, artificial intelligence, industry-leading security expertise, and a Web-based management portal – regardless of the size of their deployment.

Why: Why do you need Managed Security Services with Protection on Demand?

An on-demand solution affords protection for ever-changing business demands while maintaining a company's competitive edge. In order to focus critical resources on the primary business, instead of security, companies need outsourced expertise that affords protection on demand.

Managed security services leverage existing technology investments – such as routers, application servers and security technologies. The solution is scalable for growth, so as the network expands, managed services accommodate. Likewise, as staff changes and focus shifts, managed security services give businesses the flexibility they need to secure business processes.

With technology-enabled services and primary security intelligence, managed security services are designed to give businesses access to security expertise when they need it. This approach speeds time to protection, reduces demands on internal resources and increases focus on operational excellence.

How: How do you get Managed Security Services with Protection on Demand?

Selecting the right managed security service partner could mean the difference between success and failure. Only the right combination of managed services, technology, security intelligence and ability to execute will deliver the benefits of protection on demand. The optimal solution should combine these elements to provide cost savings that can be reinvested into future growth. Managed security services with protection on demand can only be delivered by security-focused experts that offer:

- A complete managed security services platform
- A full suite of security technology for the entire IT infrastructure
- Real-time, proactive security intelligence on threats and vulnerabilities
- The ability to work with existing infrastructure and security technologies
- An understanding of how security affects business processes like storage, compliance, email, payroll, supply chain and more

Managed security services with protection on demand capabilities are available today from IBM Internet Security Systems (ISS), a trusted security advisor to thousands of the world's leading businesses and governments. At the forefront of security technologies like vulnerability assessment, intrusion prevention and virus prevention, IBM ISS products and services are based on the proactive security intelligence of its X-Force® research and development team – a world authority in vulnerability and threat research.

IBM ISS continues to innovate, pushing its technology and services forward to provide businesses large and small with the protection they need, using the approach they prefer. With an on-demand solution, organizations can more easily maintain a competitive edge while infusing protection into daily business operations. IBM Managed Security Services offer technology-enabled security services to speed time to protection and increase focus on operational excellence.

As part of the protection on demand approach, businesses can choose any combination of services and technology from the IBM protection platform – as well as market-leading technologies from other security vendors – as part of an integrated solution. Companies have a single view of their security landscape using the Web-based portal. Plus, IBM Managed Security Services can encompass currently-installed security technologies, potentially reducing the need for new security investments.

IBM Internet Security Systems products and services include:

- Security consulting services
- Security Technologies
- Intrusion detection and prevention systems for networks, servers and desktops
 - Virus prevention
 - Mail security and content filtering
 - Anomaly detection
 - Vulnerability assessment and management
- Managed Security Services
 - Managed protection services
 - Managed intrusion detection and prevention service
 - Managed and monitored firewall service
 - Security event and log management service
 - Vulnerability management service

IBM ISS lets businesses selectively outsource management and monitoring of security devices to IBM ISS, while using the portal to manage and monitor other security in-house. Using the protection on demand approach, businesses can consolidate the security view across diverse multi-vendor security devices and overcome the limitations of independent security stovepipes.

Conclusion

Organizations of all sizes need security that can adapt to their ever-changing environments, regulatory requirements and stakeholder demands. Integrating security with business processes can help organizations increase their efficiency and productivity, leading to cost savings and increased focus on the core business. Likewise, organizations need the ability to demonstrate that their security investment is delivering the protection they need, answering the question, “Are we more secure today than we were last year?” Most importantly, security solutions need to preempt Internet threats before they impact business processes.

Managed security services put you in the driver’s seat with protection on demand, giving you the flexibility and choice to secure your business in the manner that best suits your needs. The powerful combination of managed services, security technology and security intelligence can be delivered when, where and how you need it. It’s security that works for you, instead of putting you to work.

For more information about IBM Managed Security Services with protection on demand and the IBM protection platform, please visit www.ibm.com/services/us/iss.



© Copyright IBM Corporation 2007

IBM Global Technology Services
Route 100
Somers, NY 10589
U.S.A.

Produced in the United States of America
05-07
All Rights Reserved

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. Ahead of the threat is a trademark of Internet Security Systems, Inc. in the United States, other countries, or both. Internet Security Systems, Inc. is a wholly-owned subsidiary of International Business Machines Corporation.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

IBM assumes no responsibility regarding the accuracy of the information provided herein and use of such information is at the recipient's own risk. Information herein may be changed or updated without notice. IBM may also make improvements and/or changes in the products and/or the programs described herein at any time without notice.

1 *InformationWeek*/Accenture Global Information Security survey of 2,193 Global business-technology and security professionals