



INTERNET  
SECURITY  
SYSTEMS™

**RealSecure™ 6.5**

## General Questions

### 1. What components comprise the RealSecure system?

The RealSecure system uses distributed client-server architecture and its components fall into two functional categories:

- **Sensors** - A class of modules that provide automated detection and response to threats. These modules are installed at strategic locations throughout the enterprise network and include:
  - A **network sensor** that monitors network traffic in real time for signs of malicious intent and responds automatically.
  - A **server sensor** that monitors both inbound and outbound network traffic directed at a single host as well as the operating-system log entries and key system files for indications of intrusion or unauthorized activity.
  - An **OS sensor** that monitors operating-system log entries and key system files for indications of unauthorized activity and responds automatically.
- **Workgroup Manager** - A module that provides for configuration of the sensors as well as detailed management and storage of the threat data generated by the sensors. All management of RealSecure sensors is accomplished across secure communications channels. Workgroup Manager modules include:
  - A **console** that allows centralized control of remote sensors and provides for centralized display of alerts and reporting.
  - **Event Collectors**, which collect data from many sensors in real-time and send it to the Enterprise Database and Console.
  - An **enterprise database** that stores the sensors' event data.
  - An **asset database** that contains information about assets including event collectors and sensors

### 2. What kinds of threats does RealSecure recognize?

RealSecure recognizes 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.

### 3. How do the RealSecure sensors work?

RealSecure sensors have a similar structure, although they vary considerably in what they detect and how they respond. RealSecure sensors are policy enforcement engines. The basic structure of a RealSecure sensor can be viewed as a generic-processing module. The inputs to the system include the user or administrator-specified configuration rules as well as the raw data source used to detect threats. For network sensors, this data source is raw network packets; for the OS sensor, this data source is operating system log entries. The outputs of the system include the threat responses that the system initiates. The sensor itself receives the data, compares it against the signature base, and, if it matches, initiates the

appropriate response. The signature base comes from ISS' X-Force™ industry leading research and development team. U-defined signatures are available in all sensors, supporting further customization.

The RealSecure Network Sensor is installed on a host having a network adapter card. RealSecure puts the adapter card in promiscuous mode so that it sees all the traffic on the local network segment. If a packet meets the filter criteria currently in force, it is parsed through decode and attack recognition logic. Each active session is maintained and tracked, so that attack patterns that span many packets can be detected. When an “interesting event” is detected, the appropriate actions can be taken.

The OS sensor runs as a process on a server. When a new log file entry is generated by the operating system, the operating system interrupts the OS sensor. The OS sensor reads the new log entry, compares it against the signatures currently in force, and, if a match is found, initiates the appropriate responses. Some signatures span multiple log entries, so the OS sensor also maintains the state of several user activity threads at one time. Unlike other products, the RealSecure OS Sensor does not simply rely on application logs, but it utilizes kernel-level audit data, so it cannot be fooled, spoofed, or bypassed.

The server sensor extends upon the capability of the OS sensor and allows for traffic destined to and from the system upon which it is installed to be monitored for signs of malicious activity. Server sensor also has the ability to block any malicious traffic it sees.

#### **4. Why do I need both network and host-based sensors?**

Because the data that each type of sensor generates is complementary, network-based intrusion detection is very good at providing early warning of attacks. By monitoring the traffic stream in real-time, a network sensor can see a threat and often neutralize it before it has a chance to do any damage. However, network sensors cannot tell you whether an attack was successful or not. The information they manage is very network-centric. Host-based sensors 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 sensors work in network environments where it is either impractical or too costly to deploy network sensors. 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 sensors are required to get the same level of coverage as a single network sensor on a non-switched network.

Host-based sensors are important for another reason. Local users can attack a system without being detected by the network sensor. For example, somebody who has access to the console can try passwords all day without a network sensor 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 sensor.

By deploying both network sensors and host-based sensors, ultra-fast detection and response at the network level with rich, system-specific confirmation of events at the host level are achieved. The combination of network sensors and host-based sensors is the most effective way to provide threat coverage to a switched network.

## 5. How does RealSecure respond to attacks?

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

<b>RealSecure Responses</b>		
<b>Response Type</b>	<b>Network Sensor</b>	<b>Server Sensor</b>
<b>Notification</b>	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	
<b>Log</b>	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
<b>Active</b>	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.

## 6. How many RealSecure sensors can a single RealSecure Workgroup Manager manage?

The console has been designed and tested to handle up to 50 sensors. Technically, further scalability may be possible; however, there is a human limit that is reached well before any technical limitation. The real number that works for your organization will depend on how RealSecure sensors and Event collector are configured and how an administrator elects to handle real-time incident.

RealSecure sensors can generate quite a bit of data. Some organizations choose to establish a steady flow of real-time information from the engines to the consoles so that the humans monitoring the events at the consoles can respond to events immediately. The number of sensors sending alerts to a single console is limited to the response capabilities of the humans at the consoles. While this number can vary widely, it has typically been in the range of 10 to 20 network sensors.

Other organizations, however, emphasize post-facto forensics over real time response. In these situations, RealSecure sensors are configured to generate a very small amount of real-time alerts and, instead, write event information into the Enterprise Database. In configurations like this, the number of sensors that can be effectively managed by a single console depends largely on how much real-time analysis is required. While this number can also vary widely, it is typically in the range of 20 to 30 network sensors.

Still other organizations with very large deployments choose to perform virtually all of their administrative tasks from outside the console, building management into their existing infrastructure utilizing the ISS Command Line Interface for sensor management.

## 7. How do the RealSecure sensors communicate with the RealSecure Console?

- Since RealSecure uses a distributed deployment scheme, the communications channel between sensors, Event collector(s) and console(s) is a critical part of the architecture. RealSecure uses a secure channel for passing messages between all components. This channel ensures the following:

- **Reliability** - Delivery is guaranteed with no additional action required by the user, subject to the availability of the communications path.
- **Privacy** - Data is securely encrypted to prevent unauthorized disclosure.
- **Integrity** - Data cannot be modified in, added to, or deleted from the data stream without the receiving entity detecting the corruption and aborting the session.
- **Authentication** - The party receiving the communications request is sure that the request is from a known peer and that there is no party in the middle proxying the data stream. Since communications channels are always initiated by RealSecure managers and are never initiated by RealSecure sensors, this ensures that the managers authenticate themselves to the sensors before issuing requests or retrieving data.

Data from the sensors to the consoles includes

- **Event messages** –These are passed up to the console as they occur.
- **Raw session data** – The keystroke or data content of a session is passed up to the console as it occurs if the response associated with an event is “View Session”.
- **Detailed event and log file information**-These are sent into the Enterprise Database by the event collector as it occurs.

## 8. How does RealSecure differ from a firewall? Don't they do the same things?

Firewalls and RealSecure 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 is not a product that controls network access. RealSecure does 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'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 OS/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.

## What's New in 6.5?

### 9. What are the current versions of the RealSecure family?

The current versions of the RealSecure family as of the 6.5 release are:

#### **Workgroup Manager**

- *Windows NT – 4.0 sp4-6a*
- *Windows 2000 – sp2*

#### **Command Line Interface (CLI)**

- *Windows NT – 4.0*
- *Windows 2000 – sp2*
- *Solaris SPARC – 2.6 & 7*
- *RedHat Linux – 7.1*

**Network Sensor**

- *Windows NT – 4.0 sp4-6a*
- *Windows 2000 – sp2*
- *Solaris – 2.6, 7, 8 (32 & 64 bit hardware)*
- *Nokia IPSO – 3.4 (On the following platforms IP330; IP440; IP530; IP650; IP740)*

**Server Sensor**

- *Windows NT – 4.0 sp4-6a*
- *Windows 2000 – sp2*
- *Solaris SPARC – 2.6, 7, 8*
- *Linux – 7.1*

**OS Sensor 5.0 (w/ XPU)**

- IBM AIX - 4.3.2, 4.3.3
- HP-UX - 11.x

For complete up to date system requirements go to  
[http://documents.iss.net/literature/RealSecure/rs\\_sysreqs.pdf](http://documents.iss.net/literature/RealSecure/rs_sysreqs.pdf)

Note: The OS sensor and server sensor can also detect intrusions on other Unix servers and network devices through a) its ability to receive Unix SYSLOG messages from remote servers and b) An extensive list of Unix-specific signatures.

**10. What new features will exist in RealSecure 6.5?**

The primary new functionality in RealSecure 6.5 will be inclusion of full remote upgrades. In addition, 6.5 will contain some bug fixes, and the RealSecure Server Sensor will contain some new features as described below.

**11. What is RealSecure Server Sensor 6.5?**

RealSecure Server Sensor 6.5 is part of the RealSecure™ Protection Systems, which performs attack recognition, incident response, and intrusion prevention in real time, with full customization of signatures and response capabilities, and is managed and integrated seamlessly with the RealSecure Workgroup Manager.

RealSecure Server Sensor 6.5 is the first ISS product to integrate BlackICE™ network monitoring technology, that offers many more network attack signatures, new user defined network signature capability, and proven stability of the operations and installation of the network monitoring driver. Version 6.5 is the most current version of RealSecure Server Sensor and includes updates to the Workgroup Manager and server sensor. The most current version of the network sensor is 6.5 and OS sensor is 5.0.

**12. What are the new features in the RealSecure 6.5 Server Sensor?**

The RealSecure Server Sensor has the following new features:

- **Ability to monitor SSL Encrypted Traffic** – In addition to IPSEC and SKIP encryption, RealSecure Server Sensor is capable of detecting attacks that have been encapsulated within an SSL session.
- **Full Remote Upgrades** – Via the full remote upgrade process, existing installs of RealSecure Server Sensor and Network Sensor can be easily upgrade to the most recent release of RealSecure.
- **SNMP v3** - The RealSecure Server Sensor is capable of sending an SNMP v3 response.
- **Additional Signatures** – Server sensor has additional Windows, Linux and Solaris Signatures. For complete details refer to the README file.

### 13. What is “web server protection”?

Web Server Protection enhances server sensor to be able to function more effectively in a web environment. In this release, server sensor will be able to monitor, recognize and respond to suspicious activity for IIS and Apache Servers. This includes SSL encrypted attacks. Web Protection works with the following web servers:

- **IIS** - 5.0
- **Apache** - 1.3

### 14. Can RealSecure Server Sensor monitor of SSL traffic for attacks?

Yes, in RealSecure 6.5 we will have the ability to monitor SSL traffic for signs of malicious traffic. The SSL Monitoring will work seamlessly with the web server application and respond to malicious SSL activity in the same manner that other log analysis or network traffic analysis is done through server sensor today.

## Full Remote Upgrade

### 15. What are full remote upgrades?

RealSecure 6.5 introduces the concept of a full remote upgrade. The full remote upgrade process allows for older versions of the network sensor or server sensor to be easily upgraded to the current version.

### 16. How do I upgrade to RealSecure 6.5?

Upgrading to the RealSecure 6.5 architecture involves the upgrading of the Workgroup Manager as well as the upgrading of the sensors. RealSecure 6.5 simplifies the process of upgrading the sensors via the full remote upgrade process.

The user has three options for the upgrading of the Workgroup Manager:

#### 1) Upgrade Existing Install

The user can install the RealSecure 6.5 Event Collector on the computer containing the existing RealSecure software. The benefit of this is that there is no need to push any additional \*.PubKey file to the sensors. However the downside of this alternative is that all systems are migrated at once.

#### Process Overview:

- Uninstall the previous WorkGroup Manger
- Install the 6.5 WorkGroup Manger
- Add sensors to the 6.5 Console
- Perform the Full Remote Upgrade on the sensors

#### 2) Upgrade one of the Workgroup Managers

If the RealSecure implementation consists of multiple Workgroup Manager, it is possible to upgrade only **one** of the site's Workgroup Managers. This option eases issues related to the distribution of the new \*.PubKey files, in addition to providing the basis for a methodical migration.

#### Process Overview:

- Choose one of the existing WorkGroup Mangers
- Uninstall the previous WorkGroup Manger
- Install the 6.5 WorkGroup Manger
- Add sensors to the 6.5 Console

- Perform the Full Remote Upgrade on the sensors

### 3) Install 6.5 on a New Computer

The other option is to install RealSecure 6.5 on a new computer and then to migrate computers to the 6.5 architecture in a methodical manner. RealSecure implementations that have only a single WorkGroup Manger computer may find this alternative attractive, because of the inherent rollback alternatives it provides.

#### Process Overview:

- Install the 6.5 WorkGroup Manger on new system
- Push the Public Key from new 6.5 Console and Event collector to the sensors.
- Migrate the sensors to the 6.5 Console
- Perform the Full Remote Upgrade on the sensors

### 17. What will happen if I upgrade an OS sensor to a server sensor?

The full remote upgrade mechanism performs a default install so that the server sensor's network monitoring function enabled once the full remote upgrade is completed. Similarly if a RealSecure Server Sensor has been installed with the network monitoring component disabled, when the full remote upgrade process is complete, the computer will have the server sensor's network monitoring function enabled.

### 18. What versions of the OS sensor/server sensor can be upgraded using full remote upgrades?

Server sensor 6.5 will be capable of upgrade the following platforms:

#### 5.5 Network Sensor

- *Solaris 5.5.1, 2.6*
- *Windows NT*

#### 5.5 OS Sensor

- *Solaris 5.5.1*

#### 6.0 Server Sensor

- *Windows NT/2000*
- *Solaris 2.6, 7 & 8*

#### 6.0.1 Server Sensor

- *Windows NT/2000*

### 19. I customized my previous install, what is going to happen when I perform a full remote upgrade?

The full remote upgrade process will maintain the current settings. This includes:

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

## Placement & Tuning

### 20. How is RealSecure deployed across the enterprise network?

RealSecure uses a distributed architecture. The sensors perform the threat detection and response functions on critical network segments and servers. The Event Collector collects events from the sensors for storage in the Enterprise Database and the RealSecure console displays alarms, consolidates engine data, provides report generation capabilities, and acts as a centralized engine management point.

The relationship between sensors and managers is many-to-many. Several RealSecure sensors 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 sensors, the best rule is to place a RealSecure Network Sensor 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 engines 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.

### 21. What networks can the network sensor monitor?

The RealSecure network sensor operates on the following types of networks.

- Ethernet networks (10 Mbps)
- Fast Ethernet networks (100Base-T only, 100 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.

### 22. What do I have to do to my network to run RealSecure?

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 works with your existing network infrastructure. To install network sensors, all you need to do is place a UNIX® or Windows NT® system with an adapter card on the segment to be monitored and install RealSecure. To install OS sensors, simply install the software on important servers that require protection.

### 23. Will RealSecure run on a switched network?

Yes. There are three ways to support a switched network with RealSecure:

- 1) **Strategic deployment of RealSecure Network Sensors.** 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 engine 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 sensors.** 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. For additional details refer to the Tech Notes on ISS' Web Site.

## Miscellaneous

### 24. How do I get a copy of RealSecure?

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.

### 25. Whom do I contact for technical support?

You can send e-mail to [support@iss.net](mailto:support@iss.net) or download our tech support FAQ from the ISS web site at <http://www.iss.net>. You can also search for solutions to known issues on the technical support knowledge base at [http://www.iss.net/customer\\_care/knowledgebase/](http://www.iss.net/customer_care/knowledgebase/). Finally, you can call ISS Technical Support directly at 1-888-447-4861 or +1-404-236-2700. Technical Support operates 24 hours a day, 7 days a week.

### 26. Is there an archive of technical papers and utilities for RealSecure?

You can download Tech Notes, unsupported utilities and other useful RealSecure information from the RealSecure Resource Center at [http://www.iss.net/customer\\_care/resource\\_center/realsecure\\_tech\\_center/](http://www.iss.net/customer_care/resource_center/realsecure_tech_center/)

### 27. Whom do I contact with product suggestions?

Send your enhancement request to [enhancements@iss.net](mailto: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 - 2001, Internet Security Systems, Inc. All rights reserved worldwide.*

Internet Security Systems, the Internet Security Systems logo, System Scanner, X-Press Update, and RealSecure are trademarks and service marks 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.