



IBM RealSecure Server Sensor

Protect critical assets from cyber-threats

IBM RealSecure® Server Sensor from IBM Internet Security Systems (ISS) is designed to help protect business-critical servers from both internal and external threats. Its real-time intrusion detection and prevention helps reduce network security costs while protecting enterprise server environments and reducing downtime. RealSecure Server Sensor analyzes events, host logs, and inbound and outbound network activity on critical enterprise servers to help block malicious activity from damaging critical assets. The solution applies built-in signatures and sophisticated protocol analysis to prevent known and unknown attacks.

Benefits

- Provides preemptive protection against system/network-level, application-level and internal threats
- Utilizes multiple layers of defense to combat numerous threat vectors
- Combines a server firewall with vulnerability-centric intrusion prevention and comprehensive system auditing capabilities
- Establishes security controls through customized policies to help enterprises meet and exceed internal compliance standards
- Supports regulatory compliance with preemptive protection that maps to existing infrastructure and processes
- Helps to protect at-risk systems with IBM Virtual Patch® technology before vendor-supplied patches are available
- Aids in maintaining server integrity through customizable registry and file monitoring
- Supports operating system (OS) migration paths, helping to sustain continuous protection for virtually any major operating system
- Helps to reduce system administrator workload through centralized management with IBM Proventia® Management SiteProtector™ systems
- Offers up-to-date security intelligence powered by the IBM Internet Security Systems X-Force® research and development team

Features and capabilities

RealSecure Server Sensor is designed to preemptively combat threats and address vulnerabilities at the network and application levels while performing security compliance auditing.

Analyze and block network-based threats

RealSecure Server Sensor is designed to protect against network vector attacks, including worms, bot worms, Trojans and denial-of-service (DoS) attacks, through a local firewall and inline vulnerability-centric intrusion prevention. RealSecure Server Sensor includes:

- Firewall
- Advanced intrusion prevention/blocking
- Protocol analysis module (PAM)
- Centralized management

Analyze and block application-level threats

RealSecure Server Sensor's layered intrusion prevention inspects and blocks application traffic with malicious code activity, including applications running on both Apache and Internet Information Services (IIS) Web servers. RealSecure Server Sensor provides:

- Preemptive Web application protection with Secure Sockets Layer (SSL) inspection
- HTTP/application protection
- Buffer-overflow exploit prevention*

**Available for Microsoft® Windows® operating system only*

Perform security compliance auditing

RealSecure Server Sensor helps you achieve regulatory compliance and provides centralized management of OS audit policies to protect vulnerabilities that arise from application design, development or deployment flaws. This also helps ensure that all critical servers have a consistent audit policy to protect data confidentiality and accessibility by monitoring logins, privilege escalations and other system-level activity. RealSecure Server Sensor integrates with the existing infrastructure and enables:

- Policy management and enforcement auditing
- Log monitoring
- Registry integrity monitoring
- OS auditing
- File integrity monitoring

Operating systems

RealSecure Server Sensor supports the following operating systems:

- Microsoft Windows NT® 4.0
- Microsoft Windows 2000 Server, Advanced Server
- Microsoft Windows Server 2003 Standard, Web and Enterprise Editions
- Sun Solaris 8, 9 and 10 (64-bit and 32-bit SPARC)
- IBM AIX® 5.1, 5.2 and 5.3 (64-bit and 32-bit POWERPC)
- HP-UX 11.0, 11.11 and 11.23 (64-bit and 32-bit PA-RISC)
- VMware ESX 2.5

Please reference the RealSecure Server Sensor product page online for the latest in operating system support: www.iss.net/products/RealSecure_ServerSensor/product_main_page.html



For more information

Contact the IBM Internet Security Systems office nearest you for an onsite demonstration. Ask your IBM ISS representative about evaluating complementary security systems, including:

- IBM Proventia Management SiteProtector
- IBM SecurityFusion™
- IBM Proventia Network Enterprise Scanner
- IBM Proventia Desktop Endpoint Security

For locations and additional product information, visit:

ibm.com/services/us/iss

© Copyright IBM Corporation 2007

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

Produced in the United States of America
04-07
All Rights Reserved

IBM, the IBM logo and AIX are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Proventia, RealSecure, SecurityFusion, SiteProtector, Virtual Patch and X-Force are trademarks or registered trademarks of Internet Security Systems, Inc., in the United States, other countries, or both. Internet Security Systems, Inc., is a wholly-owned subsidiary of International Business Machines Corporation.

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

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products or services do not imply that IBM intends to make them available in all countries in which IBM operates.

Information in this document concerning non-IBM products was obtained from the suppliers of these products, published announcement material or other publicly available sources. The network operating system (NOS, sometimes referred to as "operating system") has been tested with that particular system and will run on that system. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All performance data contained in this publication was obtained in the specific operating environment and under the conditions described above and is presented as an illustration. Performance obtained in other operating environments may vary and customers should conduct their own testing.