Snare System Version 6—Enterprise Event Log Management

The Snare System is a comprehensive set of event monitoring and analysis tools designed to address complex and mission critical auditing requirements. It is comprised of two toolsets: the Snare Server and the Enterprise Snare Agents. Together they provide a complete security solution for auditing of your IT Systems and its confidential data.

The ***Snare Server*** collects events and logs from your operating system, applications, and any other device that can forward system log files. Snare provides the ability for powerful drill down analysis in a format that is easy to use and navigate.

The Server includes over 100 different reports spread amongst a wide range of categories, including administrative activities, sensitive file monitoring, user login activity, web proxy access, firewall and router monitoring, user and group checks and many more.

The ***Enterprise Snare Agents*** provide the tool to capture logs from the host devices in real-time. These small programs are installed and configured to capture on the security relevant events and send to the Snare Server (or third party collector). The Enterprise Agents provide for the ability to send the information via TCP with caching, multicasting, as well as capture custom event logs.

The Snare Server also provides a mechanism to administer the agents through the console. You can check and configure the agents as per compliance or security requirements, as well as refine/change them from the console.

The Snare System Overview:

- Ability to collect any log data either via UDP or TCP protocols
- Ability to continuously collect large number of events with burst collection allowing for over 50,000 events per second.
- Ability to drill from summary information to raw log data
- Ability to filter log information at the source to ensure that only the security relevant events as defined by the organization are collected, reducing network overhead.
- Ability to collect custom event logs
- Robust Collection, intelligent caching, and superior storage
- Ability to have multiple dashboards pending your regulatory requirement
- Importing objectives that meet your requirement

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

symtrex inc.
Network Security Specialists

Who's Watching your Network?

Features at a Glance:

Flexible Pricing

The Snare System provides for flexible pricing, starting with a base model that can be increased simply by adding additional nodes or Enterprise Snare Agents, in addition choose perpetual, term or subscription based.

Easy Setup

Installation is simple, just point the agents and remote sys log to the Snare Server to start collecting events.

Monitor Active Directory

When using the agents, you can pull the information from your active directory on users and groups and ensure that company policies are being adhered to, such as password age.

Reflector Technology

Snare reflector technology allows for all collected events to be sent, in real time to a standby/backup or central Snare Server (Master/Slave Topology)

Access Controls

Access controls provide you with the ability to selectively provide read-only or change access to specific reports on the Snare Server, or you can send out them out via email, tweets, Google talk or PDF/HTML reports.

Multiple Dashboard

Create dashboards easily for your compliance requirements, or IT teams.

Reliable Event Log Collection/ USB Auditing

Using the Enterprise Snare Agents provide more reliable event log collection due to its ability to send via TCP with caching, custom event logs, and the ability to capture more than just the core windows event logs. In addition monitor USB activity.

Hardware Requirements

- An x86 compatible CPU (eg: Pentium Core I5, AMD64) running at a processing capacity equivalent to, or better than, a Pentium 4, running at 2Ghz. Dual-core CPU's are recommended.
- 200Gb hard disk or larger. This should be recognized by an operating system as one single disk, and may be either IDE, SATA or SCSI. Hardware RAID may be used, as long as the RAID controller is capable of either emulating normal IDE/ SATA/SCSI protocols, or has a supported driver available in Snare.
- An IDE, SATA or USB DVD writer supported by Snare. 2 Gb RAM, or more.
- A 100 megabit, or (preferably) a 1000 megabit (1 Gigabit) network card.
- Keyboard, mouse and monitor as appropriate.

And can be installed on a virtual server.

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

Contact us for a demonstration of the Server or to arrange for an evaluation of the product in your own environment.

symtrex inc.
Network Security Specialists

Who's Watching your Network?