



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.

Key Features:

- €# Straightforward, single CD installation, or preloaded on optimized hardware
- €# Multiple platform and application support with SNARE Agents
- €# Ability to collect any arbitrary log data, either via UDP or TCP protocols
- €# Web interface allows for easy setup of queries for reporting
- €# Archiving and storage of data setup is effortless
- €# Collected events to be sent, in real time, to a standby/backup Snare Server or Master/Slave Topology
- €# Ability to continuously collect large numbers of events, with burst collection allowing
- €# Automatic collection of events to compressed analysis
- €# Ability to drill down from top level summary reports to raw log details
- €# Ability to create "cloned" objectives that allow fine tuning reports based on inclusion or exclusion of certain parameters



Contact Us:
Symtrex Inc.
 264 Jane Street
 Toronto, Ontario
 Canada M6S 3Z2
 416.769.3000 ph.
 866.431.8972 Toll Free
 416.769.4477 fax
 snaresales@symtrex.com
 www.symtrex.com
 www.snare-server.com

Who's Watching Your Network?

Snare Server Licensing & Hardware Specifications

SNARE Server Models:

The SNARE Server is provided as a base model that will allow you to collect up to 250 devices/ nodes (remote syslog or the open sourced agents). Depending on regulatory requirements and security best practices Enterprise Agents can be purchased to provide more reliability and integrity of the data being collected. Agents available are SNARE For Windows, SNARE for Linux, SNARE for Solaris, SNARE for Irix, SNARE for AIX, Tru 64, Epilog Agent for Windows, Epilog Agent for Unix and the Microsoft SQL Agent.

The product can be purchased as either an ISO appliance or a hardware appliance.

All products are subject to a maintenance/support subscription which provides for updates, upgrades and technical support.

<UfX kUfY*GdYW]ÙWUh]cbg*

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.

Contact Us:
Symtrex Inc.
264 Jane Street
Toronto, Ontario
Canada M6S 3Z2
416.769.3000 ph.
866.431.8972 Toll Free
416.769.4477 fax
snaresales@symtrex.com
www.symtrex.com
www.snare-server.com



Who's Watching Your Network?