Defend your data with broader, deeper server protection

IBM ISS Threat Mitigation Services – endpoint system protection – server protection

Highlights

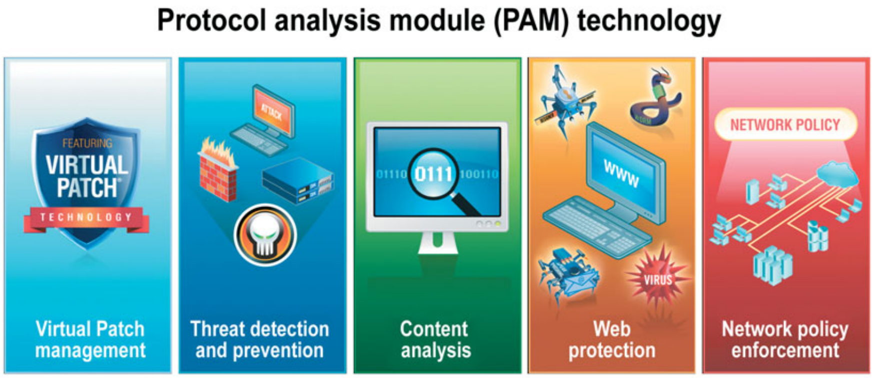
- ***Designed to protect against multiple types of attacks, including those tunneling through encrypted Web transactions***
- ***Combines multiple inspection technologies to offer superior protection at the deepest network levels***
- ***Helps ensure data confidentiality and ease regulatory compliance through extensive monitoring***
- ***Aids in reducing cost and complexity through centralized security management and extensive support for multiple operating systems***
- ***Helps you realize the benefits of virtualization***

Deepening your defense strategy

Every year, one in two organizations suffers a serious security breach—costing an average of $6.6 million per breach—despite having a firewall and antivirus protection in place[1]. And while operating system and application patches attempt to stem the continual waves of attacks, hackers are increasingly stealing sensitive data through Web applications, as can be seen by the exponential growth in Web attacks. Internal breaches, unintentional or deliberate, are also a continuing source of potential security hazards.

Backed by IBM Internet Security Systems™ (ISS) X-Force® research and development team, IBM Internet Security Systems – server protection delivers multilayered intrusion prevention and detection to help protect your servers from growing methods of attack and more thoroughly manage compliance through extensive monitoring, recording and auditing capabilities.

IBM ISS – server protection is enabled in two proven products: IBM Proventia® Server Intrusion Prevention System (IPS) and IBM RealSecure® Server Sensor. Each supports a broad range of operating systems and provides robust security against numerous attacks, including denial of service, remote exploit, SQL injection and cross-site scripting.


Protocol analysis module (PAM) technology

The IBM protocol analysis module (PAM) drives security convergence to deliver network and server protection that goes beyond traditional IPS.

Protecting servers while maintaining maximum throughput and uptime

Security is the sum of its parts. Unlike other server protection solutions, IBM ISS – server protection provides deep packet inspection as one of its six layers of security. Among their blocking capabilities, Proventia Server IPS and RealSecure Server Sensor offer:

- *A **firewall** that puts you in control by enabling you to decrease the number of threats both from resourceful, external hackers and from internal sources who might have better aim at your vulnerabilities.*
- *An **intrusion prevention system** that utilizes multiple layers of defense to help provide accurate, preemptive protection against system, network, application-level and internal threats.*
- ***IBM Virtual Patch® technology**, which helps prevent known and unknown attacks regardless of whether a vulnerability patch has been issued.*
- ***Buffer overflow exploit protection (BOEP)** to help prevent the exploitation of known and unknown buffer overflow vulnerabilities.*
- ***Application black and white listing**, which helps you enforce the application policy to reduce the number unauthorized applications running, thereby decreasing server exposure to malicious activity.*
- *The **ability to inspect secure Web transactions** before they're delivered to the Web application.*

IBM ISS – server protection features the protocol analysis module (PAM), a deep packet inspection engine, which is core to all IBM ISS security technology. Combining multiple inspection technologies, PAM goes far beyond what other server protection solutions offer to provide comprehensive, proactive defense. Furthermore, IBM ISS – server protection integrates seamlessly with your existing IT infrastructure to preserve legitimate traffic flows without interruption, so you can keep your business running smoothly while shielding data with malware delivery protection.

Easing data confidentiality and regulatory compliance measures

To help you manage compliance with standards and regulations, such as the Payment Card Industry (PCI) Data

Security Standard (DSS) and the Health Insurance Portability and Accountability Act (HIPAA), as well as internal security standards, IBM ISS – server protection incorporates four types of monitoring:

- ***System integrity monitoring*** *alerts you of user interaction with the operating system and applications and provides information about who logged in, what actions they took and when they logged off.*
- ***File integrity monitoring*** *helps you meet intensive data integrity standards like Sarbanes-Oxley by monitoring user interaction with sensitive files and folders. The key use of this technology is to detect system tampering and to monitor access to sensitive data.*
- ***Registry integrity monitoring*** *also helps you meet data integrity standards by monitoring and recording successful and failed actions taken on registry keys, creating a forensic trail of administrative and user behavior–essential for some standards reporting–that can home in on potential vulnerability points.*
- ***Third-party log monitoring*** *helps keep track of events triggered by third-party applications that are potential security threats.*

In addition, IBM ISS – server protection incorporates antivirus enforcement to confirm that servers are receiving the latest antivirus updates and report non-compliant servers. Proventia Server for Microsoft® Windows® is certified by NSS Labs for host intrusion prevention systems (HIPS) and PCI compliance.

Simplifying security across a broad range of operating systems

IBM ISS – server protection is designed to provide intrusion prevention and detection across a broad array of enterprise operating systems, including Microsoft Windows, Linux®, IBM AIX®, UNIX®, Solaris and HP-UX. At the same time, it gives you simple, guided control over the entire solution through the IBM Proventia Management SiteProtector® system for security devices, policies, events analysis, alerts and workflows. Through a single interface, you can monitor, analyze, make adjustments and generate reports—without sinking time and money into deploying and learning multiple management tools.

Optimizing IT operations through virtualization

IBM ISS – server protection is virtual-environment ready to help you achieve the return on investment (ROI) that server virtualization offers while helping to maintain security at the server and operating system levels. Virtual machine-centric protection secures intra-virtual network communications by analyzing network traffic going to and from virtual machines where the HIPS agent is installed. Another key benefit is the support of mobility by maintaining persistent protection while traveling with the virtual machine as it is moved from physical host to physical host. IBM ISS – server protection is designed to deliver continuous security, providing support for the following environments:

- *VMware ESX*
- *Windows Server 2008 Hyper-V*
- *IBM Power Systems™ logical partitions and workload partitions*
- *Hewlett-Packard vPars and nPars*
- *Solaris Container*

Why IBM?

IBM ISS – server protection is backed by the world-renowned X-Force team, which maintains the most comprehensive vulnerability database in the world and whose research and threat analysis have contributed to the development of security solutions that stay ahead of the hackers. Consulting services and skilled service professionals from IBM can help with your solution assessment, design and deployment or more comprehensive management. IBM Managed Protection Services (MPS) offers real-time, around the clock protection and live, expert management, monitoring and escalation for critical server devices across a variety of platforms and operating systems.

For more information

To learn more about IBM ISS – server protection, please contact your IBM representative or IBM Business Partner, or visit the following Web site:

ibm.com/services/security

IBM reserves the right to change specifications or other product information without prior notice. This publication could include technical inaccuracies or typographical errors. IBM PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions; therefore this statement may not apply to you. Use of the information herein is at the recipient's own risk. Information herein may be changed or updated without notice. IBM may also make improvements and/or changes in the products and/or the programs described herein at any time without notice.

Any performance data for IBM and non-IBM products and services contained in this document was derived under specific operating and environmental conditions. The actual results obtained by any party implementing such products or services will depend on a large number of factors specific to such party's operating environment and may vary significantly. IBM makes no representation that these results can be expected or obtained in any implementation of any such products or services.

Any material included in this document with regard to third parties is based on information obtained from such parties. No effort has been made to independently verify the accuracy of the information. This document does not constitute an expressed or implied recommendation or endorsement by IBM of any third-party product or service.

[1] CSI/FBI Computer Crime & Research Survey and Ponemon / PGP: U.S. Cost of a Data Breach Study.

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

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

IBM, the IBM logo, ibm.com, AIX, Internet Security Systems, Power Systems, Proventia, RealSecure, SiteProtector, Virtual Patch and X-Force are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at **ibm.com**/legal/copytrade.shtml

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

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product or 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.

Disclaimer: 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.