

## IBM Internet Security Systems White Paper

### *Protection on Demand*

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

**IBM Internet Security Systems  
Ahead of the threat.™**

## Table of Contents

<b>PROTECTION ON DEMAND— INFORMATION SECURITY THAT WORKS FOR YOU, INSTEAD OF PUTTING YOU TO WORK</b> .....	2
<b>WHO: AS IN, WHO NEEDS IT?</b> .....	2
<b>WHAT: WHAT IS PROTECTION ON DEMAND?</b> .....	2
<b>PROTECTION ON DEMAND IS FLEXIBILITY</b> .....	3
<b>PROTECTION ON DEMAND IS RESPONSIVENESS</b> .....	4
<b>PROTECTION ON DEMAND IS PERFORMANCE</b> .....	4
<b>WHEN: WHEN DO YOU NEED PROTECTION ON DEMAND?</b> .....	4
<b>WHERE: WHERE DO YOU NEED PROTECTION ON DEMAND?</b> .....	5
<b>WHY: WHY DO YOU NEED PROTECTION ON DEMAND?</b> .....	5
<b>HOW: HOW DO YOU GET PROTECTION ON DEMAND?</b> .....	5
<b>CONCLUSION</b> .....	6
<b>FOR MORE INFORMATION</b> .....	7
<b>ABOUT IBM INTERNET SECURITY SYSTEMS</b> .....	7

## 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 protecting their business. 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? It is absolutely part of technology, but it also affects business process. It 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 is that there is no answer. 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 survey<sup>1</sup>:

- 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 cybercrime taking a more sinister, sophisticated approach as professional criminals replace 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. Protection on Demand, a new approach to security, aims to solve these problems for businesses large and small.

Protection on Demand combines managed services, technology and security intelligence to integrate security with existing business processes, prevent attacks and misuse, address key stakeholder demands, and meet environmental changes. 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 reduce costs.

The demands on security require Protection on Demand: it's the Who, What, When, Where, Why and How of security. When used properly, Protection on Demand will optimize resources, enhance profitability, improve flexibility and responsiveness, and address regulatory requirements. In essence, it's security that works 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. Protection on Demand works for the largest enterprises, as well as small businesses and anywhere in between. It also satisfies security needs across industries, from government to retail to manufacturing.

### What: What is Protection on Demand?

Protection on Demand is a services-based approach that delivers protection to organizations of all sizes allowing them to proactively respond to Internet threats while integrating security with key business processes. This innovative managed security services approach blends market leading services, technologies, and security intelligence into a single solution that is delivered when, where and how you need it. The result is a cost-effective solution that enables you to optimize resources, enhance profitability, improve flexibility and responsiveness, and address regulatory requirements.

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

One of the keys to understanding Protection on Demand is to see it in contrast with the current approach to security involving multiple technologies, management systems, manpower and manual integration. To achieve the benefits of Protection on Demand, a business would have to handle the following components:

- Security technology – antivirus, 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 their 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 security expertise and expert systems 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 much of this technology is automated, human resources, in the form of 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. 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?" Protection on Demand provides the answer without the management hassle.

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

Protection on Demand is not a one time event, it is an anytime imperative. With it, security can help drive productivity and scale to address security needs across an organization's ever-changing infrastructure. By making protection more proactive, Protection on Demand transforms the way organizations approach security, while aligning security technology to address evolving business requirements more strategically.

## Protection on Demand is Flexibility

Protection on Demand 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 Protection on Demand, businesses select the security technologies they need, when they need them. Then the 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 Protection on Demand to secure particular aspects of their business. For example, a business adding a VoIP solution may want to secure the VoIP platform implementation. With a Protection on Demand solution, the VoIP devices can be managed so that the VoIP traffic is monitored and analyzed, automatically preventing any threats.

Vulnerability management also becomes much simpler with Protection on Demand. Instead of the patch-and-panic cycle many businesses currently engage in, Protection on Demand enables vulnerability scanning at any time, at whatever location – all according to individual business needs. For example, a retail chain may choose to perform scans for all locations overnight to avoid traffic slow-down during business hours. Protection on Demand enables the retailer to schedule scans for the time that works best for the retailer. 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, Protection on Demand enables businesses to temporarily entrust the security of the newly-acquired company assets to managed security services while a long-term solution is developed. If a business fails an audit and wants to ensure security and produce detailed reporting moving forward to demonstrate due diligence, it can rely on Protection on Demand until further notice. Consider the expense, time and resources saved with this approach.

## Protection on Demand is Responsiveness

Businesses can make security proactive with Protection on Demand, stopping threats before impact and taking the worry out of security. A Protection on Demand solution enables companies to apply security technology as needed to preempt Internet threats. Security can be applied where it is most needed to address business requirements. Protection on Demand's responsiveness 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. Protection on Demand makes 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, Protection on Demand allows companies to quickly apply those technologies as they see fit. Increasing speed-to-protection ensures that businesses will have the security they require to protect business processes.

## Protection on Demand is Performance

Measuring security performance has been a tricky prospect in the past. If information security does its job correctly, then nothing happens. It's hard to use "nothing" as a measure for success. The real questions businesses face regarding security is whether they are more secure than they were the year before? 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 Protection on Demand businesses have a consolidated view of business security posture – there is only one place to go (a security portal) for all the information needed. Protection on Demand provides numerous customized reporting options to effectively demonstrate that progress has been made regarding vulnerability management, security policy maintenance, event and log archival for meeting compliance requirements and investigative purposes and much more. Protection on Demand reporting allows companies to prove the business value of their security investment. It enables organizations to 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 events, 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 Protection on Demand?

Protection on Demand is designed to fit individual business needs at the time it is needed. If a business normally manages its own IPS devices but wants to hand over the management of those devices to a managed service in the event of a worm outbreak, Protection on Demand makes it possible. Just as easily, the management of those devices can be turned back over 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. It also provides 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 makes security more proactive, Protection on Demand can transform the way businesses operate, aligning security with evolving business requirements like never before. Protection on Demand is available at any time, but its 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, Protection on Demand works fluidly in a changing IT environment due to its managed services foundation.

## Where: Where do you need Protection on Demand?

Wherever businesses want to protect information assets, Protection on Demand will work. 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 with Protection on Demand. Instead, they can selectively test the service 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 Protection on Demand?

An on-demand solution is the best approach to security, affording 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 Protection on Demand.

Protection on Demand leverages existing technology investments – such as routers, application servers and security technologies. The solution is scalable for growth, so as the business and network expands, Protection on Demand accommodates. Likewise, as staff changes and focus shifts, Protection on Demand gives businesses the flexibility they need to secure business processes.

With technology-enabled services and primary security intelligence, Protection on Demand gives businesses access to security expertise when they need it. This approach speeds time to protection, reduces demands on internal resources, enhances profitability and increases focus on operational excellence.

## How: How do you get Protection on Demand?

Selecting the right partner for Protection on Demand could mean the difference between success and failure. Protection on Demand requires the right combination of managed services, technology, security intelligence and ability to execute. The optimal solution should combine these elements to deliver cost savings that can be reinvested into future growth. 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, e-mail, CRM, human resources, supply chain and more

Protection on Demand is available today from IBM Internet Security Systems, the 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 Internet Security Systems products and services are based on the proactive security intelligence of its X-Force® research and development team – the unequivocal world authority in vulnerability and threat research.

IBM Internet Security Systems continues to innovate, pushing its technology and services forward to provide businesses, both large and small, with the protection they need, using the approach they prefer. Only with an on-demand solution can organizations maintain a competitive edge while infusing protection into daily business operations. Protection on Demand offers technology-enabled security services to enhance profitability, 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 Internet Security Systems portfolio – as well as market-leading technologies from other security vendors – as part of a fully integrated solution. Companies have a single view of their entire security landscape using the Web-based portal. Plus, Protection on Demand can encompass currently-installed security technologies, 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 Internet Security Systems lets businesses selectively outsource management and monitoring of security devices to IBM Internet Security Systems 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 enterprises and overcome the limitations of independent security stovepipes.

Selecting the right partner for Protection on Demand could mean the difference between success and failure. It requires the right combination of managed services, technology and ability to execute. Ultimately, Protection on Demand should deliver security according to the who, what, when, where, why and how demands of each organization, along with cost savings that can be reinvested into future growth.

## Conclusion

Organizations of all sizes need the ability to adapt to their ever-changing environments, regulatory requirements and stakeholder demands. This is just as true for security as it is of any other aspect of business. Integrating security with business processes can help organizations increase their efficiency and productivity, leading to cost savings and increased profitability. 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.

Protection on Demand puts you in the driver’s seat, giving you the flexibility and choice to secure your business in the manner that best suits your needs. This powerful combination of managed services, security technology and security intelligence into a single solution can be delivered when, where and how you need it. It’s security that works for you, instead of putting you to work.

**IBM Internet Security Systems**  
**Ahead of the threat.™**

## GLOBAL HEADQUARTERS

6303 Barfield Road  
Atlanta, GA 30328  
United States  
Phone: (404) 236-2600  
e-mail: sales@iss.net

## REGIONAL HEADQUARTERS

**Australia and New Zealand**  
Internet Security Systems Pty Ltd.  
Level 6, 15 Astor Terrace  
Spring Hill Queensland 4000  
Australia  
Phone: +61 (0)7 3838-1555  
Fax: +61 (0)7 3832-4756  
e-mail: aus-info@iss.net

**Asia Pacific**  
Internet Security Systems K. K.  
JR Tokyu Meguro Bldg. 3-1-1  
Kami-Osaki, Shinagawa-ku  
Tokyo 141-0021  
Japan  
Phone: +81 (3) 5740-4050  
Fax: +81 (3) 5487-0711  
e-mail: jp-sales@iss.net

**Europe, Middle East and Africa**  
Ringlaan 39 bus 5  
1853 Strombeek-Bever  
Belgium  
Phone: +32 (2) 479 67 97  
Fax: +32 (2) 479 75 18  
e-mail: isseur@iss.net

**Latin America**  
6303 Barfield Road  
Atlanta, GA 30328  
United States  
Phone: (404) 236-2709  
Fax: (509) 756-5406  
e-mail: isslatam@iss.net

## For More Information

For more information about Protection on Demand, please visit [www.iss.net](http://www.iss.net).

## About IBM Internet Security Systems

IBM Internet Security Systems is the trusted security advisor to thousands of the world's leading businesses and governments, providing preemptive protection for networks, desktops and servers. An established leader in security since 1994, the IBM Internet Security Systems Proventia® integrated security platform automatically protects against both known and unknown threats, keeping networks up and running and shielding customers from online attacks before they impact business assets. IBM Internet Security Systems products and services are based on the proactive security intelligence of its X-Force® research and development team – the unequivocal world authority in vulnerability and threat research. The IBM Internet Security Systems product line is complemented by comprehensive Managed Security Services and Professional Security Services. For more information, visit the Internet Security Systems Web site at [www.iss.net](http://www.iss.net) or call 800-776-2362.

© Copyright IBM Corporation 2007. All rights reserved worldwide

IBM Internet Security Systems, Ahead of the Threat, SiteProtector, SecurityFusion and Virtual Patch are trademarks, Proventia and X-Force are registered trademarks, of IBM Internet Security Systems. All other companies and products mentioned are trademarks and property of their respective owners.

Distribution: General

SM-PoDWP-0107

# IBM Internet Security Systems

## Ahead of the threat.™