SNARE

System iNtrusion Analysis & Reporting Environment

SNARE System for Security Control & Audit Compliance

SNARE (System iNtrusion Analysis and Reporting Environment) is an Enterprise level Security Event Management solution. The SNARE System is comprised of two toolsets: a central service that provides audit event collection, event analysis & reporting, and archiving (SNARE Server); coupled with the SNARE agents designed for a wide range of operating systems and applications. The Agents, which have been available as an open source product, are widely used globally and are defined as the defacto standard for log collecting for the Windows Operating System, are now offered with additional functionality (refered to as Enterprise 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 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.

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.

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 ability to facilitate the development of 'objectives' that meet organizational risk requirements, as well as Government and International Security recommendations, and in essence SNARE can be tailored to meet your specific requirements.

Key Features and Benefits

- *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*
- *Snare reflector technology that allows for all 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 text format, suitable for offline forensics analysis*
- *Ability to drill down from top level summary reports to raw log details*
- *Ability to create "cloned" objectives that allow very specific reporting against any collection profile*
- *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

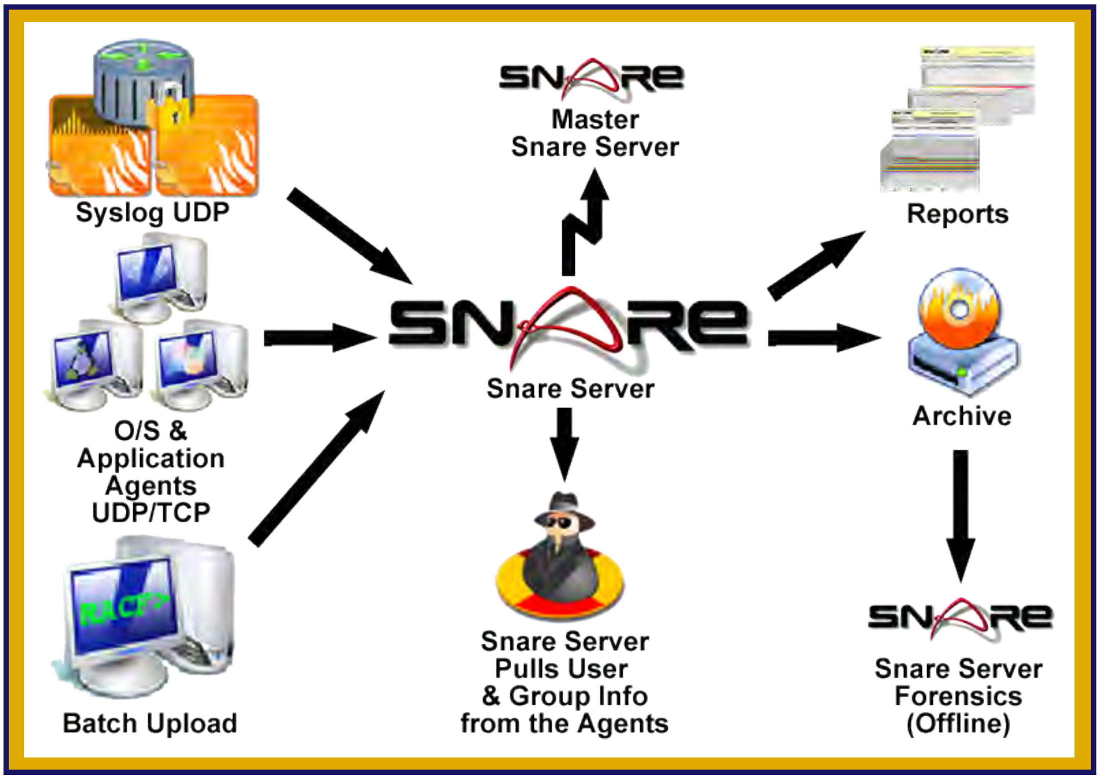
symtrex inc.
Network Security Specialists

Who's Watching Your Network?

How the System Works

To reiterate, the SNARE System is comprised of two toolsets. The SNARE Agents provide a filtering capability and send the event logs in real time to the Snare Server. The SNARE Agents, which are currently available for Windows, Linux, Solaris, AIX, Irix, IIS, ISA, Apache, Squid, and the Epilog Agents for text based log files, are the tools that allow the organization to send to the collector only the security relevant events, thereby reducing network congestion. In addition, the SNARE Server can collect from any device that sends out remote syslog.

The SNARE Server receives the information from both the SNARE Agents and standard System Log files, normalizes the data and deposits the information into a collection database (refered to as a datastore) depending on the type of event log, enabling a user to perform queries against individual log types or across various log types for reports through the Web Interface. The reports can be emailed to the security relevant personnel on an hourly, daily, weekly, bi-monthly, monthly basis depending on your requirements, in addition, through certain objectives, an email can be sent immediately for those security critical events, where time is of the essence.



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

symtrex inc.
Network Security Specialists

Who's Watching Your Network?

SNARE Enterprise Agents

SNARE Enterprise Agents build upon the open source SNARE Agents by providing extensions specifically designed to greatly enhance the 3 pillars of information security: ***Confidentiality***, ***Integrity*** and ***Availability*** of critical log data.

SNARE Enterprise Agents, which are included with the SNARE Server or can be purchased as a standalone product, provides users:

➔ Access to the official support mechanism for Snare agents. Note that official Snare agent support is currently not offered through ***any*** other channels.

➔ The ability to quickly and easily gather the necessary information to comply with ***NISPOM, PCI, SOX*** or other regulatory requirements.

➔ Access to all future Snare Enterprise Agent versions and upgrades (included as part of the annual maintenance fee).

➔ Additional agent features summarized in the table below

Feature	**Open Source**	**Enterprise**
Gather operating system specific events	✓	✓
Easy to use installer	✓	✓
Silent install option	✓	✓
Upgrade option to preserve existing configuration settings	✓	✓
Provide access to local and network users and groups	✓	✓
Remote control interface	✓	✓
UDP and Syslog transmission options	✓	✓
Objective-based event filtering	✓	✓
Debug mode	✓	✓
Encryption		✓
Event log caching		✓
Guaranteed log message delivery		✓
Log message simulcasting		✓
Advanced remote control		✓
Dynamic DNS support		✓
Centralized configuration management		✓

symtrex inc.
Network Security Specialists

Snare Server Categories

System Security	The System Security Monitoring category contains objectives for monitoring accounts, login activity, specific processes, security activity and specific files or resources. ***The key sub-categories are:*** • Account Administration • Login Activity • Process Monitoring • Security Activity • Sensitive Files and Resources
Application Auditing	The Application Auditing category contains objectives for creating dynamic queries and reporting on information from application logs. ***The key sub-categories are:*** • Apache/IIS Web Server Logs • Dynamic Clonable Queries • E-Mail Server Logs • General Windows Event Logs • IBM SOCKS Server Event Logs • Microsoft RAS Server Logs • NetIQ Directory and Resource Administrator Logs • Squid/ISA Proxy Server Logs • Syslog Reports • Universal Log Searcher • Dynamic Data Query
Network Events	The Network Event Analysis category contains objectives for monitoring activity detected in firewall and router logs. ***The key sub-categories are:*** • CISCO Router Logs • Cyberguard Firewall Logs • Firewall1 Firewall Logs • Gauntlet Firewall Logs • Host Vulnerability Scanner • IPTables Firewall Logs • ISA Firewall Logs • Netgear Firewall Logs • Netgear Router Logs • Network Intrusion Detection Scanner • Network Mapper • PIX Firewall Logs

For detailed information on each of the categories please refer to the SNARE Users Guide, located under resources at www.snare-server.com. Additional documentation is also available.

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

symtrex inc.
Network Security Specialists

Who's Watching Your Network?

Configuration Checking	The Configuration Checking category contains objectives for checking details of users and groups, your system security configuration, and system access. ***The key sub-categories are:*** • System Access Controls - ACF2 Resource Permissions - Lotus Notes Checks • System Security Configuration - PIX/Router Configuration Checker - Solaris JASS Security Report - Windows Registry Change Watcher • User and Group Related Checks - AIX Checks - Cognos Checks - Irix Checks - Linux Checks - Notes Checks - Solaris Checks - Windows Checks
ALARM Status and Statistics	The Status and Statistics category contains objectives for monitoring the status and performance of the SNARE Server. This includes information on user access to the SNARE Server, current scripts and processes that are running or queued to run, summaries of the data in the database and general health check information. ***The key sub-categories are:*** • Access Logs • General Statistics • Monitor Incoming Data • SNARE Health Checker • SNARE Process Management • System Status • Total Events • Total Events per 15 minutes, over the last 35 days
Snare Agents	The SNARE Agent Information category contains objectives for checking the status of and communicating with the SNARE Agents that are reporting to the SNARE Server. ***The key sub-categories are:*** • Data Retrieval • Check SNARE Agent Version • Check and Set Agent Configuration • Select Individual Client Systems
Snare Utilities	The SNARE Server Utilities category contains objectives for maintenance, upgrades, and configuration of the SNARE Server. ***The key sub-categories are:*** • Archival and Backup • Data Restoration • SNARE Server Administrative Tools • My SNARE Server Account • SNARE General Configuration Items PCI / SOX / NISPOM - Depending on the regulatory act chosen, a detailed list of objectives are created.

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

symtrex inc.
Network Security Specialists

Who’s Watching Your Network?

Snare Server Models & 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.

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' (Version 4.x) distribution of Linux or Ubuntu karmic koala (Version 5.x)

Snare Server Hardware Models:

- IPC Case 2 U Compact ATX 3 Slot
- Seasonic 2U 460ATX Power Supply
- Intel MB uATX, DH55TC V/L/A
- Intel Pentium G6950 (2.8 Ghz, 3MB) Dual Core
- Sony DVD Recorder
- WD 500gb SATA 7.2k rpm, Hard Drives (Quantity 2) Mirror Raid 1
- 2 GB DDR3 Memory (Quantity 2)
- Triple PCI Relocation 2U Riser Card Mtg
- 3Ware 9650SE - 2LP

Any hardware supported out-of-the-box by Ubuntu, 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

symtrex inc.
Network Security Specialists

Who's Watching Your Network?