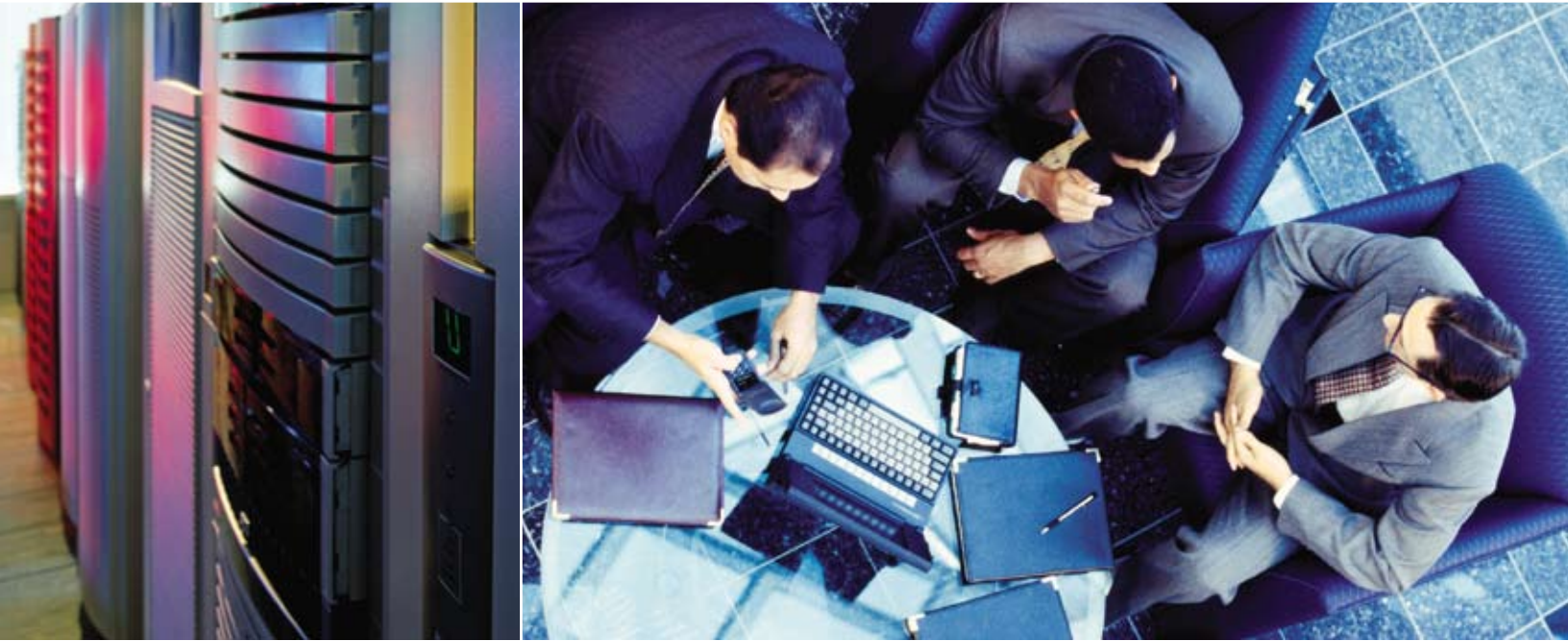


## Preemptive Security Products and Services

*IBM Internet Security Systems™ – 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 the IBM security expertise is the modular product architecture embedded in the Proventia® and RealSecure® brand of product offerings. The security engines fueled by the IBM Internet Security Systems X-Force® research and development team drive security convergence by seamlessly adding entirely new modules of protection as threats evolve. From worms to botnets to data security to Web applications, the IBM ISS security offerings deliver the protection demanded for business continuity, data security and compliance at a lower total cost of ownership.

The centrally managed Proventia product family includes the following:

- The *IBM Proventia® Network Intrusion Prevention System (IPS)* is designed to stop Internet threats before they impact your business and delivers protection to all three layers of the network: core, perimeter and remote segments. Preemptive protection—protection that works ahead of the threat—is

available through its proprietary combination of line-speed performance, security intelligence and a modular protection engine that enables security convergence. By consolidating network security demands for data loss prevention and protection for Web applications, IBM Proventia Network IPS serves as the security platform that reduces the costs and complexity of deploying and managing point solutions. The system is available in multiple hardware models to match the speed of your network, as well as a virtual appliance.

- *IBM Proventia® Network Multi-Function Security (MFS)* helps protect more assets at a lower total cost by combining IPS, Proventia Web application security, content analysis, firewall, VPN, SSL VPN, behavioral and signature-based anti-virus, content filtering, anti-spam and application protection. Backed by the X-Force research and development team, it pulls content from the world's largest vulnerability database to provide protection for thousands of vulnerabilities, offering ahead of the threat detection for both known and unknown threats including viruses and spam. This unified threat management (UTM) system is available in both hardware and a virtual software form factors.

- *IBM Proventia® Network Mail Security System* provides preemptive protection and spam control for your messaging infrastructure. Utilizing X-Force research and technologies, it helps to enforce outbound content compliance and acceptance use policies with customizable analysis modules that easily adapt to various company needs. Designed to provide protection to organizations of all sizes, it is available as both a hardware appliance and a virtual appliance. In either form factor, Proventia Network Mail receives automatic updates to keep spam, viruses and other malicious traffic at bay.
- The *IBM Network Data Loss Prevention solution*, Fidelis Security Systems appliances and support, provides a comprehensive solution that helps prevent data loss through enhanced visibility and control of all network ports and internal traffic. The solution can also simplify day-to-day security management. Powered by Fidelis XPS™ appliances, the solution reduces the risk of sensitive data loss at the network layer. By identifying risky network behavior and dangerous protocols, it can protect all 65,535 ports at multi-gigabit speeds without impeding normal business operations.

*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® Server Protection*  
IBM server security helps to proactively protect servers from malicious attacks while supporting your compliance needs. To combat threats, it combines several protection technologies including IPS, Proventia Web application security, buffer overflow exploit prevention (BOEP), file integrity monitoring (FIM), secure socket layer (SSL) inspection, firewall, OS audit log monitoring and application policy enforcement, into a single, multi-layered software agent. IBM ISS offers the broadest operating support in the industry to guard business critical systems and data helping you to meet stringent audit and compliance standards with two brands:
  - *Proventia Server* providing coverage for Microsoft® Windows®, Linux® and VMware; and
  - *IBM RealSecure® Server Sensor* protecting Microsoft Windows, IBM AIX®, Sun Solaris, and HP-UX.
- *IBM Proventia® Endpoint Secure Control* helps you escape from the constraints of endpoint vendor lock-in with the ability to manage endpoint security products from a single management console. This solution combines many of the key areas of security endpoint management—including intrusion prevention systems (IPS), firewall and network access control; data protection

such as device control, data loss prevention and endpoint encryption; security configuration, and compliance management; as well as IT security operations such as security patch management, and deployment/removal of security tools. The end result can be superior security with increased ease-of-use at a lower overall cost.

- *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 Endpoint Encryption solution*, PGP Corporation encryption software and support, provides a comprehensive solution that helps protect sensitive data across endpoints, removable storage media, and e-mail, against loss, theft or unauthorized access. The solution builds security into the most commonly used applications, protecting data wherever it resides—from outbound e-mail, to file servers, to removable storage devices such as USB flashdrives and PDAs. Multiple encryption applications can also

leverage a single framework to help expedite deployment, reduce operational costs and free administrative resources for other tasks.

- The *IBM Endpoint Data Loss Prevention solution*, Digital Guardian software from Verdasys, provides a comprehensive solution designed to automatically discover and classify sensitive data on desktops and servers and monitor the data as it is exchanged and used, applying automated security controls as necessary to secure it. The solution helps enforce corporate security policies in real-time and reduce the risk of data loss. Whether on PCs, laptops, or servers (inside or outside the organization), the IBM endpoint DLP solution can monitor, log, warn, encrypt and, if necessary, block prohibited actions by trusted end users.
- *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.

- The *IBM Proventia® Management SiteProtector™ system* manages and monitors enterprise security, helping to support regulatory compliance with reports that illustrate an organization's security posture. By providing one console to manage the industries broadest array of security products, the SiteProtector system reduces demands on IT. By designing the SiteProtector system with security professionals, IBM simplifies security analysis with guided analysis and automated correlation techniques. The X-Force team provides the SiteProtector system with powerful help information to decipher the root cause of security threats. An IBM user-community allows SiteProtector users to share and collaborate on security report design, saving time and money.

## Reducing online threats to critical business assets

IBM ISS complements its product family with security services to help you assess, 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) 27002 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 ISS Security Governance Services*  
IBM Security Governance Services helps businesses facilitate a responsive security model that supports business needs and goals. Managing rapid changes in business demands, regulatory mandates and threats from hackers, spy ware, malware and viruses pose a variety of risks to your enterprise. To protect your business,

you need to create a robust, adaptable security framework—one that quantifies and qualifies business risks and balances them with business goals—so that you can conduct business with confidence and efficiency, now and into the future.

- *IBM Security Risk Assessment* allows you to assess the risks facing your information assets—and understand the gaps in your security controls and how to address them. Our security risk assessment provides an in-depth evaluation that encompasses all areas of your business environment. Our experienced security consultants leverage proven tools, practices and methods—including International Standards Organization (ISO) 27002 and 27005 standards, as well as other standards support—to help provide a unified, prioritized view of your security risks and their potential impact on your business. Our security risk assessment can support you in managing regulatory requirements by helping you understand the business risks introduced by information security weaknesses in your processes, organization and IT. We also evaluate the ability of your current security controls to help you mitigate the risks to your business more effectively.
- *IBM Security Health Check* provides a focused, high-level review designed to identify the strengths and weaknesses

in your security controls. Experienced IBM specialists use an interview format and leverage the International Standards Organization (ISO) 27002 or the Control Objectives for IT (CobIT) guidelines to assess the security mechanisms used by your hardware and software systems, networks, databases and personnel. Our comprehensive analysis can help you enhance your current security plan.

- *IBM Security Workshop* provides a high-level overview of your key security challenges. This workshop is designed to help you develop a long-term security plan that's driven by regulatory compliance standards, internal control requirements and well-defined risk management goals, as well as your future business plans and the impact they may have on your current enterprise architecture. The IBM security workshop, which is conducted by two IBM security consultants, provides a cost-effective, one- to two-day, onsite workshop at your location. We customize your workshop based on the identified regulatory mandates and internal controls that are most critical to your business.
- *IBM Information Security Framework* simplifies the planning and execution of your enterprise security program. The IBM Information Security Framework is an integrated and

comprehensive best-practice-driven approach to security. It's based on our research, extensive portfolio of security offerings, and leadership in performing assessments and developing and supporting security solutions for global clients. The framework's best practices address core security themes such as governance, privacy, threat mitigation, transaction and data integrity, identity and access management, application security, physical security and personnel security.

- *IBM ISS Identity and Access Management Services* can help you design, implement, deploy and maintain an integrated identity management system. Such a system can standardize access management across platforms for users, devices, applications and business processes, as well as physical security points such as biometric, smart-card and badge readers. With IBM, you can benefit from a comprehensive portfolio of identity and access management products that offers your choice of an integrated solution or discrete components for a more efficient, cost-effective identity management process that support regulatory compliance.
- *Identity Assessment and Strategy* provides an effective identity and access management (IAM) solution, IBM Identity and Access Management

Services for Identity Assessment and Strategy provides a cost-effective and efficient assessment service that provides a view of current strengths and weaknesses and a clear path for getting started with IAM. Unlike many of our competitors, IBM has many years implementing Identity and Access Management solutions—this extensive experience with implementation has afforded us a deep understanding of IAM and an expertise with the associated technologies so we are very adept at recommending realistic and implementable solutions. Our successful implementation record, combined with the use of our proprietary assessment tool, enables us to evaluate every aspect of identity and access management in an effective and efficient manner—so the customer receives more value in less time. We spend much of our time with our customers on their premises to develop a deep understanding of their unique requirements providing a comprehensive assessment so we are able to develop an appropriate identity and access management strategy to address each customer's specific needs and goals.

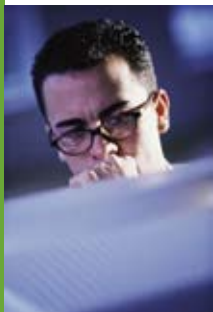
- *Enterprise Single Sign On Services* reduce the adverse impacts of proliferation of application passwords to user productivity, help desk cost, identity security, and compliance

effectiveness. IBM ISS enterprise single sign-on services can help customers plan, design and implement a highly secure, cost-effective, and enterprise-wide single sign-on infrastructure. IBM's world-class consultation and professional services provide a customer with highly skilled and experienced practitioners who can facilitate and enable a highly efficient implementation of a single sign-on system. One that can be fully integrated with TIM or other user provisioning systems for an end-to-end identity management solution.

- *Web Access Management Services* helps protect the client's organization by validating and managing user access. Building on the proven capabilities of the IBM Tivoli suite of identity and access management products, this service can help clients comply with regulations, streamline access protocols and enhance organizational security. IBM helps clients to establish access authorization, validation and single sign-on processes and policies that can be applied and enforced on the organization's web resources.
- *User Provisioning Services* can assist with planning and design, implementation or ongoing identity management. IBM Internet Security Systems can help you establish

*With IBM, you can benefit from a comprehensive portfolio of identity and access management products.*





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

automated processes and policies for managing user identity from initial sign-on to termination. Leveraging IBM Tivoli Identity Manager software and other third-party products, we establish automated processes based on user role authorization and predefined policies, develop workflow escalation criteria for determining when human intervention is required, and implement consistent policy administration and enforcement processes.

- *Managed Identity Services* are designed to help you protect your information by managing user account provisioning and password management, IBM provides a service level agreement-based managed identity service that can help increase user productivity, improve security and compliance, and reduce total cost of ownership. Unlike strategic integrators who only offer outsourcing of your current model with some incremental improvements, the IBM service is designed to transform your identity management processes using industry-leading technology with enhancements only available through this service offering. In addition, creative financing solutions from IBM Credit can help you match the timing of expenditures on the project with the anticipated benefits.

- *IBM ISS Threat Mitigation Services* Understanding your organization's security state and identifying vulnerabilities are the first steps toward protecting the confidentiality, integrity and availability of critical data. These steps are also integral to regulatory compliance efforts. Remaining unaware of security risks can leave your organization vulnerable to attacks targeting the network, or a breach resulting in the loss, misuse or exposure of sensitive data. IBM ISS Threat Mitigation Services provide assessment, planning, design, and remediation services to help you establish the security posture right for your business.
- *IBM Penetration Testing* performs safe and controlled exercises that demonstrate covert and hostile attack techniques and identify vulnerable systems. The services validate existing security controls and quantify real-world risks, providing clients with a detailed security roadmap that prioritizes the weaknesses in the network environment and provides specifies remediation steps.
- *IBM Application Security Assessment* can help clients balance time-to-market demands with security best practices. The application security assessment performs attack simulations and a comprehensive vulnerability assessment of the application and the network infrastructure directly supporting it. IBM

security experts conduct an analysis to identify security weaknesses and misconfigurations and provide detailed recommendations for remediation.

- *IBM Information Security Assessment* provides a comprehensive evaluation of the existing security landscape in relation to industry best practices and regulatory requirements. Consultants not only gather information regarding current controls in place, but also evaluate their effectiveness to identify risks and provide detailed, actionable recommendations for mitigating risks and improving protection. In addition, IBM ISS expert security consultants frame the Information Security Assessment recommendations in terms of your business objectives.
- *IBM Payment Card Industry (PCI) Assessments* help you determine your level of compliance with Payment Card Industry (PCI) Data Security Standard, as well as validate your adherence to PCI requirements. IBM ISS is recognized by the PCI Security Standards Council as a Qualified Security Assessor (QSA), Approved Scanning Vendor (ASV), Payment Application Qualified Security Assessor (PA-QSA), and a Qualified Incident Response Assessor (QIRA). IBM PCI assessments include PCI on-site assessment and certification, PCI quarterly scanning, penetration testing, remediation services, incident response services, and payment

application assessments. IBM PCI assessments help businesses achieve and maintain PCI compliance in accordance with annual audits.

- *IBM Emergency Response Services* includes incident response, preparedness planning and data 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 data analysis, discovery and litigation to help find and prosecute perpetrators of information security breaches.
- *IBM Deployment and Migration Services* help you install effective security solutions to reduce risk. IBM deployment and migration services strive to minimize impact on IT resources and shorten implementation cycles—helping clients achieve better protection faster.
- *IBM Staff Augmentation Services* are designed to provide cost-effective security expertise to organizations for the offloading of critical security management tasks from in-house staff resources. IBM Professional Security Services consultants augment existing resources to handle designated tasks

that promote network security best practices and reduce online threats to your critical business assets.

- *IBM SCADA Assessments* help reduce risk to critical process control systems with thorough identification and analysis of internal and external vulnerabilities that could result in a successful breach. IBM will evaluate the overall effectiveness of the SCADA security management program against industry best practices, identify gaps and recommend action items for improving the security of the environment. The service also works to fulfill regulatory compliance mandates designed to protect critical process control systems from attack
- *IBM Data Security Services* can help you cost-effectively identify and protect your organization's critical data from internal and external threats, offering adaptable solutions for strategy and planning, discovery of sensitive data, designing policies, implementation services and support services for network data loss prevention, endpoint encryption and endpoint data loss prevention. Whether implemented individually or in combination, IBM can help you create data protection solutions for your specific environment. IBM consultants and specialists have experience with a wide range of industry solutions and IT architectures to help organizations of all sizes quickly adopt a data protection solution that supports collaboration

across the enterprise while protecting data in transit or at rest—without slowing your business.

- *Network Data Loss Prevention Services* provide a comprehensive solution for your unique environment that uses market-leading data loss prevention technology to drive consistent coverage from endpoint to network. From policy creation and implementation to continued management and remediation, the solution leverages the IBM security expertise and proven services methodologies designed to stop leakage of sensitive data outside the enterprise and unauthorized movement of data within the enterprise.
- *Endpoint Data Loss Prevention Services* are designed to help clients overcome the challenges associated with deploying a comprehensive endpoint security solution, IBM ISS Endpoint Data Loss Prevention Services provides consulting, a proven implementation methodology and support services.
- *Endpoint Encryption Services* provides a comprehensive solution that helps protect sensitive data across endpoints, removable storage media, and e-mail, against loss or unauthorized access. IBM combines technology, service expertise, and world-class support in a flexible, integrated platform for encryption that provides immediate returns and facilitates expanded coverage in the future.

### 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 and 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 Identity Services* delivers efficient identity lifecycle management technology that can help them manage user account provisioning and password management. At the same time, many organizations do not have the requisite skills to both deploy and support such technology. IBM ISS managed identity services provides a service level agreement—based solution that is designed to help you protect your information from unauthorized users by providing service authorizations only to individuals with a valid business need and removing such authorizations when access is no longer required. IBM provides full lifecycle services from planning and design to implementation to ongoing management.
- The *IBM Managed Security Service for Unified Threat Management (MUTM)* helps protect enterprises from a broad array of threats with 24x7x365 expert monitoring and management for

multi-vendor unified threat management appliances, change management services and security policy design. For a fraction of the cost of traditional solutions, the MUTM service from IBM can help protect critical networks and applications, save valuable time and money, improve overall security posture and help demonstrate compliance.

- *IBM Managed IDS and 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 Security Event and Log Management Service* 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.

- *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.

## Managed Web Security

- The *IBM Managed Web Security* offering helps reduce the threat of spyware and viruses delivered via Web browsing. It also works to automatically enforce Internet usage policies by filtering access to inappropriate or potentially dangerous URLs. As a cloud-based hosted service, IBM Managed Web Security is simple to install, requires no hardware or software investments and very little client management.

## Managed E-mail Security

- *IBM Managed E-mail Security* helps mitigate the inherent risks of e-mail communication. Designed to block both inbound and outbound e-mail containing viruses, worms and spam, the solution can be deployed all the way from the desktop to the outermost edges of the network. IBM Managed E-mail Security helps remove distracting or damaging e-mail from the inbox without adding complexity to the IT environment.



## 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:

- 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 2009

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

Produced in the United States of America  
September 2009  
All Rights Reserved

IBM, the IBM logo, Internet Security Systems, Proventia, RealSecure, SiteProtector, Ahead of the threat 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.

The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.

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.