



RealSecure® Server Sensor for ISA Server

The *RealSecure® Server Sensor for ISA Server* application provides comprehensive intrusion protection against attacks specifically targeted at Microsoft ISA Server and the networks the server defends. As ISA Server monitors traffic across the network perimeter, RealSecure Server Sensor works as a real-time alarm, continuously monitoring, alerting and responding to unauthorised or suspicious network behaviour. RealSecure Server Sensor protects against network attacks that operate across the firewall — including HTTP, FTP, buffer overflows, and back doors — by leveraging protection policies and log-based signatures specific to ISA Server. Designed specifically for smaller networks, RealSecure Server Sensor for ISA Server features low operational overhead and simple, straightforward administration.

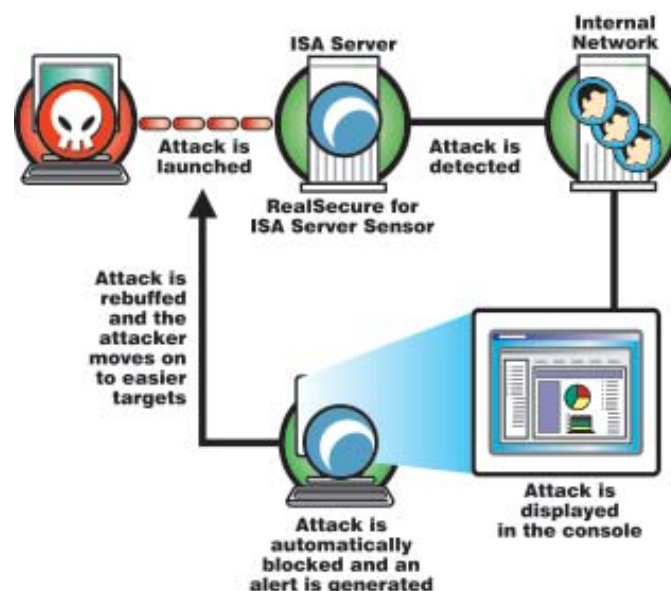
Designed, tested and tailored to co-reside on the same host and protect both the ISA Server and networks protected by the ISA Server against attacks or misuse, RealSecure Server Sensor for ISA Server is an inexpensive, easy-to-install and highly effective security solution. It allows ISA Server users to stay ahead of the curve with technology that shields them against the broadest range of attacks and misuse.

RealSecure Server Sensor for ISA Server offers perimeter intrusion detection by constantly monitoring all network traffic passing through the combined host for signs of malicious intent. Once an attack is detected, the product can log the event, instantly alert the selected security administrator and automatically block the attack — constantly protecting against the latest threats to valuable information assets.

While the ISA Server acts as the “security guard” for networks, deciding which traffic is allowed to pass, RealSecure Server Sensor for ISA Server takes on the role of an alarm system, continuously monitoring, alerting and responding to unauthorised or suspicious network behaviour in real-time.

Specially Designed for ISA Server

Internet Security Systems and Microsoft previously worked together to provide ISA Server customers with several built-in, network-based intrusion detection checks. RealSecure Server Sensor for ISA Server expands this protection by using Internet Security Systems’ industry leading RealSecure Server



Sensor technology to provide both host- and network-based intrusion protection. The product is a fully functioning intrusion protection system containing hundreds of checks, which are easily and automatically updated to protect against the latest threats as they are discovered. In addition to normal RealSecure functions, Server Sensor for ISA Server contains protection policies specific to the ISA Server, using log-based signatures designed to alert on relevant ISA Server events.

RealSecure Server Sensor for ISA Server offers protection by detecting any network-level attacks that pass through the firewall including HTTP, FTP, buffer overflows and back doors. Critical events such as ISA Server filter failure or critical server errors are also tracked, identified and an alert is immediately passed along to the system administrator. The ISA Server also protects the computer running the ISA server itself by watching user and group configurations, monitoring critical files and watching for unexpected OS processes.

Tailored, Cost-Effective Solution

Designed for smaller networks with lower bandwidth requirements, utilising Network Address Translation (NAT) and no DMZ hosts, RealSecure Server Sensor for ISA server provides protection for those networks behind the host upon which it resides — as packets must pass through the host for the analysis to take place.

The RealSecure Server Sensor for ISA Server Advantage

Easy to install and manage – Features custom ISA Server intrusion detection policy with specific event alerts.

Comprehensive intrusion protection – Builds on the Internet Security Systems network-based attack signatures already embedded in the ISA Server to protect both ISA Server and the networks and systems behind it using NAT.

Automatically responds to improper activity – Responses include log events to a database, record a complete session for playback and forensics, kill a connection, block a connection, send an email, send a SNMP trap, suspend an account, disable an account, reconfigure a firewall, or create a user defined alert.

Common console – The same console is used to monitor events and alerts in real-time for both ISA Server and RealSecure Server Sensor for ISA Server.

Eliminates the need for a dedicated intrusion detection host – Installs on the same host as ISA Server.

Automatic product updates – Self-installing **X-Press Update™** product enhancements for RealSecure's attack signature database and program code ensure that the latest network security information is available and active. In addition, RealSecure sensors are remotely upgradeable, including full release updates.

Backed by the ISS X-Force™ – Internet Security Systems' X-Force delivers world-class security research and development for all Internet Security Systems offerings. The X-Force is Internet Security Systems' team of leading computer security scientists and intelligence officers. These information security professionals provide an invaluable edge in managing online risk and protecting key online digital assets. For more information about the ISS X-Force, visit the X-Force Web site at <http://xforce.iss.net>.

More information about *RealSecure Server Sensor for ISA Server* is available from the Internet Security Systems Web site at www.iss.net/isaserver.

System Requirements

RealSecure Server Sensor system requirements are available online in the Product Literature section of the Internet Security Systems Web site at www.iss.net.

Get Started Today

To get started securing your key information assets with RealSecure Server Sensor for ISA Server, contact a security consultant at your local Internet Security Systems office or visit our Web site at www.iss.net.

Belgium/Luxemburg: +32 2 479 67 97, be-info@iss.net

France: +33 1 55 38 00 88, fr-info@iss.net

Germany: +49 711 7819 080, de-info@iss.net

Ireland: +44 20 7653 9191, ieinfo@iss.net

Italy: +39 02 42290950, italy-info@iss.net

Middle East: +202 760 70 11, middleeast-info@iss.net

Netherlands: +31 10 286 26 00, nl-info@iss.net

Poland: +48 601 24 18 26, pl-info@iss.net

Scandinavia: +46 8 545 67 200, nordic-info@iss.net

Spain/Portugal: +34 916369879, es-info@iss.net

Switzerland/Austria: +41 1 842 6600, ch-info@iss.net

United Kingdom: 0800 085 2976 (+44 20 7653 9191 outside the UK), ukinfo@iss.net

About Internet Security Systems (ISS)

Founded in 1994, Internet Security Systems (ISS) (Nasdaq: ISSX) is a world leader in software and services that protect critical online resources from attack and misuse. ISS is headquartered in Atlanta, GA, with additional operations throughout the United States and in Asia, Australia, Europe, Latin America and the Middle East.

Copyright © 1996-2002 Internet Security Systems, Inc. All rights reserved worldwide. Internet Security Systems, the Internet Security Systems logo, X-Press Update and X-Force are trademarks, and RealSecure a registered trademark, of Internet Security Systems, Inc. Other trademarks and trade names mentioned are marks and names of their owners as indicated. All 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.