INTERNET
SECURITY
SYSTEMS™

RealSecure® Server Sensor
Frequently Asked Questions

6303 Barfield Road • Atlanta, GA 30328 Tel: 404.236.2600 • Fax: 404.236.2626

RealSecure®Server Sensor Frequently Asked Questions

As part of the Dynamic Threat Protection framework, 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 down-time.

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

RealSecure Server Sensor Version 7.0

1. What platforms are supported by RealSecure Server Sensor?

The platforms currently supported as of the 7.0 (Windows and HP-UX) release are:

Server Sensor 7.0

- *Windows NT – 4.0 sp 6a and higher*
- *Windows 2000 Professional, Server, Advanced Server SP 1, 2, 3*
- *HP-UX 11.0, 11i*
- *IBM AIX* – 4.3.3, 5L

Server Sensor 6.5

- *Solaris SPARC – 2.6, 7, 8*
- *Linux – Linux Red Hat 7.1, Kernel 2.4.2-2*

For complete up to date system requirements go to
http://documents.iss.net/literature/RealSecure/rsss_sysreq.pdf

Note: The 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.

2. What is RealSecure Server Sensor 7.0?

RealSecure Server Sensor 7.0 is a part of the RealSecure Protection System, 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 SiteProtector and Workgroup Manager.

RealSecure Server Sensor 7.0 is the latest ISS product to integrate the Protocol Analysis Module (PAM). PAM offers an increased number of attack signatures, improved accuracy and a quicker update process. Version 7.0 is the most current version of RealSecure Server Sensor and includes updates to the Workgroup Manager and Server Sensor.

3. What are the key benefits of RealSecure 7.0 Server Sensor?

- Protects against unknown and known attacks that circumvent traditional perimeter security measures
- Blocks malicious and abnormal behavior such as buffer overflows, malformed packets and root access before they cause damage
- "Virtual Patch" provides a cost effective way to manage the resource planning, patch and upgrade process while still protecting critical assets
- Plugs holes in your network without relying on resource intensive analysis
- Lower total cost of ownership using the SiteProtector™ Centralized Management & Security Fusion advanced correlation module.
- Eliminates false alarms and false positives by preventing the misidentification of attacks
- Provides real-time diagnosis of attacks driving security incident response time down

4. What new features exist in RealSecure®Server Sensor 7.0?

- **Advanced Intrusion Prevention -** Blends a combination of signature protection methods which protect host environments from known exploits with protocol anomaly detection/protocol analysis to actively prevent unknown exploits in real-time from causing damage. 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.
- **Active Blocking and Decision Support -** Actively blocks buffer overflow, malformed packets, root access and other types of attack methods based on behavior.
- **Console and Network-Based Intrusion Protection -** RealSecure Server Sensor provides you with the flexibility to prevent both console and network-based attacks through it's log monitoring capabilities preventing local users from launching attacks not being detected by network protection agents while also preventing brute force attacks and un-authorized access to critical system resources that would otherwise compromise data confidentiality, integrity and accessibility.
- **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.
- **Broad Platform Coverage –** Windows, , HP-UX, AIX, Linux
- **Audit Policy Management -** Centralized management of an OS audit policy ensures that all critical servers have a consistent and effective audit policy and allows for the management of true kernel-level auditing.
- **Centralized management** – Allows for the aggregation, correlation, analysis and management of data thereby preventing event propagation as well as providing a centralized means to deploy, manage and update complex server environments. Using SiteProtector™ Customers can control, monitor and analyze their security protection systems from one central site with a minimum of staff and operational costs. This integrated environment enables monitoring of intrusion activity, vulnerability assessment, event prioritization and correlation of ongoing security activity, as well as multi-site management capabilities. No other solution provides the real-time end-to-end visibility into and across the enterprise-wide security program while capitalizing on resource investments.

- Reduces training time and removes integration costs
- Scales from small organizations to large, global enterprises
- Deployment and configuration tools save time in the rollout of desktop agents
- Security management functions are executed on groups of devices
- Scheduling and automation remove the burden of repetitive tasks
- Guided security analysis makes sense of large amounts of security information for even non-security experts
- Reporting of security data allows effective information sharing

- **Event correlation and attack analysis** – Instantly correlates and analyzes the impact and attack patterns providing real-time diagnosis of "real-attacks" and is fully integrated with the ability to perform these actions in conjunction with network-based attacks as well.

- **Elimination of false positives and false negatives** – Prevents the misidentification of attacks eliminating false positives as well as provides for the identification of malicious behavior prior to those behaviors casing damage.

5. Does RealSecure 7.0 work with SiteProtector?

Yes, RealSecure 7.0 will work with SiteProtector. Furthermore, if you wish to add RealSecure 7.0 to the Deployment Manager, copy the "web" package (single EXE) to the Deployment Manager. Refer to the SiteProtector documentation for complete details.

6. Can data stored in a Workgroup Manager database be migrated to SiteProtector?

Yes. Migration information can be found on the SiteProtector documentation page.

http://www.iss.net/support/documentation/docs.php?product=16&family=8

Full Remote Upgrade

7. What are Full Remote Upgrades?

RealSecure Server Sensor 7.0 offers full remote upgrade capability. The full remote upgrade process allows for older versions of the Network Sensor or Server Sensor to be easily upgraded to the current version.

8. How do I upgrade to RealSecure 7.0?

Upgrading to the RealSecure 7.0 architecture involves the upgrading of the Workgroup Manager as well as the upgrading of the sensors. RealSecure 7.0 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 6.7 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 Workgroup Manger*
- *Add sensors to the 7.0 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 Managers*
- *Uninstall the previous Workgroup Managers*
- *Install the 7.0 Workgroup Manager*
- *Add sensors to the 7.0 console*
- *Perform the full remote upgrade on the sensors*

3) Install 7.0 on a New Computer

The other option is to install RealSecure 7.0 on a new computer and then to migrate computers over to the 7.0 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 7.0 Workgroup Manger on new system*
- *Push the Public Key from new 7.0 console and event collector to the sensors.*
- *Migrate the sensors to the 7.0 console*
- *Perform the full remote upgrade on the sensors*

9. How do full remote upgrades work?

Full remote upgrades will allow for RealSecure to be upgraded over the network. From the RealSecure Workgroup Manager an update is pushed over the network to the sensor. The operation is similar to the mechanism in which X-Press Updates are currently applied to a sensor.

10. What versions of the OS Sensor/Server Sensor can be upgraded using full remote upgrades?

Server Sensor 7.0 will be capable of upgrade the following platforms:

5.5 Server Sensor

- *Windows NT*
- *Solaris*

6.0 Server Sensor

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

6.0.1 Server Sensor

- *Windows NT /2000*

6.5 Server Sensor

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

11. If I upgrade a Server Sensor without the Network Monitoring components installed, what will happen?

If you chose to install a RealSecure 6.0, 6.0.1 or 6.5 Server Sensor without the network monitoring components, the full remote upgrade process will detect this and not install the network monitoring components of the Server Sensor 7.0.

12. Can I upgrade an OS Sensor to Server Sensor 7.0?

No, currently an OS Sensor cannot be upgraded to a Server Sensor. In the case of an OS Sensor, uninstall the current RealSecure OS Sensor and then perform a new install of the RealSecure Server Sensor 7.0.

13. 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:

- *Installation directories*
- *Sensor name(s)*
- *Existence of network monitoring components*

General RealSecure

14. 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 applications.
- **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.
- *RealSecure is shipped with the most comprehensive set of threat detection signatures in the industry.*

15. Why do I need both Network Sensors and host-based sensors?

Because the data that each type of sensor 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 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 intrusion detection systems complement their network counterparts very nicely. 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, more networks are becoming 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. The RealSecure OS and Server Sensors detect all of these examples.

By deploying both Network Sensors and host-based sensors, you can have the best of both worlds: ultra-fast detection and response at the network level with rich, system-specific confirmation of events at the host level. In addition, the combination of Network Sensors and host-based Sensors is the most effective way to provide threat coverage to a switched network.

16. How does RealSecure respond to attacks?

The actions taken upon detection of an attack or unauthorized activity are determined by the administrator and fall into three categories:

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
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.

RealSecure offers security administrators the widest variety of intrusion response options in the industry today.

17. 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 and 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 or 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.

18. Do I need firewalls if I have RealSecure?

Absolutely. RealSecure is an essential addition to, but not a replacement for, your firewall security. When firewalls are properly configured, they keep out most undesired traffic. However, in order to provide some level of access, firewalls have tunnels that can be exploited by would-be attackers. A good example is FTP. Many companies have an FTP server inside their network and associated tunnels through the firewall to allow access. A common attack is to attempt to gain root access to the FTP server. Once an attacker has access to a system inside the network, other systems become vulnerable. And although the firewall will not stop this type of attack, RealSecure will. By monitoring the traffic stream on the network behind the firewall, RealSecure can detect and terminate attempts to gain root access on the FTP server.

19. Do I need RealSecure if I have firewalls?

Yes. Threat management is a complementary technology to firewalls access control. While firewalls provide excellent packet-level protection for your network, they can never do it all:

- *Firewalls have tunnels that allow packets through. Packets that pass through these tunnels are typically not analyzed by the firewall, but are passed through unexamined. This means that you are relying on the security of your internal devices to protect your network for these specific data streams. For example protocols like SSH can enable virtually any traffic to be tunneled through any open port on a firewall. Such circumstances can be dangerous to the integrity of the network. RealSecure can detect the use of SSH and monitor traffic streams and their system targets for malicious activity.*
- *Firewalls are frequently misconfigured. Does your firewall have a filter that prevents ICMP requests? What about the new video streaming protocol that's just been announced to the Internet? Has a vice-president requested a specific hole in the firewall's filtering rules because he needs to access his personal files from home? These are examples of configuration mistakes or omissions that weaken a firewall's effectiveness. RealSecure works in conjunction with your firewall (whatever its configuration) by monitoring all the activity on your network and servers for attempts to breach your security. Although firewall misconfigurations should ideally be fixed as soon as possible, having RealSecure Sensors inside the network can bring attention to much of the undesirable traffic that's leaking through. Even if you choose not to terminate these undesired connections, the sheer number of alarms that RealSecure will generate will quickly indicate that your firewall is not doing its job.*
- *Firewalls can be compromised by an external attacker. The security marketplace is a dynamic, evolutionary battleground between attackers and defenders. Attack methods that were popular six months ago have been defeated by today's defense systems, but have been replaced by new methods. There are now techniques to scan through firewalls that didn't exist one year ago. New Trojan horse programs and denial of service attacks are being discovered weekly. RealSecure can help you stay ahead of the curve with technology that sees all the packets and notes the suspicious anomalies. Moreover, if your firewall is compromised, RealSecure offers another processor dedicated to the*

defense of your network – doubling the work an external attacker must do to penetrate your enterprise.

Placement & Tuning

20. How is RealSecure deployed across the enterprise network?

RealSecure uses a distributed architecture. The RealSecure sensors perform the threat detection and response functions on critical network segments and servers. The event collector(s) collect 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.

You should also 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 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 Server Sensors, all you need to do is install the software on important servers that you want to protect.

22. 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.*

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. Since 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****. Network taps allow for traffic on a critical network segment to be copied off to a RealSecure Network Sensor. For additional details refer to the TechNotes on ISS' Web Site*

Server Sensor

General Server Sensor Questions

23. Is a reboot required for Windows?

No, after Server Sensor 7.0 for Windows is installed, a reboot is not required.

24. Is a reboot required for Solaris?

A reboot is required for a Solaris Server Sensor installed with the Network Monitoring component.

Server Sensor for Solaris requires Sun's Basic Security Module (BSM) for some of its OS events. A reboot is required to enable BSM (to deactivate Volume Manager); however, if BSM has been enabled prior to the installation of Server Sensor, a reboot is only required if the Network Monitoring component is installed. If BSM is enabled at the time of the Server Sensor installation and the Network Component is also enabled, only a single reboot is required. In 7.0, BSM is not a prerequisite for the installation of Server Sensor for Solaris.

The reason BSM deactivates Volume Manager is that its functionality can be viewed as a security risk by some organizations. It is important to note that Solaris clusters rely on the volume manager functionality. If your organization relies on this functionality, it is possible to do one of two things:

- *Modify the BSM convert script to not disable volume management*
- *After running the BSM Convert script*
- *Reboot*
- *Install the RealSecure Server Sensor. After installing the RealSecure Server Sensor for Solaris follow the instructions given to re-enable Volume Management.*

25. Is a reboot required for Linux?

No, a reboot is not required after the install of the RealSecure Server Sensor for Linux.

26. How do the RealSecure host-based sensors ensure that the operating system is logging the right things?

OS and Server Sensors can automatically clear/set audit flags when you make changes to the policy so the user does not have to know what flags to set. They can also enforce auditing to be sure auditing flags are not accidentally changed by users or programs.

Obviously, the host-based sensors cannot detect a brute force login attack if the operating system is not recording failed login attempts. The RealSecure manager eliminates this problem by allowing you to control both the configuration of the sensors and the configuration of the operating system log files.

- *The detection policy is the configuration of the host-based sensors. It specifies which signatures are enabled and which are disabled; identifies how the system should respond to each signature match; and lists any user-defined signatures and actions.*
- *The audit policy is the audit configuration of the underlying operating system. It specifies which events are detected and logged by the operating system; identifies how log files are handled; and enumerates any key system resources that should be monitored by the operating system.*

- *The RealSecure manager allows you to specify both the detection policy of the agent as well as the audit policy of the operating system. You are prevented from trying to detect items in the detection policy that are not logged in the audit policy – the RealSecure manager won't let that happen.*

In addition, because you can push detection policies and audit policies down to remote agents, you can use the RealSecure manager to ensure that all of your critical servers have a consistent and effective audit policy.

Server Sensor Performance

27. What is the performance impact of Server Sensor on a system?

It is, in general, difficult to provide detailed numbers when discussing the performance overhead on a system resulting from the installation of the RealSecure Server Sensor. These numbers will depend greatly upon the installation and environmental factors. In general the default policies provided with the product will result in roughly a 3-8% utilization increase on the system when the Server Sensor is active. If the Server Sensor is idle, there is roughly a 1% overhead on the system.

Compatibility Questions

28. With what software is RealSecure Server Sensor 7.0 compatible?

For a complete and detailed list of software the RealSecure Server Sensor has been tested and supported, refer to the README.

29. Can I install a Server Sensor and Network Sensor on the same system?

Yes, a Server Sensor without the network monitoring components and a Network Sensor can coexist on a computer. This option is provided via a custom install of the Server Sensor.

30. 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 from our web or FTP site.

31. Whom do I contact for technical support?

You can send e-mail to support@iss.net. Or 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.

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

You can download free tech notes, unsupported utilities and other useful RealSecure information from the RealSecure resource center at: http://www.iss.net/support/

33. 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.

Version 3.2