



System iNtrusion Analysis & Reporting Environment

Snare Enterprise Agents



The Benefits of Snare Enterprise Agents

Centralized log management and analysis is essential to assuring the integrity of critical logs and achieving compliance with a growing list of regulations. However the requisite process of transmitting log data across public or even private networks can simultaneously work against these important objectives. Unfortunately to date, log management vendors have not provided users with the tools necessary to address the challenge.

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 (which is included with the purchase of a Snare Server) 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 Snare Agent	Enterprise Snare 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		✓
Custom Windows Event Logs		✓

Snare Enterprise Agent Features

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. Common sources of transmission failures include:

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

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 *Advance 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.

Custom Windows Event Logs

Snare Enterprise Agents for Windows extend the reach of the open source Snare Agents beyond the core Windows Event Logs. The Snare Enterprise Agents for Windows enable the collection, filtering and transmission of non-standard and third party Windows Event Logs as well, greatly expanding the reach of the agent.

Summary

Is the Confidentiality, Integrity and Availability of distributed system logs critical to you? Do you currently manage a large deployment of open source Snare Agents? Are you looking for a cost-effective, end-to-end log analysis and management system? If the answer any of these questions is “yes”, then Snare Enterprise Agents offer high-value capabilities that simply cannot be found in any other solution available today.

If you have any questions about the features mentioned above, or would like to learn more about Snare Agents and Snare Server, please contact the team at Intersect Alliance using the details below.

Email: sales@intersectalliance.com

Web: <http://www.intersectalliance.com>

Telephone: +61 402 03 3347

© 1999-2011 Intersect Alliance Pty Ltd. All rights reserved worldwide.

Intersect Alliance Pty Ltd shall not be liable for errors contained herein or for direct, or indirect damages in connection with the use of this material. No part of this work may be reproduced or transmitted in any form or by any means except as expressly permitted by Intersect Alliance Pty Ltd. The Intersect Alliance logo and Snare logo are registered trademarks of Intersect Alliance Pty Ltd. Other trademarks and trade names are marks and names of their owners as may or may not be indicated. All trademarks are the property of their respective owners and are used here in an editorial context without intent of infringement. Specifications and content are subject to change without notice.