

## Preemptive security products and services

*Providing protection ahead of the threat*



# Today, security threats to your organization leave little margin for error.

To consistently preempt online enemies that are smart and destructive, your enterprise security must incorporate a constantly evolving array of technologies and technical disciplines—vital assets that few organizations can afford to develop and maintain on their own.

Effective security management is rife with challenges. It requires highly skilled personnel who are expensive to recruit, hire and retain. The process of seeking out these highly skilled professionals can divert scarce IT resources from core activities essential to your company's productivity and growth. This issue is compounded by increasingly stringent government regulations that place additional pressures on businesses to maintain mandated levels of security. Consequently, effectively managing enterprise security can be a delicate balancing act. If enterprise security is improperly managed, it can inadvertently block legitimate traffic, causing lost or delayed transactions, which can undermine customer satisfaction and cut into revenues. Moreover, the spiraling and often unpredictable cost of security can make it difficult for companies to conduct financial planning and resource optimization.



To help you address this complex set of challenges, IBM Internet Security Systems™ (ISS) offers a broad array of centrally managed preemptive products and services built on vulnerability-based research and multilayered security techniques.

### Helping to safeguard the entire IT infrastructure

IBM ISS offers preemptive protection that is tightly integrated with existing IT business processes to help fortify virtually your entire infrastructure—from the gateway to the core to even the most remote endpoints. The foundation of IBM's capabilities is the IBM Proventia® product family. Consisting of anti-virus, firewall, virtual private network (VPN), intrusion detection and prevention, application protection, anti-spam, and content filtering technologies, this robust and comprehensive protection platform is built on security intelligence gathered by the IBM X-Force® research and development team.

The centrally managed Proventia product family includes the following:

- *IBM Proventia Network Intrusion Prevention System* is designed to automatically block malicious attacks while preserving network bandwidth and availability. Based on primary security research conducted by the X-Force team, this security appliance is exceptional in its ability to offer preemptive protection against unknown threats.
- *IBM Proventia Network Multi-Function Security* helps protect more assets at a lower cost, combining intrusion prevention with firewall, VPN, behavioral and signature anti-virus, Web filtering, and anti-spam services. This unified threat management (UTM) appliance is designed to provide automatic protection for more than 1,000 vulnerabilities, more than 120,000 known viruses, more than 93 percent of unknown viruses and other blended threats, and 95 percent of spam.
- *IBM Proventia Network Anomaly Detection System* enhances network intelligence and security by auditing network flow data from existing infrastructure devices. Using network

behavior analysis, this product can help deliver a clear view of the network's vulnerability by automatically detecting active security threats, risky end-user behavior, performance issues and security policy violations.

- *IBM Proventia Network Enterprise Scanner* scans your entire network to identify assets and vulnerabilities, prioritizing and assigning protection activities and reporting on results. Powered by the X-Force team's comprehensive, industry-acclaimed vulnerability database, this product provides vulnerability management using native trouble ticketing supported by workflow capabilities to drive management activities throughout your infrastructure.
- *IBM Proventia Network Web Filter* is designed to block unwanted Web content using sophisticated technology that combines text and image analysis with one of the world's largest URL and image databases. Powerful and accurate, it helps improve productivity and enforce Internet usage policies.

*The foundation of IBM's capabilities is the IBM Proventia product family.*



*IBM ISS offers protection that helps fortify virtually the entire infrastructure.*



- *IBM Proventia Network Mail Filter* monitors the content of e-mail traffic, automatically blocking spam and other undesirable or illegal content. Combining sophisticated analysis techniques with a database containing more than 200,000 relevant samples of spam and more than 20 million Web sites, it identifies harmless e-mail and forwards it virtually instantly, while blocking undesirable e-mail.
  - *IBM Proventia Server Intrusion Prevention System* combines a firewall and application control with preemptive technologies such as buffer overflow exploit prevention and intrusion prevention. This multilayered product receives automatic security content updates to protect vulnerabilities before vendor patches are applied and helps secure servers for both Microsoft® Windows® and Linux® technology-based operating systems.
  - *IBM Proventia Desktop Endpoint Security* is designed to preemptively block attacks before they cause outages, employee downtime and excessive calls to the help desk. This single agent combines a personal firewall, intrusion prevention, buffer overflow exploit prevention, application protection and virus prevention to help ensure that desktops are protected and adhere to corporate standards.
  - The *IBM Proventia Management SiteProtector™* system manages, monitors and measures enterprise security, helping to support regulatory compliance with reports that illustrate due diligence and delivering failover capabilities that help ensure business continuity. By providing one console to manage a comprehensive range of security products, the SiteProtector system reduces demands on IT and security staff and provides enterprise-wide visibility of security posture.
- IBM ISS offers additional products, also aligned with the Proventia product family, that help provide protection ahead of the threat. They include the following:
- *IBM RealSecure® Server Sensor* is designed to provide automated, real-time intrusion protection and detection by analyzing events, host logs, and inbound and outbound network activity on critical enterprise servers to help block malicious activity from damaging critical assets. This robust product applies built-in signatures and sophisticated protocol analysis with behavioral pattern sets and automated event correlation to help prevent known and unknown threats.
  - *IBM RealSecure Network* provides network intrusion detection and response capabilities that monitor network segments within a centralized operational

and management framework. This product supports exceptional network security performance and offers industry-leading accuracy in detecting malicious threats.

### Reducing online threats to critical business assets

IBM ISS complements its product family with world-class security services to help you design, implement and maintain a sound security strategy. IBM Professional Security Services delivers expert security consulting that can help organizations of all sizes reduce risk, achieve regulatory compliance, maintain business continuity and reach their security goals. IBM Professional Security Services consultants are focused on security and use proven consulting methods that are based on the globally accepted International Organization for Standardization (ISO) 17799 best security practices. This team of security experts employs proprietary tool sets, the latest threat intelligence and advanced countermeasures to help you build effective security programs that can protect and enhance business operations.

IBM Professional Security Services includes the following:

- *IBM Penetration Testing* discovers the vulnerabilities in an organization's network and quantifies real-world risks by

conducting demonstrations of covert and hostile activities typical of network attacks in a safe and controlled exercise. More than a typical assessment or network scan, this service is one of the most comprehensive in the industry. Our expert consultants use their expertise to provide a hacker's-eye view of the network and provide thorough deliverables with prioritized, actionable remediation steps to improve security posture.

- *IBM Application Security Assessment* provides a detailed review and targeted code review of custom applications to discover security weaknesses, helps secure applications where valuable data is stored and provides a detailed deliverable with solid recommendations for improving application security.
- *IBM Information Security Assessment* evaluates an organization's overall security posture—including security policies, procedures, controls and mechanisms—as well as physical security, networks, servers, desktops and databases. This comprehensive assessment helps identify vulnerabilities in existing IT infrastructure and gaps in controls, policies and procedures. Based on industry best practices, this service provides organizations with a plan to improve overall security posture.

- *IBM Payment Card Industry Assessment* helps organizations achieve compliance with the Payment Card Industry (PCI) Data Security Standard. IBM ISS is recognized by the PCI Security Standards Council as a Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV). Assessments are conducted by consultants who are certified to conduct PCI assessments. Payment application is also available, delivered by consultants who are Qualified Payment Application Security Professionals (QPASPs).
- *IBM Emergency Response Services* includes incident response, preparedness planning and forensic analysis conducted by our security experts. Available both as a subscription service and an on demand service, the Emergency Response Services team responds quickly to attacks in progress and works with organizations to develop customized emergency response plans designed to help minimize the effect of future attacks. In addition, security experts can assist with computer forensic analysis, discovery and litigation to help find and prosecute perpetrators of information security breaches.

- *IBM Policy Development* defines the strategy and policies that guide critical process, technology, management and administrative decisions to protect IT assets and comply with regulations.
- *IBM Network Architecture Design Services* evaluates existing network architecture and collaborates with security staff to devise a detailed security architecture design to protect an organization's IT environment.
- *IBM Technology Implementation Planning* helps make the most of an organization's existing security technology by developing a plan for implementing security solutions with a minimal effect on network operations. It also helps organizations plan ongoing management and maintenance of their security solution.
- *IBM Deployment Consulting* helps maximize the value of an organization's investment in IBM ISS solutions. IBM ISS security experts assist with installation, configuration and tuning and can also assist when migrating to new IBM ISS solutions.
- *IBM Staff Augmentation* extends internal resources with IBM ISS security experts. Acting as an extension of an existing in-house team, IBM ISS consultants provide cost-effective security know-how, which allows teams to focus on maintaining normal business operations.
- *IBM Vertical & Regulatory QuickStart Programs* can help assess the gaps between existing security and compliance with industry and government regulations, including supervisory control and data acquisition (SCADA), the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act and the Federal Information Security Management Act (FISMA). These programs also provide detailed recommendations for achieving compliance and improving security posture.
- *IBM Security Awareness Training* helps organizations educate their employees about security best practices and policies through an online training program. In addition to providing awareness training, IBM ISS helps organizations get the most out of their investment in IBM ISS solutions with a variety of other training courses offered at client or third-party locations.
- *IBM Security Event and Log Management Services* assembles the collective mindshare of an organization's network applications and operating systems along with disparate security technologies into one seamless platform. This enables an organization to archive, analyze, correlate and trend security and network events, while managing response and

remediation workflow. This service also queries logs across many disparate device types through one common interface, which can dramatically improve the speed of conducting security investigations. Further, IBM ISS also provides archiving of this log data, drastically streamlining regulatory compliance operations.

### Offering real-time, around-the-clock security management

Few organizations have the resources to keep pace with the constantly changing Internet threats that put corporate operations and profits at risk. Enterprise security is a 24x7 endeavor that includes escalating patch-management requirements and device management over a diverse IT landscape. The enforcement of enterprise security policies can also dramatically affect employees, vendors and customers. IBM Managed Security Services offers comprehensive outsourced solutions for real-time security management, including system monitoring, emergency response and 24x7 protection—all at a fraction of the cost of typical in-house security resources.

IBM Managed Security Services offerings include the following:

- *IBM Managed Protection Services* provides preemptive protection backed by performance-based service level agreements and “guaranteed” services that stand out from other security providers. As a result, organizations can rest assured that their security provider has a vested interest in protecting their infrastructure.\* Managed Protection Services offers real-time, around-the-clock monitoring, management and escalation across a variety of platforms and operating systems for networks, servers, desktops and wireless applications.
- *IBM Managed & Monitored Firewall Services* provides comprehensive, 24x7 expert monitoring, management and analysis of firewall logs to detect, prevent and respond to evolving threats. The service comes in a variety of options designed to help maximize existing security investments at a fraction of the cost of in-house solutions.
- *IBM Managed IDS & IPS Services* is designed to help protect networks and servers from attacks originating inside or outside the network perimeter much more cost-effectively than in-house intrusion prevention system (IPS) and intrusion detection system

(IDS) services. The service provides comprehensive, 24x7 monitoring, management and analysis of IDS events, allowing for real-time response and escalation as well as assistance with forensic investigations and recovery.

- *IBM Vulnerability Management Service* is designed to automate the vulnerability management lifecycle while delivering visibility into each area of potential risk. This turnkey service enables sustained business operations by providing real-time management and analysis of servers, firewalls, switches and other devices. It also combines managed scanning services with expert workflow and case management to protect an organization’s network infrastructure from intrusions that could potentially damage its business.
- *IBM X-Force Threat Analysis Service* delivers customized information about a wide array of threats that could affect network security. This service provides detailed and customized analyses of global online threat conditions by combining high-quality, real-time threat information from the international network of IBM ISS security operations centers with security intelligence from the X-Force research and development team.



*Few organizations have the resources to keep pace with the constantly changing Internet threats that put corporate operations and profits at risk.*



## Monitoring security through a centralized command center

The IBM Virtual-Security Operations Center (Virtual-SOC) gives you the ability to see and manage virtually all of your security operations—managed and unmanaged, from IBM ISS or from other vendors—within the Virtual-SOC portal, a single Web-based console. In effect, the Virtual-SOC delivers the power of six IBM ISS global security operations centers to each client's Virtual-SOC portal, with full access to:

- Renowned X-Force team security intelligence
- 24x7x365 monitoring and management
- Comprehensive IBM ISS consulting services
- Trouble ticketing, tracking, alerting, escalation and response
- Reporting, archiving and retrieval
- Live collaboration with IBM ISS security experts.

## Why IBM?

Preemptive security requires industry leading research, a keen eye for attack trends and techniques, and a streamlined and affordable platform for delivering advanced security solutions that are knowledge based. IBM ISS has the extensive knowledge, innovative research methods and complex technologies required to achieve preemptive security. Our experienced and certified consultants, architects, project managers and subject matter experts are prepared to provide your organization with a comprehensive platform of preemptive security products and services designed to protect your entire IT infrastructure, from the network gateway to the desktop.

## For more information

To learn more about IBM ISS products and services, contact your IBM ISS representative to schedule a consultation. Call 1 800 776-2362, send an e-mail to [consulting@iss.net](mailto:consulting@iss.net) or visit:

**[ibm.com/services/us/iss](http://ibm.com/services/us/iss)**

© Copyright IBM Corporation 2007

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

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

IBM, the IBM logo, Internet Security Systems, Proventia, Real Secure, SiteProtector and X-Force are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

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.

---

\* Money-back payment (for IBM Managed Protection Services – Premium Level only): If IBM Internet Security Systems fails to meet the Security Incidents Prevention Guarantee, client shall be paid US\$50,000 for each instance this guarantee has not been met. Please see IBM Internet Security Systems SLAs for more details.