



SNARE System for Security Control and Audit Compliance

SNARE ('System iNtrusion Analysis and Reporting Environment)

is an Enterprise Audit Event Log Analysis solution. The SNARE System is comprised of two toolsets: a central service that provides audit event collection, event analysis and reporting and archive capabilities (SNARE Server); coupled with agents that are designed for a wide range of operating systems and applications. These SNARE Agents have been released primarily as Open Source, and are used worldwide, plus there are commercialized agents.

Government and regulatory bodies are requiring organization's to protect the confidentiality, integrity and availability of sensitive information, which has increased the work load placed on the IT security departments.

The IT security departments are now required to review log files from their heterogeneous networks and provide useful and time-sensitive information on the activity within their organizations. This not only means to monitor but also to review, correlate and report on the activity.

This can be done easily and cost effectively by automating the processes, and having only the pertinent and germane information presented.

THE SNARE SYSTEM TOOL SET

The SNARE Server acts as the central collection system and comes equipped with an array of security objectives that allow you to meet common security audit goals. The SNARE Server is aimed at business with extensive audit requirements. The key value of the SNARE Server is the ability to define complex security objectives in an easy-to-program language, and to reports it findings in a simple manner but concise manner, providing the necessary information to the Security Professional. This means that the SNARE Server can be tailored to suit your specific requirements.

SNARE was originally developed to meet the auditing needs of organization with significant security requirements, most notable of these being agencies of the Intelligence communication and the Department of Defense.

One of the key advantages of the SNARE System is the capability to facilitate the development of 'objectives' that meet organizational risk requirements, and Government and International Security recommendations.

SNARE System Benefits

- Multiple platform support with SNARE Agents, application support and firewall support
- Event log analysis and correlation from multiple platforms
- Detection of sensitive activity (including use of special account privileges, access to sensitive files and directories)
- Easy to use reporting and archive capabilities
- Network congestion reduced through the use of the SNARE Agents
- Single point access to remote SNARE Agents
- Nessus and NMAP included with the SNARE Server and the ability to collect and analyze from SNORT based log files.
- Forensics/Redundancy License (with selected models) included, and the SNARE reflector technology, which provides the ability to send the data from one SNARE Server to another, in realtime.
- Available as both a software only solution or appliance.

SNARE Server Models:

The SNARE Server is available in as both an applianced solution or software only,

All SNARE Servers include support for the open source agents.

The benefits of an applianced solution is the superior performance, supportability and implementation. This also provides for some of the regulatory acts where physical security and access is mandatory.

The operating system, which is preloaded has one account defined, specifically for support access that might be required. All SNARE user and administration is accessed via browser.

With our two base models, an organization can expand their system as the need arises. The ability to collect from additional devices (either through the use of SNARE Agents or system log files) is an easy upgrade path.

All models and additional collection devices are subject to a mandatory maintenance package, which includes software upgrades/updates and basic email support. Optional support and training packages available.

SNARE-50 SNARE Server 50 permits the collection of up to 50 devices * (SNARE Agents and system log files).

SNARE-200 SNARE Server 200 permits the collection of up to 200 devices * (SNARE Agents and system log files). This model also includes the Enterprise Agent and a SNARE Server Back up license.

SNARE-600 SNARE Server 600 permits collection of up to 600 devices * (SNARE Agents and system log files). This model includes Enterprise Agents and a SNARE Server backup license

* *Collection from additional devices over the base limit can be purchased.*

Software only pricing is also available.

Highlights

Report Templates for Compliance Regulation

SNARE Server has a large library of pre-defined objectives, such as login activity and access to sensitive files. It also provides the flexibility for organizations to create their own audit reports.

Ability to Collect from Virtually Any Source

SNARE Server can collect from the SNARE Agents, both Open Source and Commercial Agents, plus any system log enabled device. When using the agents the information is forwarded in real time which ensures that the audit information is accurate and has not been tampered with.

Ease of Use:

The SNARE Server is easy to implement and use. When purchased as an appliance, the device can be up and running within the hour, collecting log files. The

software is provided as a single CD install. Access to the SNARE Server is via a web browser over either http or https.

Positive Return on Investment from Non-Automated Audit and Log Correlation:

Most acts require a daily review of all Audit logs. If you have approximately 30 systems; it is estimated that it takes 1 hour to review per system per day; a System Administrator earns approximately \$35.00 per hour; the estimated labour cost for the year would equal \$382, 200. The cost of the SNARE Server would equal less than one months salary.

The logs are also archived and available in standard text file format to allow for any possible investigation or litigation.

The SNARE Systems allows for consolidation of all your audit requirements on your network.