IBM Security Solutions

# Security products and services to manage risk across the enterprise

*Providing protection ahead of the threat*

IBM

# 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 or inappropriately prohibit legitimate users from accessing business-critical information, 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 Security Solutions offers a broad array of centrally managed preemptive products and services built on vulnerability-based research and multilayered security techniques.

*IBM Security Solutions. Secure by Design.*

## Helping to safeguard the entire IT infrastructure

IBM Security Solutions offer 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. Security engines fueled by the IBM 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 security offerings deliver the protection demanded for business continuity, data security and compliance at a lower total cost of ownership.

The IBM Security Solutions product family includes the following; all can be centrally managed:

- The IBM Security Network Intrusion Prevention System (IPS) (formerly, IBM Proventia® Network Intrusion Prevention System) is designed to stop Internet threats before they impact your business. 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 Security 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, 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 IBM 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 protection for both known and unknown threats including viruses and spam. This unified threat management (UTM) system is available in multiple hardware models.
- IBM Security Server Protection (formerly, IBM Proventia® Server Protection) helps to proactively protect servers from malicious attacks while supporting your compliance needs. To combat threats, it combines several protection technologies including IPS, 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 Security Server Protection 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 protection for Microsoft® Windows®, Linux® ,VMware, IBM AIX ®, Sun Solaris, and HP-UX®.

*IBM Security Solutions help organizations build a strong security posture to help reduce costs, improve service, and manage risk.*

- IBM Security Virtual Server Protection for VMware® offers integrated threat protection for VMware vSphere™ 4 that provides protection for every layer of the virtual infrastructure, including host, network, hypervisor, virtual machine (VM) and traffic between VMs. The solution leverages VMware VMsafe™ integration to offer protection that is scalable, isolated, centralized, visible and efficient. Providing multilayered intrusion prevention and firewall, the solution enforces automatic VM discovery in order to reduce VM sprawl, provides VM rootkit detection and virtual infrastructure auditing, and offers inter-VM traffic analysis. The solution also helps to accelerate and simplify your PCI DSS audit, and achieve compliance with security and reporting functionality customized for the virtual infrastructure. Virtual Server Protection helps reduce cost and complexity over using physical security solutions in virtual infrastructures with automatic protection features, including automatic protection, discovery and assessment features and IBM Virtual Patch® Technology.

- 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.
- 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 IBM 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 Security SiteProtector™ System (formerly, 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 industry's 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 IBM 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.

IBM Security Solutions also offer a comprehensive portfolio of security solutions to address the people, processes, and information risks in your environment, while helping you improve service delivery and reduce cost. These solutions offer comprehensive, end-to-end security across identities, data and information, applications, processes, and infrastructure. Automated compliance management capabilities are integrated with each offering, closing the loop from controls and management to audit and compliance. By establishing an integrated compliance management mechanism throughout these offerings, synergies are established to help ensure consistent compliance across platforms and to improve customer value.

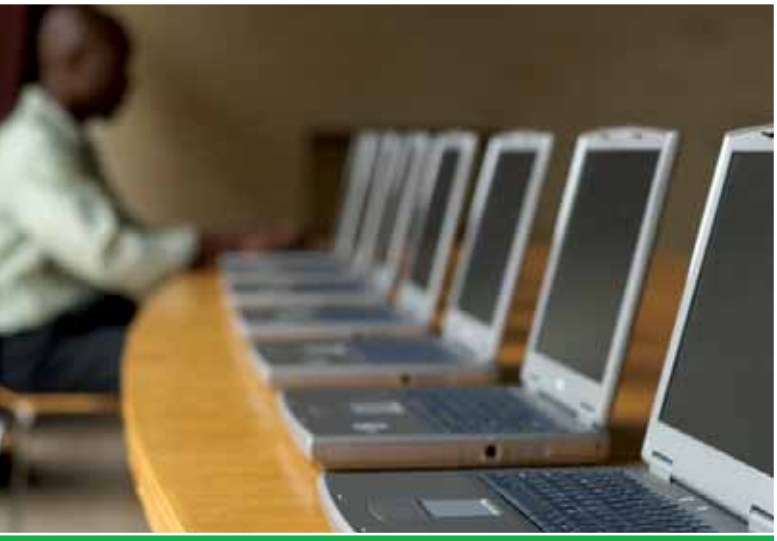
- IBM Tivoli® Identity and Access Assurance can help organizations ensure that the right users have access to the right information in a timely manner, providing comprehensive identity management, access management, and user compliance auditing capabilities. The solution centralizes and automates the management of users, then closes the identity and access loop, providing industry-leading capabilities not only for assigning and enforcing user access rights, but also for monitoring user activity and for detecting and correcting situations that are out of compliance with security policy.
- IBM Tivoli® Data and Application Security is a comprehensive solution that helps organizations protect data and applications by providing auditable access controls, enabling fine-grained control of user privileges, and centralizing management of data encryption keys. This solution provides end-to-end protection of sensitive data both in enterprise storage systems and within critical applications, helping organizations support regulatory compliance initiatives and improving data and application reliability.
- IBM Tivoli® Security Management for z/OS enhances the flagship security of the IBM z/OS platform by providing integrated, automated and simplified mainframe security capabilities. Organizations can pro-actively enforce security policy compliance on Resource Access Control Facility, prevent internal security errors, identify noncompliant security commands, and issue alerts when risky security commands are issued. Simplified security administration and more effective user management improves productivity with group and role-based task administration. Comprehensive monitoring for threat incidents, audit configuration changes, and resource usage can help detect changes to established baselines, abuse of privileges, and insider threats. Comprehensive compliance capabilities with cross-platform log collection, sophisticated data analysis and prepackaged reporting across operating systems, applications and databases help demonstrate compliance with industry regulations, government regulations and standards such as PCI, SOC, GLBA, HIPAA, FISMA and BASEL II. This solution brings together key functionality from the IBM System z security software portfolio to help exploit the mainframe as their enterprise security hub.

## Reducing online threats to critical business assets

IBM 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 Security Governance, Risk and Compliance Services help businesses facilitate a proactive 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 Governance, Risk and Compliance Services - 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 Governance, Risk and Compliance Services - 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 Governance, Risk and Compliance – security policy planning and development help clients rapidly create and deploy comprehensive security policies, standards, guidelines and operating procedures that are designed to align with best practices and satisfy regulatory compliance requirements. As part of the services, IBM experts evaluate clients' existing policies and practices to help ensure documentation is developed in accordance with business goals and the ISO 27002 framework. The security policy program will help set the direction for investment in security controls and security management and satisfy regulatory compliance requirements. At the end of the service engagement, clients will have a comprehensive security policy in place, along with documentation, training, communication and maintenance procedures. IBM can meet a full spectrum of policy development needs—from high-level governing policies down to specific operating procedures.
- IBM Security Governance, Risk and Compliance Services - Payment Card Industry (PCI) security assessment helps you determine your level of compliance with Payment Card Industry (PCI) Data Security Standard, as well as validate your adherence to PCI requirements. IBM 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.



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

- IBM Security Governance, Risk and Compliance – enterprise security architecture offers a cost-effective and efficient assessment service which delivers a high quality plan for a client's enterprise security architecture using an advanced set of models, security design guidelines, patterns and templates.
- IBM Security Governance, Risk and Compliance – IBM Privacy Services helps clients who need to manage information privacy within the entire organization establish a management framework to initiate and control the implementation of information security and privacy.
- IBM Security Governance, Risk and Compliance Services - information security framework simplifies the planning and execution of your enterprise security program. The information security framework from IBM is an integrated and comprehensive best-practice-driven approach to security. 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 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.

- IBM Identity and Access Management Services for identity assessment and strategy provides a cost-effective and efficient assessment service that includes a view of current strengths and weaknesses and a clear path for getting started with and identity and access management (IAM) solution. IBM works with each client on their premises to develop a deep

understanding of their unique requirements, in order to develop an appropriate identity and access management strategy to address each customer's specific needs and goals.

- IBM Identity and Access Management Services for enterprise single sign-on reduce the adverse impacts of proliferation of application passwords to user productivity, help desk cost, identity security, and compliance effectiveness. Our enterprise single sign-on services can help customers plan, design and implement a highly secure, cost-effective, and enterprise-wide single sign-on infrastructure. The IBM 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.
- IBM Identity and Access Management Services for Web access management 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.
- IBM Identity and Access Management Services for user provisioning can assist with planning and design, implementation or ongoing identity management. IBM can help you establish 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, IBM establishes automated processes based on user role authorization and predefined policies, develops workflow escalation criteria for determining when human intervention is required, and implements consistent policy administration and enforcement processes.
- IBM Identity and Access Management Services - managed identity services are designed to help clients protect their 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. The IBM service is designed to transform 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 organizations match the timing of expenditures on the project with the anticipated benefits.
- IBM Identity and Access Management Services – total authentication solution is designed to be a cost-effective, enterprise wide, and fully integrated solution to help clients establish a security-rich authentication infrastructure for strong authentication across a variety of consumer-oriented business applications or corporate IT infrastructure components. With the ability to choose hardware or software authentication methods based on your unique security risk, deployment cost and usability requirements, IBM total authentication solution can help organizations manage evolving security and regulatory challenges.
- IBM Identity and Access Management Services for user activity compliance management helps provide centralized and demonstrable automated log collection and storage from heterogeneous sources. The service helps address demands of regulators and auditors by establishing clear audit trails for incident response, reducing the risks associated with security incidents and data breaches and monitor and audit the actions taken by privileged users, helping prevent costly damages or outages due to inadvertent mistakes or malicious actions. IBM helps clients leverage market-leading technologies, services expertise and proven methodologies to deploy and manage an integrated security solution.

### IBM Infrastructure Security Services

Understanding an 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 Infrastructure Security Services provide assessment, planning, design, and remediation services to help clients establish the security posture right for their business.

- IBM Infrastructure Security Services - 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 Infrastructure Security Services - 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 expert security consultants frame the information security assessment recommendations in terms of your business objectives.
- IBM Infrastructure Security Services - 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 Infrastructure Security Services - deployment and migration services help you install effective security solutions to reduce risk. Deployment and migration services from IBM strive to minimize impact on IT resources and shorten implementation cycles—helping clients achieve better protection faster.
- IBM Infrastructure Security Services - staff augmentation service is 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 Infrastructure Security Services - Supervisory Control and Data Acquisition (SCADA) assessment helps 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.

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

**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.

- IBM Data Security Services - network data loss prevention provides 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.
- IBM Data Security Services - endpoint data loss prevention is designed to help clients overcome the challenges associated with deploying a comprehensive endpoint security solution. Endpoint data loss prevention from IBM provides consulting, a proven implementation methodology and support services.
- IBM Data Security Services – encryption provides a comprehensive solution that helps protect sensitive data across endpoints, removable storage media, and email, 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.

IBM Professional Security Services also include the following services for application security:

- IBM Application Security Services - 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 Application Security Services – application source code security assessment is designed to identify vulnerabilities in applications early in the software development lifecycle to help reduce risk and cost of remediation. The service can also help meet compliance requirements for application security testing. Built on a "testing-as-a-service" model, IBM leverages its market-leading Rational®AppScan®Source Edition software without requiring customers to acquire or maintain any software.

## 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 device management and cloud security 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 Infrastructure Security Services - managed protection services (MPS) 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 from IBM 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 Infrastructure Security Services - firewall management 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 Infrastructure Security Services - unified threat management helps protect enterprises from a broad array of threats with 24x7x365 expert monitoring and management for multi-vendor unified threat management UTM appliances, change management services and security policy design. For a fraction of the cost of traditional solutions, this service from IBM can help protect critical networks and applications, save valuable time and money, improve overall security posture and help demonstrate compliance.

- IBM Infrastructure Security Services - Intrusion detection and prevention system management 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 Application Security Services - secure Web gateway management is designed to help reduce risks associated with web-based threats and protect your online transactions by managing your secure web gateway devices.

- IBM Identity and Access Management Services - 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. Managed identity services from IBM 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.

## IBM Managed Security Services (Cloud Computing)

- IBM Managed Security Services - hosted security event and log management assembles the collective mindshare of an organization's network applications and operating systems along with disparate security technologies into one seamless platform. This cloud security service 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 also provides archiving of this log data, drastically streamlining regulatory compliance operations.
- IBM Managed Security Services - hosted vulnerability management 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® hosted 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 security operations centers with security intelligence from the X-Force research and development team.
- IBM Managed Security Services (Cloud Computing) - hosted email and Web security offerings help reduce the threat of spam, spyware and viruses delivered via web browsing and in-bound and outbound email. They work to automatically enforce Internet usage policies by filtering access to inappropriate or potentially dangerous URLs and help remove distracting or damaging email from the inbox without adding complexity to the IT environment. As cloud security services, hosted email and Web security from IBM is simple to install and requires no hardware or software investments and very little client management.

## 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 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 Security 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 consulting services
- Trouble ticketing, tracking, alerting, escalation and response
- Reporting, archiving and retrieval
- Live collaboration with IBM security experts

## Why IBM?

IBM has the extensive knowledge, innovative research methods and complex technologies required to deliver products and services that are recognized for leadership in IT security. IBM builds security technology into the fabric of the hardware, software and services it delivers – not bolting it on after the fact. As your trusted partner for security, IBM 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 Security Solutions and IBM Security Services, contact your IBM representative or visit: ibm.com/security



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

Produced in the United States of America
June 2010


SEB03007-USEN-02