IBM Internet Security Systems

Preemptive security: changing the rules

If you're not ahead of the threat, you're only reacting to it.

Introduction: the new rules.

On August 13, 2005, a vicious Internet worm called the Zotob Bot ran rampant on the Internet. Within days, it was followed by at least a dozen other worms that exploited the same Microsoft® "Plug and Play" vulnerability. Some were Zotob variants and others were completely different. Among the afflicted organizations were major news and media companies – CNN, ABC, NBC, Associated Press and The New York Times.

One security company offered protection well ahead of the threat.

This event starkly illustrates the challenge facing Internet-driven businesses, but it also suggests the solution. In the case of Zotob, as with earlier catastrophic attacks such as Sasser, Blaster and Slammer, Internet Security Systems (ISS), now a division of IBM, had developed a defense well in advance of this threat. Thus, ISS (now IBM Internet Security Systems) customers avoided potential network damage and business disruption — not only from the initial attack, but also from the variants that followed.

It is this revolutionary "preemptive" security capability that has made the IBM Internet Security Systems division a trusted security provider to governments and Fortune 500 companies. Unlike traditional security methods that can only analyze and respond to attacks after they occur, preemptive security is designed to stop Internet threats before they can impact networks. Until recently, IBM Internet Security Systems provided this preemptive security to its clients via methods that were manual and therefore, complex. These methods have been refined and automated, and incorporated into a simplified Internet security platform that delivers this elite caliber of protection to organizations of all sizes.

This comprehensive solution is called the IBM Internet Security Systems protection platform and, with it, IBM Internet Security Systems is redefining the rules of business continuity and compliance. These new rules raise the bar in security, and can serve as a standard against which security solutions are measured:

- **"Preemption" beats "reaction"** With sophisticated new Internet threats, business losses are measured in seconds. In this environment, preemption is essential because no "reaction" can be fast enough to prevent the threat.
- **The Internet security challenge is not about networks or hardware; it is about the software that drives these systems …** specifically, software vulnerabilities. If the key to security is preemption, then the key to preemption is the capability to find and defend the vulnerabilities in software before they are exploited. Attack-based security methods (the traditional anti-virus security model of analyzing and providing antidotes after the attack has been launched) still play a role, but it is vulnerability-based security that defines the performance standard and preemptive approach.
- **Real security is dynamic — it is not a commodity or an infrastructure "feature."** Threats are rapidly multiplying and morphing as software becomes more complex. Since 1990, software applications have grown exponentially across network servers and appliances and are continuing to introduce a broad spectrum of threats. To be effective, security must stay ahead of this trend. Preemptive security is designed to keep you ahead of the threat, by applying ever-evolving intelligence and techniques developed from highly innovative and aggressive research methods.
- **Preemptive security is designed to keep you ahead of threats:** Preemptive security is designed to allow a company to remain ahead of potential network security threats.
- **Preemption has the potential to lower security costs by making security require less work.** Organizations buy technology to make things easier, but traditional security solutions (patching, IDS, firewalls, etc.) can create work. In some cases this can account for up to half of security's growing price tag. Cost containment requires better security. By preemptively stopping threats before they impact your business, preemptive security has the potential to reduce workloads and costs.
- **A better solution.** With preemptive security delivered within an integrated platform, organizations can have comprehensive protection that is not only designed to be effective, but can also scale, be centrally managed, and comes with a money back incentive if it fails to prevent threats.

The business need for a strategic Internet security approach

The Internet now drives business, and that means that Internet security is key to business success. Internet security dramatically affects how well companies manage internal networks, integrate new technologies and applications, and can play a role in helping them to meet their obligations to comply with new government regulations and industry standards—all while the variety and sophistication of security threats continue to evolve. Given the scope of the challenge, simply expanding the inadequate patchwork of tactical and "reactive" security point solutions is not a desirable option. Internet security should be viewed as a strategic business imperative. The goal: Align effective "preemptive" security technologies within an integrated platform that can span the enterprise (servers, networks and desktops), scale easily, provide actionable intelligence, and enable simplified central management.

Moving beyond old assumptions and unpleasant results

Even with all the attention and money being directed at the security challenge, today's enterprise landscape defies protection by conventional security solutions. Companies frequently see their expensive and complicated security systems beaten by a single, unforeseen Internet attack. As a result, they are constantly being forced into reactive mode—scrambling to pick up the pieces and restore order when security breaches occur. Internet security impacts virtually all aspects of enterprise management, technology migration and business growth—instead, corporate managers should raise their expectations concerning the capabilities of Internet security solutions. They should demand security that is both effective and manageable, and they should view its role within a broader, more strategic context.

Improve network security to secure productivity gains

Corporate networks are expanding rapidly at the perimeter by incorporating not only branch offices and telecommuters, but also vendors, customers, contractors and other outside organizations and individuals. In addition, new technologies such as wireless, smartphones and virtual private network (VPN) access are growing and being implemented rapidly. This integrated approach brings with it huge potential business gains, which can include shorter supply chains, improved customer response times and reduced error rates, as well as lower costs across the board. Unfortunately, conventional security methods can be overwhelmed by this ballooning population of network users, allowing outside users "default access" to critical systems and data. Effective strategic Internet security should be designed for enterprise-class protection and to empower businesses to confidently extend the horizons of their networks which may have such benefits as to further improve productivity, reduce costs and compete more effectively in a dynamic global economy.

Help to secure more than network uptime—help to secure bandwidth optimization

Catastrophic downtime is like a business heart attack, which explains why network managers strive so hard to avert it. On the other hand, bandwidth loss—which is akin to a chronic, low-grade affliction—tends to be routinely tolerated despite its debilitating effect on the health of the business. Unauthorized traffic across the network consumes bandwidth needed to support business-critical applications. It degrades network efficiency, increases infrastructure support costs and introduces a variety of associated security threats.

A strategic Internet security approach can help to prevent both downtime and bandwidth loss by incorporating anomaly detection, along with intrusion prevention and other security technologies, within an integrated platform that is designed to protect the entire network—from the core outward.

> *Internet security must be viewed as a strategic business imperative.*

Leverage new applications without adding new risks

Businesses are routinely challenged by security issues inherent in well-established technologies. The challenge is greatly compounded by the rapid adoption of newer applications, such as Voice over Internet Protocol (VoIP), customer relationship management (CRM) and others. Many of these technologies bring new vulnerabilities into the enterprise, with a multitude of new entry points and direct interaction with critical back-office applications. Here, as with every new generation of technology, conventional security is of limited value. Conventional security is designed to combat known threats. Yet threats associated with any new technology are largely unknown. That is why strategic Internet security must be vulnerability-based, rather than attack-based. It is not possible to foresee the infinite variety of possible attacks that can be launched against a new technology. However, it has been demonstrated that, with aggressive vulnerability research and technology development, it is possible to focus on the vulnerabilities—the weak points—where those attacks will be targeted, and establish a system designed to provide the ability to detect behavioral patterns that are indicative of new and previously uncategorized attacks.

Scale at the pace of network growth while streamlining security management

Growing networks are typically populated by hundreds, even thousands, of security applications and devices designed to protect against a growing variety of threats—and, for the most part, not communicating or coordinating with each other. These layers of disparate systems create increasing network complexity, along with costly administrative and support requirements.

Furthermore, such a conglomeration of tactical fixes typically cannot provide adequate enterprise protection because they do not address fundamental weaknesses at an enterprise level. They, in fact, can become the on-ramps for attackers:

- Functional "gray areas" between the stand-alone products remain as entry points for threats.
- There is no unifying architecture or technology foundation that eases the deployment of the applications.
- There is no centralized view or management of the various products that allow effective control and documentation of functions, nor the ability to provide accuracy with regard to reporting requirements.

Again, the answer is a strategic "platform" approach to Internet security. A platform can enable a technology to scale—across increasing numbers of users and physical locations—and be designed to do without degradation in performance or significantly increased complexity of management.

Effective security can simplify compliance

Regulatory compliance raises the stakes significantly in the quest for effective Internet security. Measures such as HIPAA, Sarbanes-Oxley, Basel II and the Gramm-Leach-Bliley Act pose a range of potential legal and financial liabilities. In addition, any findings of non-compliance or the required disclosure of security breaches can yield adverse publicity and the loss of business and brand value. These compliance obligations are and remain the customer's. But an effective security system can be an aid to a customer in fulfilling certain regulatory obligations.

Viewed strategically, Internet security should assist in compliance due to two factors:

- Effective security reduces the likelihood of security failures
- A platform approach to Internet security should facilitate visibility, and thereby assist in necessary reporting.

The elusive holy grail of security

Some in the business world may continue to operate under the belief that they are sufficiently protected by their conventional security systems. Others may settle into a conventional wisdom that the risks are simply unavoidable—that reactive protection is the only alternative.

The elusive vision of security has always been a solution that can stop threats before they impact business—a system that is designed to preempt both known and unknown attacks in an automated, cost-effective fashion.

The fact is, the vision is not out of reach. It simply requires an integrated, preemptive platform approach firmly rooted in vulnerability research. It is the only practical approach because it fulfills three essential requirements:

- It is designed to be effective in preventing security-related business losses.
- It allows security to be planned and managed as a long-term investment by establishing a foundation for evolving security technologies.
- It provides the means for delivering a high level of protection through security services on an on demand basis.

Rethinking what security technology should do

At a functional level, the security challenge is similar to a leaking roof in an intensifying rainstorm. The question is: To stop the leaks and the damage taking place, do you choose a solution that attempts to examine individual rain drops as they fall, or one that finds and fixes the holes in your roof?

At a strategic level, the challenge lies in extending the value of security solutions beyond patching holes in your roof. The question is: What can security intelligence do for your business?

To really understand the nature of security threats, look at the “Swiss cheese” software that runs your business

Businesses depend on software, including business applications, back-office and network operating systems. Virtually all software has vulnerabilities—flaws in the code. As software becomes more complex and evolves through versions and updates, the volume of code is multiplied and the number of flaws increases proportionately. These vulnerabilities are the “holes in the roof” in the rainstorm analogy. This growing number of software vulnerabilities yields an ever-greater number of potential threats because, in theory, any given vulnerability may be exploited by multiple methods. Many of those methods can be highly sophisticated and damaging.

Vulnerability research is one key to the preemptive security platform pioneered by IBM Internet Security Systems. By discovering vulnerabilities before attacks can be launched, IBM Internet Security Systems delivers a security-rich defense against major Internet threats and offers relief from routine emergency patching with an IBM Internet Security Systems Virtual Patch® technology that allows organizations to shield software flaws until permanent patches can be tested and then deployed as a part of normal, scheduled maintenance. In the rainstorm analogy, Virtual Patch technology is similar to a protective tarp that shields the leaking roof until repairs can be made at the owner's convenience.

With preemption as a foundation, a security platform yields business-enabling intelligence

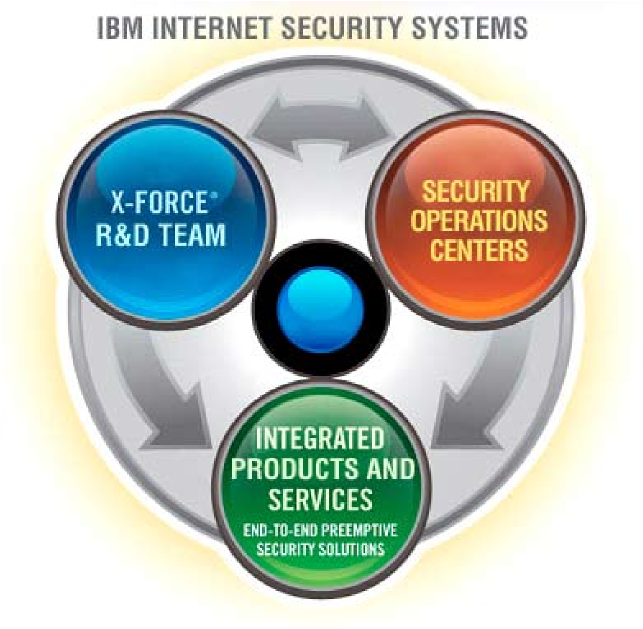
The IBM Internet Security Systems protection platform is constructed to provide centralized visibility and control over the entire enterprise security infrastructure. This approach empowers corporate managers to leverage security as a strategic enterprise asset. The system is designed with the following objectives in mind:

- Vulnerabilities are detected, mapped and remediated.
- Security assets are mapped and centrally managed.
- New users are detected and documented.
- Network bandwidth efficiency is optimized.
- Security conditions and events are documented and reported.
- Patching is managed as routine maintenance.
- Security-related information is efficiently shared across departments and functions.
- Help desk traffic is reduced.
- New applications are tested and evaluated more effectively before general deployment.
- New security applications are deployed and managed on the common platform.
- Risk management processes are more effectively managed.
- Network availability and reliability can be improved.

The IBM Internet Security Systems protection platform

IBM Internet Security Systems is uniquely positioned to provide comprehensive preemptive security, with the combination of three critical elements: 1) superior research and development, 2) a worldwide security operations footprint and 3) a unified security platform.

IBM Internet Security Systems has established its place at the leading edge of security research and innovation, including the invention of vulnerability assessment, intrusion detection and prevention technologies. IBM Internet Security Systems is uniquely qualified among security providers to deliver the preemptive security needed by today's Internet-driven companies. The combination of the IBM Internet Security Systems X-Force® research and development organization, the global scope of IBM Internet Security Systems security operations centers and managed services, and the IBM Internet Security Systems protection platform constitutes the most advanced and complete security solution, delivering a preemptive security capability that has eluded the market for so long.


IBM INTERNET SECURITY SYSTEMS
X-FORCE® R&D TEAM
SECURITY OPERATIONS CENTERS
INTEGRATED PRODUCTS AND SERVICES
END-TO-END PREEMPTIVE SECURITY SOLUTIONS

IBM Internet Security Systems X-Force — the research and development edge

Aggressive, in-depth security research is—and always has been—the core of IBM Internet Security Systems and all of its products and services. The IBM Internet Security Systems X-Force research and development team provides innovative research methods aimed at business applications, back-office and network operation systems that comprise the evolving infrastructure of commerce. This superior grasp of software vulnerabilities provides the foundation for the company's preemptive security solutions.

IBM Internet Security Systems security operations—our "ear to the ground"

Twenty-four hours a day, every day, IBM Internet Security Systems manages the security infrastructure for many of the most security-sensitive companies and government agencies in the world. Overseeing hundreds of globally dispersed networks allows IBM Internet Security Systems a sensitive feel for the pulse of the Internet providing an advantage over unknown exploits. Through multiple security operations centers, IBM Internet Security Systems security specialists analyze "chatter" and suspicious network traffic. They watch and study attack techniques, all while learning how to duplicate them, anticipate them and stop them.

The IBM Internet Security Systems protection platform—the new standard

With the protection platform, IBM Internet Security Systems has created a simple, truly integrated solution that is designed to put preemptive protection within the reach of all security-conscious organizations.

IBM Internet Security Systems provides a family of advanced security applications and services available as stand-alone solutions or together in a modular, integrated system. The IBM Internet Security Systems protection platform is a complete and powerful combination that offers an end-to-end solution. Not only does it incorporate advanced intrusion prevention, anomaly detection, firewall, VPN, vulnerability scanning and anti-virus protection, it is also designed for mail security and Web content filtering. Plus, it can provide end-to-end coverage of the enterprise, with solutions for desktops, servers, networks and gateways. All of the security applications of the IBM Internet Security Systems protection platform can be managed from almost anywhere. There are two delivery options available for the protection platform. Customers can either take a do-it-yourself approach or have IBM Internet Security Systems directly monitor and manage their company network infrastructure.

IBM Internet Security Systems protection platform components constitute a revolutionary architecture that delivers the value of end-to-end security.

- Single, integrated view into the network (compliance, reporting)
- Platform and service extensibility
- Correlations and integration of multiple data sources
- Underlying “best-of-breed” appliances
- Ability to integrate uniquely innovative technologies (e.g., Anomaly Detection Service)
- 24x7 outsourced security management
- Improved system uptime and performance without a large investment in technology or resources
- Security-rich management protection services

Conclusion

Internet-driven organizations no longer have to depend on reactive security techniques. The potential for huge business losses from sophisticated new Internet threats, new compliance pressures and the spiraling cost of managing outdated security approaches are all wake-up calls for corporate management. The optimum security approach for addressing these issues is preemption. Preemptive security requires market-leading research, a keen eye for attack trends and techniques, and a streamlined and affordable platform for delivering advanced security applications that are knowledge-based. Preemptive security is the solution for keeping security-conscious organizations ahead of the threat. Today, IBM Internet Security Systems is uniquely positioned to deliver that solution. IBM Internet Security Systems commands the extensive knowledge, innovative research methods and complex technologies required for preemptive security, and its offering is designed to deliver it all in easy-to-use appliances, software and managed services.

Why 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 security for networks, desktops and servers. An established leader in security, IBM Internet Security Systems 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 preemptive security product line is also complemented by comprehensive IBM Managed Security Services.

To learn more about IBM Internet Security Systems and preemptive security, visit:

ibm.com/services/us/iss

IBM Global Services
Route 100
Somers, NY 10589

Produced in the United States of America
10-06

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.

* Money-back payment (for Managed Protection Services - Premium Level only): If Internet Security Systems fails to meet the Security Incidents Prevention SLA for any given calendar month, Customer's account shall be credited the charges for one full month of the affected Customer's Monthly Monitoring Fee for each instance for which this payment has not been met. Please see IBM Internet Security Systems SLAs for more details.