



SYSTEM INTRUSION ANALYSIS & REPORTING ENVIRONMENT

SNARE Enterprise Agents

Snare Enterprise Agents build upon our hugely popular 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.

Licensing of Snare Enterprise Agents 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 Agents | Enterprise Agent |
|--|--------------------|------------------|
| 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 | | ✓ |

Encryption

One of the most frequently requested Snare Agent enhancements has been the ability to encrypt messages between the originating host and the Snare Server. Now using the NIST recommended Triple DES algorithm, Snare Enterprise Agents are able to protect the confidentiality of log messages in transit. Once the messages have been accepted by the Snare Server, they are decrypted and processed as normal messages. By utilizing the *Centralized Configuration Management* option (described below), agent message encryption can be quickly rolled out across the network enhancing log integrity and confidentiality throughout the enterprise

Event Log Caching

Intermittent network outages pose a significant challenge to the integrity of centralized log management. One of the most feared IT Auditor questions has long been; "What happens to the log events if there is a network disruption?" This is particularly true of systems leveraging syslog for log aggregation. *Event Log Caching* significantly enhances the integrity of the overall log management system by storing undelivered messages in memory on the originating host in the event of a transmission failure.

SNARE Enterprise Agents

Common sources of transmission failures include:

- Network outages
- Destination server being offline
- Network device failure or misconfiguration (e.g. router)
- Network stack malfunction on the host machine

Once the Enterprise Agent is notified of any problems delivering messages to the destination server, the event log cache is used to preserve subsequent messages as long as the destination server is unavailable. The size of this cache is configurable and if the agent needs to be stopped or restarted for any reason, any remaining events will be written to disk. Once a new connection can be established with the server, the cached events are gradually forwarded to their destination.

Guaranteed Log Message Delivery

System administrators and security professionals alike are under ever increasing pressure to ensure the completeness and integrity of logs. This is particularly challenging during the process of transmitting log messages from the originating host via syslog to a centralized log repository. Leveraging the features of TCP, Snare Enterprise Agents are notified of any problems encountered during transmission and take appropriate actions to preserve event log continuity and completeness.

Log Message Simulcasting

Each Enterprise Agent is able to simultaneously direct event logs to multiple destination servers for redundancy, disaster-recovery and correlation purposes. Deployed along with a hot-standby Snare Server, perhaps deployed at an off-site disaster recovery site, Snare Enterprise Agents provide an extremely cost-effective, high-availability log management system. When deployed along with a 3rd party correlation engine or SEM tool, *Log Message Simulcasting* also facilitates a best-of-breed approach to both Log and Security Event Management.

Advanced Remote Control

Users of open source Snare Agents have for years appreciated the ability to remotely configure agents from the Snare Server console. However control has been limited to a single host IP address (or host name). The *Advanced Remote Control* feature allows each agent to be remotely configured from a set of “administrator” IP addresses or the IP address associated with the backup Snare Server.

Dynamic DNS Support

If DNS names are used in the configuration of either the *Advanced Remote Control* or *Log Message Simulcast* features, generally the host name is resolved only once as the agent starts up. With dynamic DNS support, the agent will automatically refresh the associated IP address every 10 minutes. This setting is crucial for installing new Snare Servers or dynamically changing the destination server in the event of a network or site failure (i.e. disaster recovery) without having to reconfigure or restart a single agent.

Centralized Configuration Management

In large networks with hundreds or thousands of log sources, maintaining a “gold standard” Snare Agent configuration has presented a challenge. Now, leveraging technology in Snare Enterprise Agents, the Snare Server console is able to query all deployed agents for their current configuration settings. The Snare Server will then automatically compare deployed agents with the “master” agent template and remotely apply, and activate, an updated configuration if necessary.



SYSTEM INTRUSION ANALYSIS & REPORTING ENVIRONMENT

SNARE Server Models:

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

All SNARE Servers include support for the open source agents.

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 pricing is also available.

Hardware Specifications

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

- 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
- 2 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.

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.