

**NFR Sentivist™** is an intelligent intrusion management system that provides highly accurate attack detection with low false positives. The system supports today's high-speed networks, includes extensive customization and active response capabilities, and provides central management of distributed environments.

## Highly Accurate Attack Detection

Cyber assaults can result in serious financial losses. The number and types of attack are increasing, they are becoming more damaging, and they are harder to detect. Identifying them requires an array of detection mechanisms including protocol anomaly analysis, signature analysis, maintaining state, and understanding context.

Sentivist has the most sophisticated attack detection engine available. It uses advanced signature analysis to detect known attacks; e.g., planting of back-entry devices, Internet worms, port scans, ping floods, and attempts to guess passwords. Anomaly detection identifies buffer overflows, polymorphic shell code attacks, denial of service attacks, and previously unknown attacks. For example, Sentivist was able to alert customers to Code Red before it became a known attack.

Sentivist's detection capabilities result in significantly higher levels of accuracy and far fewer false positives. Traffic state is maintained, data is examined in context, and attacks are assessed for impact. Individual packet fragments and the reassembled packets are examined, and sessions are tracked to thwart IDS evasion techniques, such as fragroute. This minimizes the opportunity for disguised attacks to pass undetected. In many cases, this also provides the ability to inform the end user whether an attack was successful.

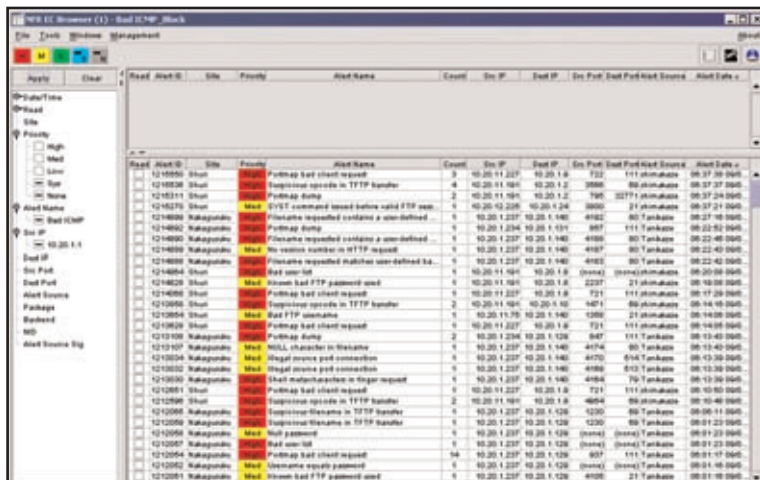
## Range of High Performance Sensors

Sentivist includes a comprehensive family of Sentivist Sensors to address all network bandwidth monitoring requirements. Sentivist 320C and Sentivist 320F provide support for monitoring gigabit Ethernet networks. Additionally, the Sentivist 320C can be used to monitor full-duplex 100 Mbps Ethernet networks. Sentivist 310C provides support for monitoring 10/100 Mbps Ethernet networks. Sentivist 320C and Sentivist 320F can be configured to monitor two distinct networks or both directions of a full-duplex network, enabling Sentivist Sensor to maintain complete state information. The same is true when monitoring dynamically routed networks. Sentivist 310C monitors a single network.

Sentivist Sensors are available as pre-configured appliances for fast, easy deployment. Sentivist Sensor is also available as a software-only version for those customers who wish to source their own hardware that match NFR certified configurations. Sentivist Sensors can be placed anywhere on the network, monitoring traffic coming to or through the firewall, crossing from one subnet to another, or accessing particular IT resources such as e-mail servers, web servers, database servers, etc.

## Flexible Alert Notification and Response

On detecting suspicious activity, Sentivist Sensor records event information, raises an alert that can be displayed on Sentivist Enterprise Console, Sentivist Administration Interface, in an e-mail or on a pager, and, at the user's discretion, can initiate automated responses.



**Figure 1:** Sentivist Enterprise Console Main Alert Screen

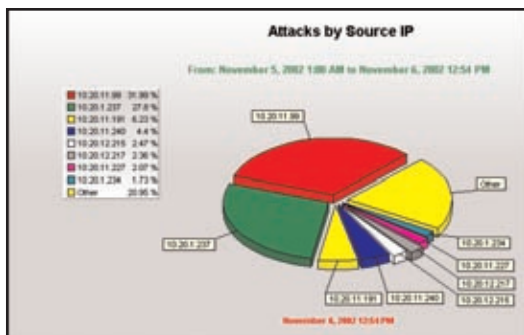
Activity details can include type of attack, source and destination addresses with host names, raw packet capture data, source and destination operating systems, help based on best practices, and a user-definable annotation field; e.g., to describe the user action to be taken. Additionally, Sentivist Enterprise Console includes alert consolidation, alert correlation across multiple Sentivist Servers, real-time graphing and alert filtering directly from the main alert screen.

Automatically initiated responses include notifying IBM Tivoli and HP OpenView enterprise management systems, generating SNMP traps, resetting the TCP session, and initiating firewall actions.

End users can also create alert responses and automatically invoke third-party tools; e.g., to look up the details of an attacker.



**Figure 2:** Alert Tuning Screen



**Figure 3:** Report of Attacks by Source IP



**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



## Easy Tuning and Customization

The capability to tune and customize network intrusion detection systems is necessary for optimal operation. Sentivist provides a range of facilities. From Sentivist Enterprise Console, users can eliminate alerts, define what information is displayed, and how it is presented. Alerts can be consolidated by type, sorted by column, color coded by priority, and throttled to display only if the alert has occurred a defined number of times within a specified period. Unwanted alerts can be easily excluded; e.g., when there is a legitimate IIS attack identified but no such servers exist within the enterprise.

Users may also want to modify existing signatures or create new ones to accommodate organization-specific protocols and internal applications. NFR provides the N-Code<sup>TM</sup> signature language and publishes signature libraries in open source.

## Options for High Availability Networks

Sentivist 320C and Sentivist 320F have the capability to monitor multiple NICs, enabling continuous monitoring of high-availability or fail over networks.

Sentivist Sensors can be configured to automatically redirect their data to an alternative Sentivist Server in the event of failure, ensuring continuity of alerting and event recording. In the event of a Sentivist Sensor hardware failure, a backup Sentivist Sensor can be rapidly deployed simply by inserting the product distribution CD and the configuration floppy into standby hardware and powering it on.

Sentivist Sensor is delivered as a tamperproof system that when deployed is invisible to hackers. The operating system, application code, and signatures are fully protected from deliberate or accidental manipulation.

## Flexible Administration and Operation

Multiple Sentivist Sensors can be managed from a Sentivist Server, and multiple Sentivist Servers can be deployed within an environment. This architecture scales to support from the smallest to the largest enterprises. Alert data is stored in both the Sentivist Enterprise Server and Sentivist Server databases, where it is available to local administrators for querying and reporting. Queries can be performed against any type and level of data from single or multiple Sentivist Sensors.

The Enterprise Console includes over 40 new management reports such as: Attacks by Type, Attacks by Source IP, Attacks by Destination IP, Attacks by Sentivist Sensor, Attacks by Date, etc.

## Fast, Easy Deployment and Maintenance

Sentivist Sensor software, which includes an embedded operating system, runs from the product distribution CD. This eliminates the task of installing software or reconfiguring the operating system, thus reducing the reliance on skilled personnel. Sentivist Sensors can be deployed at remote locations without the administrator being present. Unskilled personnel at the remote location simply insert the product distribution CD and configuration floppy into the Sentivist Sensor hardware and the administrator completes the installation. Sentivist Sensors can be up and running within minutes.

## Rapid Response to New Attacks

NFR's Rapid Response Team (RRT) constantly monitors for new attacks and develops signatures in response, making them immediately downloadable from a secure site. The RRT is noted for its security expertise, which manifests itself in the quality of the signatures and the best practices built into the alert help files.

## World-Class Customer Service

NFR prides itself on its world-class Customer Service organization, which offers 24 x 7 support and a range of professional services to its customers, ensuring successful initial deployment and ongoing operations.