

NFR Sentivist™ is an intelligent intrusion management system that unobtrusively monitors the network in real-time, raises alerts when attacks or misuse are detected, and actively responds if configured to do so. Highly accurate, high-performance Sentivist Sensors are available for gigabit and full duplex 100 Mbps Ethernet networks. Available as pre-configured appliances, Sentivist Sensors can be operational immediately. Multiple Sentivist Sensors can be managed from a central location, and their information consolidated for inquiry and reporting.



Figure 1: Sentivist Sensor

Features

Advanced, stateful traffic analysis: Sentivist Sensor performs advanced signature and stateful protocol analysis for many network-based protocols, enabling it to detect all types of attacks - including known attacks, stealth attacks, anomalous behavior, first strikes, DoS floods, brute force entries, and polymorphic attacks. Sentivist Sensor includes a new global ignore variable feature which allows the user to minimize false alerts from trusted network sources, it also examines IP packets and packet fragments, reassembles TCP streams, tracks sessions to identify disguised attacks and supports IPv6 (for protection against tunneling exploits).

Few false positives: In-depth examination using signatures, rules, and anomaly analysis results in highly accurate attack detection and, as a result, few false positives.

Alert management and suppression: Using point and click from Sentivist Enterprise Console, individual users can easily suppress unwanted alerts; e.g., ignore alerts from a particular IP address. Administrators can also reprioritize alerts, drill down into packet capture data, set up filters that block unwanted alerts, define correlated alerts, query events and run a selection of management reports.

Range of powerful Sentivist Sensors: Support for gigabit and 100 Mbps networks in full-duplex mode, ensuring maintenance of state.

Fail over mechanisms: Sentivist Sensors feature multiple monitoring interfaces, which allow them to monitor high-availability networks. Automatic redirection of data to an alternate Sentivist Server ensures continuity of alerting should the primary server fail. In the event of Sentivist Sensor hardware failure, another sensor can be brought up immediately simply by inserting the product CD and configuration floppy into the standby hardware, and powering it on.

Tamperproof system: The Sentivist Sensor software and operating system run from the product CD. The standard UNIX services, shells, and drivers have been removed to make the system resistant to attack. Transmissions between system components are encrypted.

No operating system to install or maintain: The Sentivist Sensor operating system and software are embedded, eliminating the need to install or maintain an operating system.

Fast, easy upgrade to new versions of software: Simply swap out the CD containing the Sentivist Sensor software and embedded operating system, and reboot the system.

Customizable: Administrators can easily disable or modify existing signatures and create new ones, using NFR Security's powerful N-Code™ signature language and the open signature library, to support customer-specific environments and proprietary protocols.

Extensive help information: Descriptions provide attack information, as well as references to Mitre's CVE database. Alerts can be annotated by the user; e.g., to define the action to be taken.

Immediate availability of new signatures: Users are notified as soon as new attack signatures are available for download from a secure NFR site. New signatures are instantly pushed to all Sentivist Sensors with a single button click.

Active response: At the user's discretion, alerts can trigger TCP resets and changes to firewall policies, and can be sent to IBM Tivoli and HP OpenView. Users can create their

own responses; e.g., invoking third-party tools such as traceroute and nslookup, and piping the data into a web server for viewing. NFR Sentivist is OPSEC compliant.

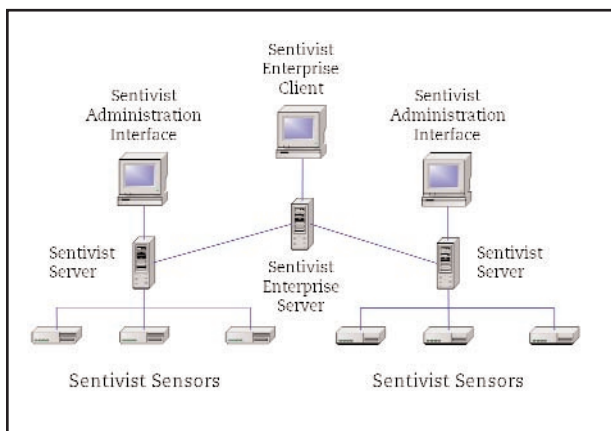
Central management: Allows users to manage multiple Sentivist Sensors from a central location, and consolidate data for querying and reporting. Different levels of administration privilege are provided.

An NFR Sentivist system comprises:

Sentivist Sensors for monitoring network traffic. Three models are available:

- Sentivist Sensor 320C - Includes three copper 10/100/1000 Ethernet interfaces, one of which is used for management; the others can be used for monitoring.
- Sentivist Sensor 320F - Includes two fiber Gigabit Ethernet interfaces and two copper 10/100/1000 Ethernet interfaces, one of which is used for management. The remaining interfaces are used for monitoring.
- Sentivist Sensor 310C - Includes two copper 10/100/1000 Ethernet interfaces, one for monitoring and one for management.

(nfr) sentivist architecture



All Sentivist Sensors are delivered as pre-configured appliances; there is also a software-only version available.

Sentivist Administration Interface for administration of Sentivist Sensors and querying and analysis of data.

Sentivist Server for management of multiple Sentivist Sensors. Sentivist Server provides central administration and storage of alert and event data for the sensors that report into it. Multiple servers can be distributed throughout the network as needed.

Sentivist Enterprise Console, an optional component, for receiving input streams from one or more Sentivist Servers. Sentivist Enterprise Console provides a unified picture of alert activity.

Recommended System Requirements

* The latest hardware specs for the Sentivist Sensor software-only version can be found on the NFR Security support website, <https://support.nfr.com>.

Configuration	Sentivist Sensor	Sentivist Administrative Interface	Sentivist Server	Sentivist Enterprise Console	
				Server	Client
Intel Platform RedHat Linux v7.3 or v8.0 1.4 GHz Pentium with dual CPU's 2 GB RAM Two SCSI drives in a RAID 0+1, 1, or 5 configuration (40 GB usable)			✓	✓	✓
SPARC Platform Solaris 8 or 9 400 MHz UltraSPARC with dual CPU's 4 GB RAM Two SCSI drives in a RAID 0+1, 1, or 5 configuration (40 GB usable)			✓	✓	✓
Intel Platform Windows 2000 or Windows XP 1+ GHZ Pentium 512+ MB ram 1+ GB usable disk space		✓			✓
Pre-configured Appliance*	✓				



nfr.com

Headquarters

NFR Security, Inc.
 5 Choke Cherry Road, Suite 200
 Rockville, MD 20850-4004
 1-800-234-4079

Europe Office

NFR Security, Inc.
 Stockerhof
 Dreikonigstrasse 31 A,
 8002 Zurich, Switzerland
 41 1 208 37 76