

RealSecure® Server Sensor

Organizations rely on critical servers to run applications and host data to drive their business. New intrusions, exploits and vulnerabilities, discovered daily, continue to threaten the vital operations of these key servers. As a focal point for attacks, securing server environments while enabling them to keep data and applications running continues to be a challenge.

The Solution

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

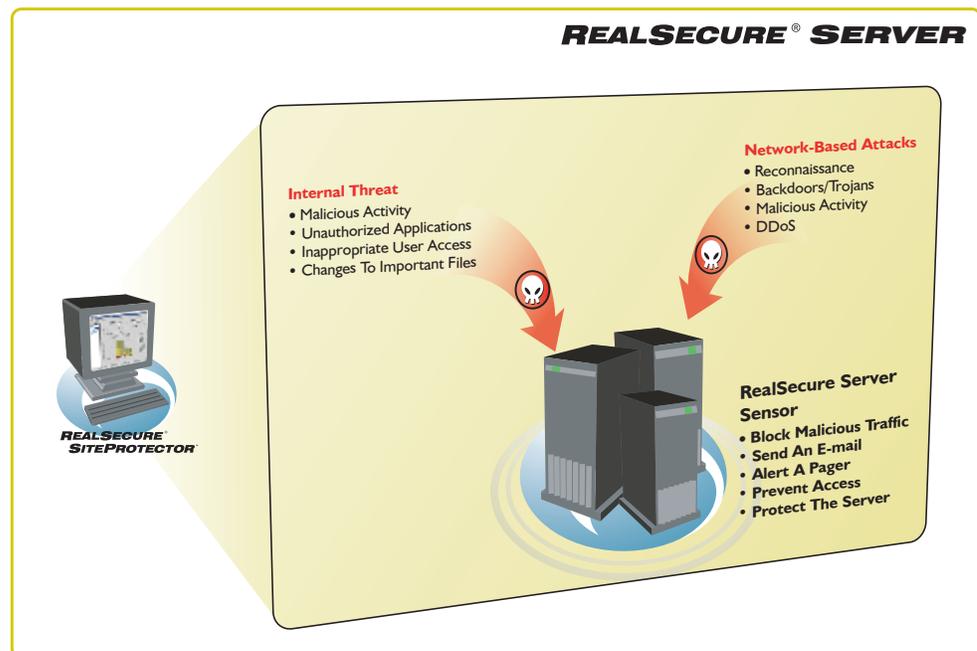
Features & Benefits

RealSecure® Server Sensor – Provides automated, real-time intrusion monitoring, detection and protection by analyzing events, host logs and inbound and outbound network activity on critical enterprise servers to block malicious activity from damaging critical assets. RealSecure Server Sensor applies over 500 built-in signatures and sophisticated protocol analysis with behavioral pattern sets and automated event correlation to prevent both known and unknown attacks. RealSecure Server Sensor dramatically reduces security costs while protecting enterprise server environments and reducing downtime.

Web Application Protection – RealSecure Server Sensor provides Secure Sockets Layer (SSL) encrypted application layer intrusion monitoring, analysis and response capability for both Apache and IIS web servers.

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 traffic to and from the server or network to detect and prevent inbound attacks as well as block new and unknown outbound attacks such as buffer overflows, Trojans, brute force attacks, unauthorized access and network worms.

Console and Network-Based Intrusion Protection – RealSecure Server Sensor provides you with the flexibility to detect and prevent both console and network-based attacks through log monitoring capabilities, preventing local users from launching attacks which are undetected by network protection agents, while also preventing brute force attacks and unauthorized access to critical 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 – With RealSecure® SiteProtector™ management console, customers can control, monitor and analyze their server protection system from one central site with minimum impact to staff operations.

RealSecure® Security Fusion Module – Is the first plug-in module for RealSecure SiteProtector. The Security Fusion Module 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™ – The X-Force™ organization underpins all of Internet Security Systems' products and services. X-Force is the most respected security research group in the industry, having researched and identified security issues in products from Cisco, Microsoft, IBM, Sun, Hewlett-Packard, Oracle, Peoplesoft, BMC, Polycom, Apache and many more. This cutting-edge research team actively turns security research into product improvements, allowing Internet Security Systems' customers to respond far more rapidly to evolving threats. X-Force researches security issues, tracks the evolution of threats through its Global Threat Operations Center and quickly delivers protection against the very latest threats and vulnerabilities.

System Requirements

RealSecure Server Sensor:

Operating System

- *Microsoft Windows*
- *Solaris*
- *RedHat Linux*
- *AIX*
- *HPUX*