



INTERNET
SECURITY
SYSTEMS™

**RealSecure® Network Sensor and
Gigabit Network Sensor
Frequently Asked Questions**

Updated March 2003

RealSecure® Network Sensor and Gigabit Network Sensor Frequently Asked Questions

As part of the RealSecure Protection platform, RealSecure Network Sensor and Gigabit Network Sensor combine powerful application-level protocol analysis and sophisticated pattern-based detection technologies to protect 10/100/1000Mbps network segments. Supporting commonly deployed operating system environments, RealSecure Network Sensor and Gigabit Network Sensor deliver detection and response capabilities that provide proven performance and accuracy. Centrally managed by RealSecure® SiteProtector™ and backed by X-Force™ security knowledge to keep the product up to date with newly emergent threats and vulnerabilities, customers can effectively monitor and protect their networks with minimal impact on staff or operations.

This document answers the most frequently asked questions regarding RealSecure Network Sensor and Gigabit Network Sensor, specifically questions pertaining to Version 7.0.

RealSecure Network Sensor and Gigabit Network Sensor Version 7.0

1. What are the current versions and platforms for RealSecure Network Sensor and Gigabit Network Sensor?

The current versions and platforms for RealSecure Network Sensor and Gigabit Network Sensor are as follows:

Network Sensor 7.0

- *Windows 2000 – sp2*
- *RedHat Linux 7.3*
- *Solaris – 7, 8 (32 and 64 bit)*

Gigabit Network Sensor 7.0

- *Windows 2000 – sp2*
- *RedHat Linux 7.3*

Network Sensor 6.5

- *Nokia IPSO – 3.4 or above (On the following platforms: IP120, IP330, IP350, IP380, IP440, IP530, IP650, IP710, IP740)*

For complete, up-to-date system requirements go to:

<http://www.iss.net/support/documentation>.

2. What are the key benefits of RealSecure Network Sensor and Gigabit Network Sensor 7.0?

- **Ease of deployment** – Can be installed on a broad variety of hardware or purchased in appliance form factor.
- **Easy installation** – Wizards and installers guide the user through deployment and initial set-up.
- **Easy maintenance** – X-Press Update™ security releases keep the agents up-to-date, while full remote upgrades allow for simplified updates to the latest version.
- **Top Performance** – RealSecure Network Sensor supports fully utilized 10Mbps, 100Mbps half and full-duplex networks. RealSecure Gigabit Network Sensor supports 1000Mbps or Gigabit network segments.
- **Powerful network protection** – Using a combination of sophisticated protocol analysis and pattern matching to interpret network activity, it detects known attacks and previously unknown attacks with unprecedented accuracy.
- **Sophisticated responses** – By providing a broad range of responses, RealSecure Network Sensor and Gigabit Network Sensor protect as well as provide critical data required for attack investigation. The user-defined response allows any application to be used to respond to a detected attack, allowing for integration with paging solutions, trouble ticket systems, or other event management solutions.

- **Centralized Management** – With the RealSecure SiteProtector™ management console, customers can control, monitor and analyze their security protection systems from one central site with a minimum of staff and operational costs.

3. What new features exist in RealSecure Network Sensor and Gigabit Network Sensor 7.0?

- **Hybrid detection technology** – Employs a powerful combination of sophisticated, 7-layer protocol analysis and attack pattern matching detection technologies to interpret network activity. This technique is the most accurate and modern method of intrusion detection and is used to foil hacker evasion techniques, even detecting some attacks before they become widely known.
- **Cutting edge accuracy and performance** – Performance and attack detection on fully utilized 10Mbps, 100Mbps half and full-duplex networks for RealSecure Network Sensor as proven in the recent NSS Group report (<http://www.nss.co.uk>). RealSecure Gigabit Network Sensor is OSEC certified, verifying its performance and accuracy for gigabit network segments.
- **Standard user defined signatures** – In addition to its advanced analysis engine, the agent can import most of the published rules for the Snort open-source intrusion detection system. Users can take advantage of X-Press Update product enhancements and publicly posted Snort rules. This enables companies to leverage their experience with unsupported network-based intrusion detection systems and upgrade to a commercially available, fully supported family of protection products without significant new training.
- **Advanced event consolidation** - Reduces the total number of unique events that the agent generates to consolidate and significantly reduce stress on the IDS communications architecture, increasing data storage efficiency by a factor of ten or more in real-world environments.
- **Automatic product updates** – Updates through secure, authenticated methods. X-Press Update product enhancements provide additional and newly developed security coverage, including integrated help, up to and including full remote upgrades. X-Press Updates can all be applied from the GUI without having to go to the agent. This allows for the application to be updated with minimal user intervention.
- **Dynamic correlation and analysis** – The RealSecure SiteProtector security fusion module allows for the aggregation, correlation, investigation and response to attack data and elimination of false alarms.

4. What new features will BlackICE enterprise customers notice in Network Sensor and Gigabit Network Sensor 7.0 versus previous versions of Sentry?

- All previous RealSecure signatures
- Classic RealSecure 6.x 3-tiered management architecture
- RealSecure® SiteProtector™ and RealSecure Workgroup Manager management
- No support for RealSecure ICEcap® Manager
- Token Ring and FDDI Support on Windows, FDDI on Unix
- Input Filters, Connection Events, and User-defined signatures with RegEx
- Linux, Solaris, Nokia IPSO support
- Responses: OPSEC Firewall-1, SNMP traps, email, user defined actions

5. How has licensing changed?

There are two Network Sensor license types. In addition to the regular 10/100 Network Sensor license, there is a new Gigabit Network Sensor license that permits the agent to handle Gigabit network speeds. Full-Duplex capabilities are permitted with the regular 10/100 Network Sensor license and therefore do not require any special licensing provisions.

6. How can I best take advantage of Network Sensor performance enhancements?

The Network Sensor supports high-performance packet capture drivers specially designed for the 3com 3C905C/CX, SysKonnnect SK-9843 and Intel Pro/1000 F network interface cards. Although Network Sensor will work with most any 10/100Mbit PCI-based bus mastering adapters that support promiscuous mode, to obtain full utilization coverage of a 100Mbit network, or to handle full-duplex operations, you must use a 3C905C/CX and associated driver on Windows 2000. You must use the Intel Pro/1000 F NIC and associated driver to enable gigabit operations on Windows 2000. You must use the SysKonnnect SK-9843 NIC and associated driver to enable gigabit operations on RedHat Linux. Installation instructions for the high-performance drivers are detailed in the RealSecure Network Sensor and Gigabit Network Sensor Installation Guide bundled with the product.

7. Does RealSecure Network Sensor 6.5 work with SiteProtector?

Yes, RealSecure 6.5 works with SiteProtector. Furthermore, if you wish to add RealSecure 6.5 to the Deployment Manager, copy the “web” package (single EXE) to the Deployment Manager. Refer to the SiteProtector documentation for complete details.

Upgrades

8. What are Full Remote Upgrades?

The Full Remote Upgrade process allows for older versions of the Network Sensor or Server Sensor to be easily upgraded to the current version.

9. How do I upgrade?

Important notes regarding Network Sensor 7.0 full remote upgrades:

- To remotely upgrade RealSecure 5.x and 6.x Network Sensors to 7.0, all components must first be updated to version 6.5. This generally entails manually upgrading Workgroup Manager infrastructure (consoles, databases and event collectors) to 6.5 and either manually or remotely updating Network Sensors to 6.5 before updating to 7.0.
- To update the Workgroup Manager to version 6.6 (which fully supports the functions of Network Sensor 7.0), console connectivity must be established with a Network Sensor 7.0. This implies that if you are updating the RealSecure 6.5 console and a Network Sensor 6.5, you would need to establish connectivity to the Network Sensor 6.5 first, then download and apply the Network Sensor 7.0 Full Upgrade package. The newly upgraded Network Sensor 7.0 in turn will automatically send the 6.6 Console Update package to the Console.
- If you plan to update a previous version of Network Sensor to use one of the new high-performance 3C905B-C or Intel Pro/1000 F packet drivers, you will need to manually install this driver on each agent subsequent to a remote Full Upgrade. This procedure applies to Full-Duplex, high-performance 10/100 and Gigabit Network Sensor operation. An additional gigabit license is required for Gigabit operation.

10. What versions of Network Sensor can be upgraded using full remote upgrades?

Network Sensor 7.0 will be capable of upgrading the following platforms:

5.0, 6.0 Network Sensor (after upgrading to 6.5)

- *Solaris 7, 8*
- *Windows 2000*

6.5 Network Sensor

- *Solaris 7, 8*
- *Windows 2000*

11. I customized my previous install, what is going to happen when I perform a Full Remote Upgrade?

The Full Remote Upgrade process maintains the current settings. This includes:

- Non-default directories
- Non default agent names
- Existence of network monitoring components

General Questions

12. What kinds of threats do RealSecure Network Sensor and Gigabit Network Sensor recognize?

RealSecure Network Sensor and Gigabit Network Sensor recognize two types of threats against the enterprise network:

- **Attacks** - Activity patterns indicating that someone may be engaged in malicious, unauthorized, or otherwise undesirable activity involving the systems and/or data on your network. Examples of these include Denial of Service attacks (such as WinNuke, SYN Flood, and LAND), Unauthorized Access Attempts (such as Back Orifice access and Brute Force login), Pre-Attack Probes (such as SATAN scans, stealth scans, and connection attempts to non-existent services), Suspicious Activity (such as TFTP traffic), attempts to install backdoor programs (such as rootkit or BackOrifice2000), attempts to modify data or web content, and attempts to stop services or kill programs.
- **Misuse** - Non-attack activity that violates stated security or appropriate use policy. Examples of these include abuse of administrator privilege (installation of inappropriate services), HTTP activity (who's surfing the net and where they're going), analysis of access to Windows shares (e.g., connections from engineering to accounting), and e-mail session decoding.

13. Why do I need both network and host-based agents?

Network and host-based agents are necessary because the data that each type of agent generates is very complementary. Network-based intrusion detection is very good at providing early warning of attacks. By monitoring the traffic stream in real-time, a network agent can see a threat and often neutralize it before it has a chance to do any damage. However, network agents cannot tell you whether an attack was successful or not. The information they manage is very network-centric. Host-based agents provide confirmation of an attack's success or failure and they yield system-specific event data, such as user name and file name during an unauthorized access attempt.

Server agents work in network environments where it is either impractical or too costly to deploy network agents. As networks get faster, it becomes more difficult to monitor all inbound and outbound traffic. In addition, networks are becoming increasingly highly switched. A highly switched network means that more network agents are required to get the same level of coverage as a single network agent on a non-switched network.

Host-based agents are important for another reason. Local users can attack a system without being detected by the network agent. For example, somebody who has access to the console can try passwords all day without the network agent detecting it. A valid user running the hacker utilities "getadmin" or "sechole" to add him/herself to the administrator's group, or someone trying to open a file without permission or trojan a system file, can do so without being detected by the network agent. RealSecure OS and Server Sensors detect all these examples.

Deploying network and host-based agents achieve ultra-fast detection and response at the network level with rich, system-specific confirmation of events at the host level. The combination of network and host-based agents is the most effective way to provide threat coverage to a switched network.

14. How do RealSecure Network Sensor and Gigabit Network Sensor respond to attacks?

The administrator can respond to an attack in a variety of ways:

RealSecure Responses		
Response Type	Network Sensor	Server Sensor
Notification	Display an Alert on the Console	Display an Alert on the Console
	Send an e-Mail (SMTP)	Send an e-Mail (SMTP)
	Send an SNMP Trap	Send an SNMP v3 Trap
	View Session	
Log	Log results to the Database	Log results to the Database
	Log Results and Packet Payload to the database	Log Results and Packet Payload to the database
	Log intruding packets to disk	
	Log all packets captured to disk	
Active	Kill a Connect (TCP Reset)	Disable User Account
	Reconfigure Check Point FW	Block Network-based Attack
	Run a user-specified program	Run a user-specified program

The last option ("Execute a user-specified program") can be used to initiate any response that can be expressed in an executable binary (or batch file/shell script) form. Examples include initiating a pager call, playing a sound, or reconfiguring a network device that does not have an API for management.

15. How do RealSecure Network Sensor and Gigabit Network Sensor differ from a firewall? Don't they do the same things?

Firewalls and RealSecure Network Sensor and Gigabit Network Sensor use similar technologies to accomplish different things. Firewalls are controlling entities. They enforce general entry and exit rules for an entire network and aren't designed to look for attack patterns. Their main purpose is to keep the wrong kind of traffic off the network; their definition of "wrong kind of traffic" is usually based on IP address or protocol type.

RealSecure Network Sensor and Gigabit Network Sensor are not products that controls network access. RealSecure Network Sensor and Gigabit Network Sensor do not interfere with the network traffic stream at all. Instead, it allows the traffic to go by and quietly watches for signs of unauthorized activity. RealSecure Network Sensor and Gigabit Network Sensor's definition of "unauthorized activity" is a sophisticated and customizable database of attack signatures.

Think of your network as a high-rise apartment building, the firewall as the doorman, and each RealSecure Network Sensor as a guard dog on a specific floor and each RealSecure Server Sensor as bodyguard in each apartment. The doorman is generally pretty good about letting the right people in and keeping the wrong people out. However, a moderately clever criminal will be able to get past the doorman and into the building. The guard dog is better at knowing who's authorized to be on the floor and responding quickly to stop the intrusion. The bodyguard has a personal responsibility to defend the apartment in which he works. He knows the area well and monitors constantly for intruders.

16. How are RealSecure Network Sensor and Gigabit Network Sensor deployed across the enterprise network?

RealSecure Network Sensor and Gigabit Network Sensor use a distributed architecture. The agents perform the threat detection and response functions on critical network segments and servers. The Event Collector collects events from the agents for storage in the Enterprise Database and the RealSecure Console displays alarms, consolidates agent data, provides report generation capabilities, and acts as a centralized agent management point.

The relationship between agents and managers is many-to-many. Several RealSecure agents can report to a single Event Collector. Up to 5 Event Collectors can send data to a single Enterprise Database. This is all independent of the number of Consoles used for reporting, command and configuration. This flexibility is useful for environments where there are geographical or organizational management boundaries.

With regard to placement of RealSecure agents, the best rule is to place a RealSecure Network Sensor (10/100 or Gigabit) on each segment where there is critical data to protect, or a set of users that should be monitored. Note that a RealSecure Network Sensor will only see the traffic that is on the local network segment. Since routers, bridges, switches, and firewalls prevent traffic from being copied to inappropriate segments, several RealSecure agents will be needed for complete coverage of your critical network resources.

It is also a good practice to install a Server Sensor on all servers containing critical information. These include everything from internal file servers to external DMZ devices and communications servers.

17. What networks can RealSecure Network Sensor and Gigabit Network Sensor monitor?

RealSecure Network Sensor and Gigabit Network Sensor operate on the following types of networks.

- Ethernet networks (10 Mbps)
- Fast Ethernet networks (100Base-T @ half duplex 100 Mbps and full-duplex 200 Mbps)
- Gigabit Ethernet (1000 Mbps)
- FDDI (100 Mbps)
- Token Ring networks (4 Mbps to 16 Mbps) on NT only

Note: Refer to the Product README for the most current list of networks that RealSecure can monitor.

18. What do I have to do to my network to run RealSecure Network Sensor and Gigabit Network Sensor?

Nothing. You don't have to buy new routers or bridges; you don't have to install any software on your servers; you don't have to reconfigure any devices. RealSecure Network Sensor and Gigabit Network Sensor work with your existing network infrastructure. To install RealSecure Network Sensor and Gigabit Network Sensor, all you need to do is place a UNIX® or Windows 2000® system with an adapter card on the segment to be monitored and install the product.

19. Will RealSecure Network Sensor and Gigabit Network Sensor run on a switched network?

Yes. There are three ways to support a switched network with RealSecure Network Sensor and Gigabit Network Sensor:

- 1) **Strategic deployment of RealSecure Network Sensor and Gigabit Network Sensor.** In many cases, a careful look at your network reveals strategic locations where a switch can be placed that will provide excellent security coverage. If one switched port were connected to a router that connected to the Internet, then it would make sense to insert a small hub between the router and the switch and connect a RealSecure agent at that point. That would provide protection against attacks coming in from the Internet, regardless of what else was on the network.
- 2) **Use of RealSecure host-based agents.** Of course, RealSecure Server Sensor can fill the gaps that the Network Sensors cannot reach. Many switched environments involve server farms, with a high density of hosts connected to one or more switches directly. In this environment, a RealSecure Server Sensor on each host will protect each host from attack or misuse. Because the Server Sensors are small and completely configurable, each one can be configured to monitor the key files and functions on each server.

- 3) **Network Taps.** They allow for traffic on a critical network segment to be copied off to a RealSecure Network Sensor and Gigabit Network Sensor. For additional details refer to the Tech Notes on ISS' Web Site.

20. How do I get a copy of RealSecure Network Sensor and Gigabit Network Sensor?

Call ISS at 1-800-776-2362 (in North America) or at +1-404-236-2600 (outside North America) for instructions on how to download RealSecure Network Sensor and/or Gigabit Network Sensor from our website.

21. Whom do I contact for technical support?

Contact ISS Technical Support at support@iss.net or 1-888-447-4861 or +1-404-236-2700. Technical support operates 24 hours a day, 7 days a week.

22. Is there an archive of technical papers and utilities for RealSecure Network Sensor and Gigabit Network Sensor?

You can download free tech notes, unsupported utilities and other useful RealSecure Network Sensor and Gigabit Network Sensor information from the RealSecure Technical Center at http://www.iss.net/support/product_utilities/realsecure_tech_center/

23. Whom do I contact with product suggestions?

Send your enhancement request to enhancements@iss.net and it will be recorded.

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

Internet Security Systems, the Internet Security Systems logo, System Scanner, X-Press Update, and SiteProtector are trademarks, and RealSecure a registered trademark, of Internet Security Systems, Inc. Network ICE is a trademark, and BlackICE is a licensed trademark, of Network ICE Corporation, a wholly owned subsidiary of Internet Security Systems, Inc. Other marks and trade names mentioned are marks and names of their owners as indicated. All marks are the property of their respective owners and used in an editorial context without intent of infringement. Specifications and content are subject to change without notice.