

RealSecure® Server Sensor

Every organization relies on servers to run applications and host data to drive their business. Any disruption of service can result in customer dissatisfaction, lost revenue and increased costs. New vulnerabilities, or exploits of existing vulnerabilities, put your systems at risk for intrusion and constantly threaten the vital operations of these key systems. Securing server environments, while enabling them to keep applications running, continues to be a challenge.

The Solution

RealSecure® Server Sensor protects servers from the growing threat spectrum while enabling them to keep data and applications reliable, available and confidential. This centrally-managed enterprise protection agent combines a proven intrusion prevention system with powerful firewall capabilities to protect servers. Real-time monitoring and analysis of the operating system, applications and network activity guard server environments from misuse and intrusions with little to no impact on the performance of the system.

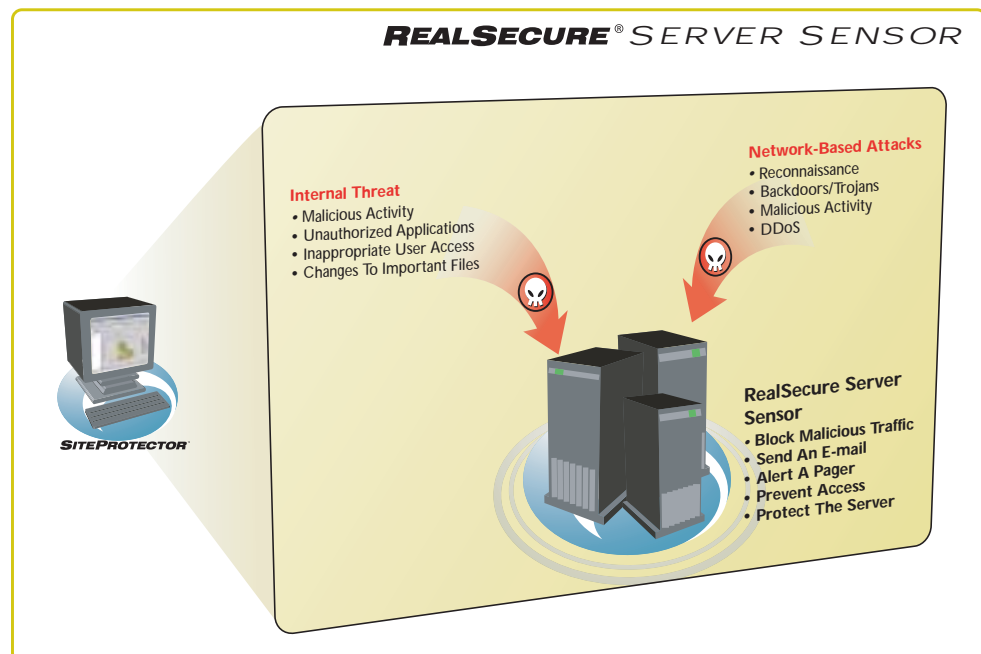
Features & Benefits

RealSecure Server Sensor provides automated, real-time intrusion detection and protection by analyzing events, operating system logs and inbound/outbound network traffic on enterprise servers, blocking malicious activity from damaging critical assets. Utilizing the ISS Protocol Analysis Module (PAM), Server Sensor applies a combination of sophisticated protocol analysis with behavioral pattern sets and automated event correlation. This dramatically reduces security costs and downtime by preventing both known and unknown attacks.

Web Application Protection – Server Sensor protects Web applications by inspecting traffic for malicious activity and is capable of adding an additional level of protection to those applications running on both Apache and IIS Web servers by inspecting Secure Sockets Layer (SSL) encrypted traffic.

Benefits

- Provides increased protection against complex Internet threats such as Nimda and Code Red
- Safeguards confidential data from loss or theft
- Allows you to enforce security according to policy
- Prevents both console and network-based attacks
- Maximizing system uptime
- Reduces security related costs



Advanced Intrusion Prevention/Blocking – Monitors all inbound and outbound traffic to detect and prevent attacks, both known and unknown. This includes buffer overflows, Trojans, brute force attacks, unauthorized access and network worms, along with many other types of attacks.

Local and Network-Based Protection – Provides the flexibility to detect and protect from both local and network attacks through log monitoring capabilities. This prevents authorized users from attacking the system, while also preventing brute force attacks and unauthorized access to system resources that would otherwise compromise data confidentiality, integrity and accessibility.

Audit Policy Management – Centralized management of an OS audit policy ensures that all critical servers have a consistent and effective audit policy that allows for the management of true kernel-level auditing.

Centralized Management – Server Sensor is incorporated into Internet Security Systems' SiteProtector™ central management application. This management console unifies the administration of enterprise protection across gateways, networks, servers and desktops, significantly reducing demands on staff and other operational resources.

SiteProtector™ SecurityFusion™ Module – This plug-in module for SiteProtector uses built-in X-Force® security knowledge to dynamically escalate threatening security incidents while reducing false alarms. The module instantly correlates security data from multiple sources to escalate serious threats, such as an attack on a vulnerable asset or a covert, multi-step attack.

Backed by the X-Force® – Internet Security Systems' X-Force® organization is a leading group of security experts dedicated to proactive counter-intelligence and public education against online threats. X-Force researches security issues, tracks the evolution of threats through ISS' Global Threat Operations Center, and ensures that ISS is the first to bring new threat management solutions to market. With more than 250 years of combined experience, the X-Force organization possesses a wide range of expertise in security management strategies and tactics. This deep understanding of distributed computing, global networking, programming and forensics keeps the X-Force at the forefront for combating the latest developments in online security.

System Requirements

Operating Systems Supported

- Microsoft Windows Server 2003
- Microsoft Windows 2000
- Microsoft Windows NT 4.0
- Sun Solaris
- RedHat Linux
- IBM AIX
- Hewlett-Packard HP-UX

Refer to the *System Requirements* document for additional details on platforms supported.

Microsoft Windows Server 2003 and Windows 2000 Server Certified

RealSecure Server Sensor is certified on the following platforms by VeriTest, the authorized worldwide lab to test enterprise applications for Microsoft's "Certified for Windows" program:

- Windows Server 2003 Standard Edition
- Windows Server 2003 Enterprise Edition
- Windows Server 2003 Datacenter Edition
- Windows 2000 Server
- Windows 2000 Advanced Server
- Windows 2000 Datacenter Server

This rigorous test is endorsed for business-critical applications by analysts and enterprise customers alike because it verifies features and functionality that make applications more robust and manageable.

The full Certification Report from VeriTest is available at: <http://cert.veritest.com/CfWreports/server/SearchResults.asp?co=1391&lo=0&bs=Search&pr=0&pc=0>



Copyright © 1996-2003 Internet Security Systems, Inc. All rights reserved worldwide.

Internet Security Systems, the Internet Security Systems logo, X-Force, System Scanner, and X-Press Update are trademarks, and a registered trademark, of Internet Security Systems, Inc. Other trademarks and trade names mentioned are marks and names of their owners as indicated. All other trademarks are the property of their respective owners and are used here in an editorial context without intent of infringement. Specifications and content are subject to change without notice.

Doc. Rev. 3.2