Delivering preemptive security products and services

IBM Internet Security Systems
products and services

---

**Highlights**

- **Helps protect critical assets and reduce costs by preemption online threats**
- **Helps secure the entire IT infrastructure, freeing IT staff to focus on core business operations**
- **Helps block malicious attacks while preserving network bandwidth and availability**
- **Supports business continuity by reducing downtime due to outages**
- **Improves employee productivity by working to block viruses and spam**
- **Manages, monitors and measures enterprise security to support regulatory compliance.**

---

**Providing protection ahead of the threat**

Today's security threats leave little margin for error. To consistently preempt online enemies that are smart and destructive, 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, and it diverts scarce IT resources from core activities essential to company productivity and growth. And increasingly stringent government regulations are placing additional pressures on businesses to maintain mandated levels of security.

Yet enterprise security is a delicate balancing act: if improperly managed, it can inadvertently block legitimate traffic, causing lost or delayed transactions, which can undermine customer satisfaction and cut into revenues. Finally, the spiraling and often unpredictable cost of security makes it difficult for companies to conduct financial planning and resource optimization.

To help companies meet 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 the entire infrastructure—from the gateway to the core to the most remote endpoints. Foundational to this is the IBM Proventia® product family. Comprising anti-virus, firewall, VPN, intrusion detection and prevention, application protection, anti-spam and content filtering, this robust and comprehensive protection platform is built on security intelligence gathered by the IBM X-Force® research and development team.

The centrally managed family of Proventia offerings includes:

IBM Proventia Network Intrusion Prevention System (IPS) – automatically blocks 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 (MFS) – protects more at a lower cost, combining intrusion prevention with firewall, VPN, behavioral and signature anti-virus, Web filtering and anti-spam. 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 (ADS) – enhances network intelligence and security by auditing network flow data from existing infrastructure devices. Using network behavior analysis, this solution delivers a clear view of the network’s vulnerability by automatically detecting active security threats, risky 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 solution provides vulnerability management using native trouble ticketing supported by workflow capabilities to drive management activities throughout your infrastructure.

IBM Proventia Web Filter – blocks 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.

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 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 solution receives automatic security content updates to protect vulnerabilities before vendor patches are applied and secures servers for both Microsoft® Windows® and Linux® technology-based operating systems.

**IBM Proventia Desktop Endpoint Security** – preemptively blocks 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.

**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 ensure business continuity. By providing one console to manage a complete 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 to provide protection ahead of the threat. They include:

**IBM RealSecure® Server Sensor** – provides 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 offering applies built-in signatures and sophisticated protocol analysis with behavioral pattern sets and automated event correlation to help prevent known and unknown attacks.

**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, helping organizations of all sizes reduce risk, achieve regulatory compliance, maintain business continuity and reach their security goals. IBM Professional Security Services consultants are 100 percent security focused and utilize proven consulting methods, based on the globally accepted ISO 17799 best security practices. This team of security experts employs proprietary
toolsets, the latest threat intelligence and advanced countermeasures to help build effective security programs that protect and enhance business operations. Service offerings include:

IBM Penetration Testing—discovers the vulnerabilities in your 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, our Penetration Testing is the most comprehensive in the industry. Our expert consultants use their expertise to provide a hacker’s-eye view of your network and provide thorough deliverables with prioritized, actionable remediation steps to improve your 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. Provides detailed deliverable with solid recommendations for improving application security.

IBM Information Security Assessment—evaluates your 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 your IT infrastructure and gaps in controls, policies and procedures. Based on industry best practices, the Information Security Assessment provides you with a plan to improve your 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 as an on demand service, the Emergency Response team responds quickly to attacks in progress and works with your organization to develop customized emergency response plans to 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 your staff to devise a detailed security architecture design to protect your IT environment.
IBM Technology Implementation Planning – helps you make the most of your security technology by developing a plan for implementing security solutions with minimal impact to network operations. It also helps you plan ongoing management and maintenance of your security solution.

IBM Deployment Consulting – helps maximize the value of your investment in IBM ISS solutions. IBM ISS security experts assist you with installation, configuration and tuning and can also assist you when migrating to new IBM ISS solutions.

IBM Staff Augmentation – extends your internal resources with IBM ISS security experts. Acting as an extension of your in-house team, IBM ISS consultants provide cost-effective security know-how and allow your team to focus on maintaining normal business operations.

IBM Vertical and Regulatory QuickStart Programs – assess the gaps between existing security and compliance with industry and government regulations, including Supervisory Control and Data Acquisition (SCADA), Sarbanes-Oxley (SOX), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act and Federal Information Security Management Act (FISMA). 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 you get the most out of your investment in IBM ISS solutions with a variety of other training courses offered at client or third-party locations.

Offering real-time, round-the-clock security management
Very few organizations have the resources to keep pace with the ever-changing Internet threats that put corporate operations and profits at risk. Enterprise security is a 24x7 proposition that includes escalating patch-management requirements, device management over a diverse IT landscape and the enforcement of security policies that can impact 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. They include the following:

IBM Managed Protection Services (MPS) – offers the industry’s leading performance-based service level agreement (SLA), enabling easy and confident transition of network protection to a trusted security partner. These protection solutions go beyond simple event monitoring and device management by offering performance-based SLAs that will provide clients with a cash payment of US$50,000 for a security breach.* 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 to maximize existing security investments at a fraction of the cost of in-house solutions.

IBM Managed IDS & IPS Services – helps protect networks and servers from attacks originating inside or outside the network perimeter at a significantly lower cost than in-house intrusion prevention system (IPS) and intrusion detection system (IDS) solutions. The service provides comprehensive, 24x7 monitoring, management and analysis of IDS events, allowing for real-time response and escalation, as well as offering assistance with forensic investigations and recovery.

IBM Security Event and Log Management Service – helps organizations assemble the collective mindshare of disparate security technologies into one seamless platform to archive, analyze, correlate and track trends in security and network events, while managing response and remediation workflow. Clients also have the ability to query logs from applications and operating systems across many disparate device types through one common interface. This dramatically improves the speed at which security investigations can be conducted across large numbers of devices. Further, IBM ISS also provides archiving of this log data, drastically streamlining regulatory compliance operations. For customers needing to subsidize internal SOC staff during off-peak or holiday hours, IBM SOC event monitoring provides live monitoring of IDS and IPS systems on as-needed or regularly scheduled terms.

IBM Vulnerability Management Service (VMS) – automates 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 your network infrastructure from intrusions that could potentially damage your business.

IBM ISS X-Force Threat Analysis Service (XFTAS) delivers customized information about a wide array of threats that could affect network security. Combining high-quality, real-time threat information from the international network of IBM ISS security operations centers with security intelligence from the renowned X-Force team, this service provides detailed and customized analyses of global online threat conditions.

Monitoring security operations through a centralized command center

The IBM ISS Virtual-Security Operations Center (Virtual-SOC) gives organizations the ability to see and manage all of their security operations, managed and unmanaged, from IBM ISS or from other vendors, all within the Virtual-SOC portal, a single Web-based console. In effect, the Virtual-SOC delivers the power of the IBM ISS own six 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 Internet Security Systems?
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 commands 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 Internet Security Systems 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 or visit: ibm.com/services/us/iss