



SYSTEM INTRUSION ANALYSIS & REPORTING ENVIRONMENT

SNARE System for Security Control & 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 & reporting, and archive capabilities (SNARE Server); coupled with the agents that are designed for a wide range of operating systems and applications. Most of 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 organizations 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 businesses 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, to report the findings in a simple but concise manner, and provide 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 organizations with significant security requirements, most notable of these being agencies of Intelligence Communications 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, as well as 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 and 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 included (with selected models), and the SNARE reflector technology, which provides the ability to send the data from one SNARE Server to another in real-time.
- Available as both an appliance solution or software only.

Phone: 416-769-3000
Toll-Free: 866-431-8972
Fax: 416-769-4477



E-mail: snaresales@symtrex.com
www.snare-server.com
www.symtrex.com



SYSTEM INTRUSION ANALYSIS & REPORTING ENVIRONMENT

SNARE Server Models and Specifications

SNARE Server Models:

The SNARE Server is available in three base models to accommodate small to enterprise level organizations.

The benefits of an appliance solution are 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.

All models utilize the identical software and are defined based on the number of SNARE Agents that can be collected as well as the use of the commercial agents.

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 backup 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 is also available.

Hardware Specifications

SNARE Server hardware requirements are significantly dependent on the volume of audit, and the type and number of audit objectives defined. The following should be considered minimal requirements for a functional Snare Server system:

Minimal Snare Server Requirement:

- An x86 compatible CPU (eg: Pentium 4, AMD, AMD64) running at a processing capacity equivalent to, or better than a Pentium 4 - 3Ghz
- 300GB hard disk or greater. Disk may be IDE, SCSI or SATA. The disk should either be one physical disk, or should appear as a single disk to the operating system, via a hardware RAID controller. Software RAID is not supported
- 4 Gb RAM
- A 100 megabit, or (preferably) a 1000 megabit (1 Gigabit) network card
- In general, the Snare Server operates on a hardened version of the 'Ubuntu Feisty' distribution of Linux

Snare Server Hardware Models (50, 200 & 600) Include:

- IPC Case 2 U Compact ATX 3 Slot
- Seasonic 2U 460ATX Power Supply
- Intel P4 MB uATX, DG965WH V/L/A
- Intel Core 2 Duo E6320 (1.86 Ghz, 4MB)
- Sony DVD Recorder
- WD 250gb SATA 7.2k rpm, Hard Drives (Quantity 3)
- 1 GB DDR2-667 Memory (Quantity 4)
- Triple PCI Relocation 2U Riser Card Mtg
- 3Ware 9500S - 4LP

Any hardware supported out-of-the-box by Ubuntu Feisty, will also work on the Snare Server. In particular:

- a) Some brands of Serial-Attached-SCSI may be supported.
- b) Most modern CD/DVD ATAPI writers will operate correctly.
- c) A majority of SATA/RAID cards will operate correctly.