

## Compliance and data loss prevention support with IBM RealSecure Server Sensor



---

## Product Highlights

---

- **Compliance focus to simplify and support organizational compliance requirements**
- **Provides data loss prevention and preemptive protection support while enforcing corporate security policies for servers**
- **Helps ensure system integrity, data confidentiality and policy compliance with internal and external standards**
- **Protects operating systems and applications from known and unknown threats with integrated firewall and vulnerability-centric intrusion prevention**
- **Supports a broad range of network operating systems and platforms, including Windows, AIX, HP-UX, and Solaris**
- **Provides controls to guard against insider threats**
- **Integrates seamlessly with existing IT infrastructure to preserve legitimate traffic flows without interruption.**

### **Protect servers from internal and external threats while meeting compliance demands**

Your business's most critical assets are under attack. Trusted insiders are threatening servers at increasing rates, as advanced hacker techniques target business critical systems while evading traditional security technology. Simultaneously, the regulatory environment is placing more emphasis on monitoring server access. Now more than ever, server security is paramount to business operations, data integrity and regulatory compliance.

IBM RealSecure® Server Sensor proactively supports compliance, protecting the enterprise as a whole. To combat threats from all angles, the RealSecure Server Sensor combines several protection technologies into a single multi-layered agent. RealSecure Server Sensor guards your business critical systems and data from attacks from the outside and from within, helping you meet stringent audit and compliance standards. The solution is also designed for ease of use and offers broad operating system and platform support.

### **RealSecure Server Sensor helps enterprises achieve and maintain regulatory compliance**

RealSecure Server Sensor helps enterprises strictly enforce security policies to keep sensitive data confidential and critical systems operational. With centralized management of operating system (OS) audit policies, RealSecure Server Sensor protects against vulnerabilities that arise from flawed application design or deployment. The solution also enforces a consistent audit policy for all critical servers by monitoring logins, privilege escalations and other system-level activity through the following technologies and processes:

- **File integrity monitoring** – monitors the who, what, when, and where of sensitive file activity; includes critical system binaries and configuration files
- **Network access policy enforcement** – sets port and IP restrictions for inbound server traffic
- **Application-level intrusion detection and auditing** – detects and responds to application-level attacks or unauthorized activity
- **OS event and log monitoring** – tracks attempted user and group additions and modifications, as well as privilege escalations; can provide attack forensics

**Data Loss Prevention using multi-layered preemptive protection**

Server security is a critical component of your organization’s data loss prevention strategy. RealSecure Server Sensor’s multi-layered prevention technology guards against threats from internal and external attacks. Today’s hybrid attacks and sophisticated cyber-criminals can break through conventional defenses, and no single technology is adequate to protect servers from the variety of modern threats. Powerful multi-layered protection from IBM Internet Security Systems™ (ISS) is designed to block attacks before they can cause damage and compromise sensitive data. With robust, multi-layered protection from a single agent, RealSecure Server Sensor is easier to manage than the variety of security technologies needed to combat sophisticated threats.

RealSecure Server Sensor includes the following security technologies:

- **Firewall** – blocks unauthorized access to ports and IP addresses, preventing IP spoofing and terminal hijacking
- **Intrusion Prevention System (IPS)** – uses both signature-based and protocol-based analysis to prevent known and unknown attacks
- **Buffer Overflow Exploit Prevention (BOEP)** – recognizes and prevents malicious code targeting memory buffer vulnerabilities (Windows)

- **Web Application Protection** – protects Web applications running on both Apache and IIS Web servers by inspecting Secure Sockets Layer (SSL) encrypted traffic (Windows and Solaris only)
- **IBM Virtual Patch® technology** – automatically applies protection for vulnerabilities before vendor-supplied patches can be installed

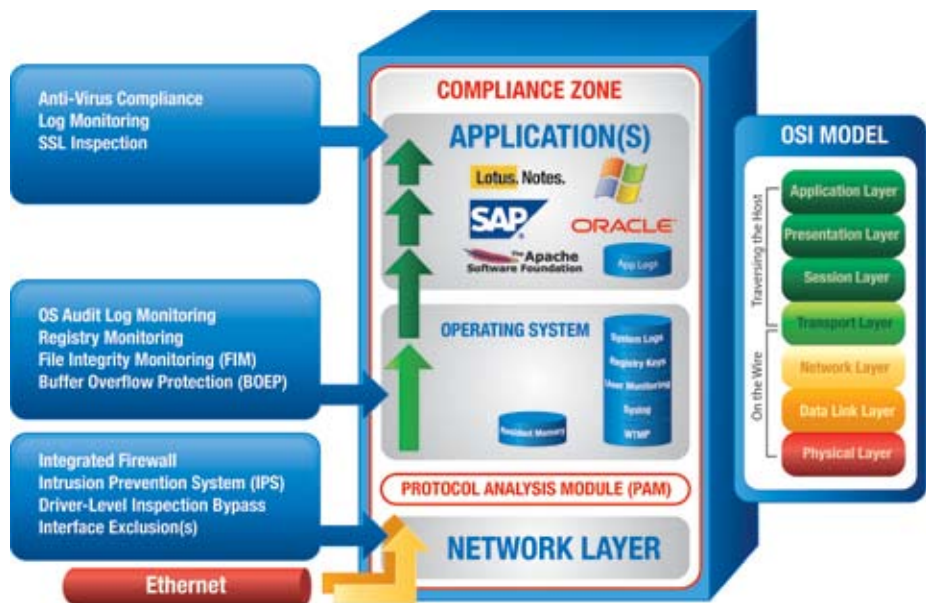
**Receive broad operating system support from the RealSecure Server Sensor**

Most enterprises rely on a variety of server platforms to keep the business functioning, and do not want a piecemeal server security solution introducing even more complexity in the IT environment. For this reason, IBM designed the RealSecure Server Sensor to work with

many different platforms, including both recent and legacy releases of Microsoft® Windows®, Solaris, IBM AIX® and HP-UX. Security that covers a broad range of operating systems is easier to implement, manage and maintain – resulting in a lower total cost of ownership.

**RealSecure Server Sensor is designed for ease of use**

Centrally managed by the IBM SiteProtector™ system, RealSecure Server Sensor is designed to work with existing IT infrastructure. RealSecure Server Sensor integrates with Active Directory, allowing grouping structures to manage policies, monitor events and create reports. The software is



RealSecure Server Sensor – multi-layered protection against internal and external threats.



designed to have minimal impact on server resources and to not interfere with legitimate traffic.

### **IBM ISS offers reliability through research**

RealSecure Server Sensor includes built-in security intelligence from the IBM Internet Security Systems X-Force® research and development team. The X-Force team's world-renowned threat and vulnerability intelligence is infused into RealSecure Server Sensor to help stop emerging threats and enhance Proventia's reliability and accuracy.

IBM ISS also tracks Internet threat levels around the world from its Global Threat Operations Center (GTOC) in order to enhance the protection from RealSecure Server Sensor. When new threats appear, GTOC security analysts are among the first to observe them and subsequently alert Proventia customers.

### **For More Information**

To learn how the RealSecure Server Sensor multi-layered protection can keep your critical servers safe from online threats, and help you meet compliance regulations, or to schedule an onsite demonstration please visit

**[www.ibm.com/services/](http://www.ibm.com/services/)** or contact 1 800 IBM 4YOU (4968).

© Copyright IBM Corporation 2007

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

Produced in the United States of America.  
11-07  
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, 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 and Windows are trademarks or registered 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.

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.

1. For Windows and Linux operating systems only

The IBM home page on the Internet can be found at **[ibm.com](http://ibm.com)**