

System iNtrusion Analysis & Reporting Environment

Integrity
Auditability
Security



A Prophecy International Company

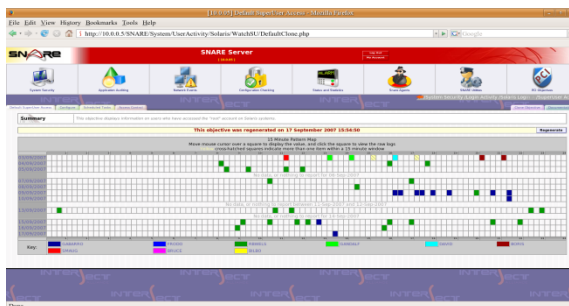
Snare

SNARE is a comprehensive set of event monitoring and analysis tools designed to address complex and mission critical auditing requirements. It comprises 2 separate yet complementary components; the Snare Server and the Snare Agents. While both can run independently of each other, together they provide a complete solution to auditing, managing and protecting your IT systems and data.

If Confidentiality, Integrity and Availability of distributed system logs is critical to your organization, or if you need to manage a large deployment of Snare Agents in a cost-effective manner, then you need the high-value capabilities of Snare which simply cannot be found in any other solution available today.

The Snare Server

The SNARE Server collects events and logs from your operating systems, applications, devices and from any other type of event-generating system. Snare provides a platform for powerful drill-down analysis and centralized log management in a format that is easy to use and navigate. Snares' growing and dynamic set of event analysis reports, coupled with effective query capabilities, provide regulatory compliance options, while managing your network and environment defenses.



In addition the Snare Server administers your Snare Agents. You can check and configure the agents as per your compliance and policy requirements as initially established or as they change over time.

The Snare Server comes equipped with a range of common security goals and objectives which can be cloned or copied to suit.

The Snare Server provides:









- 🚩 The ability to quickly and easily comply with **NISPOM, PCI, SOX** or other regulatory requirements using configuration wizards
- 🚩 The ability to collect any arbitrary log data, either via UDP or TCP protocols.
- 🚩 Proven technology that works seamlessly with the Snare agents.
- 🚩 Reflector technology that allows for all collected events to be sent, in real time, to a standby/backup Server.
- 🚩 The ability to continuously collect large numbers of events with rates exceeding 3,500 events per second and burst collection allowing over 50,000 events per second.
- 🚩 Automatic collection of events suitable for offline forensics analysis.
- 🚩 The ability to drill from summary information to raw log details.
- 🚩 Scalable Storage - billions of events on standard storage devices.
- 🚩 Responsiveness through advanced search algorithms and direct access to data.
- 🚩 Advanced Remote Control of Agents
- 🚩 The ability to track and monitor most standard requirements such as logins/logoffs, password expirations; unauthorized access to the computer systems; sensitive files; account privileges; user's access to the internet and more...

Snare Enterprise Agents

The SNARE Agents define the security relevant events for collection. Snare agents are the industry standard for logging and are available as in both Open Source and Enterprise versions. While both the Open Source and the Enterprise Agents gather operating system specific events are easy to install and upgrade, and provide objective based filtering, the Snare Enterprise Agents are specifically designed to greatly enhance the 3 pillars of information security:

1. Confidentiality
2. Integrity and
3. Availability

Any organization that needs to secure their environment and meet regulatory requirements cannot afford to do without the Snare Enterprise Agents which provide the following additional benefits:

-  **Encryption.** The Snare Enterprise Agents use the NIST recommended Triple DES algorithm to protect the confidentiality of log messages while in transit to the Snare Server.
-  **Event Log Caching.** The integrity of the overall log management system is significantly enhanced by event caching in case of a network outage or other transmission failure.
-  **Guaranteed Log Message Delivery.** Leveraging 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.
-  **Advanced Remote Administration.** Allows each agent to be remotely configured from an authorized set of “administrator” addresses.
-  **Dynamic DNS Support** is provided 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.** With the Snare Server and Enterprise Agents working in tandem, all deployed agents across the enterprise can have their configurations evaluated and updated.
-  **Custom Windows Event Logs.** 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.

Many thousands of organizations including Fortune 500, government agencies, multinational businesses and highly sensitive sites around the world rely on Snare every second of every day as the platform of choice for audit, collection, analysis, reporting, management and archival of event information.

Snare, the Trusted, Low risk, High Value SIEM choice.



For more information visit us at www.intersectalliance.com or contact us as follows:

The Americas 1 (800) 834 1060 Toll Free or +1 (303) 488 3451 Denver

Asia Pacific +61 8 8211 6188 Adelaide Australia

Europe and the UK +44 (797) 090 5011

or email us at intersect@intersectalliance.com

Intersect Alliance International 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 International Pty Ltd. The Intersect Alliance logo and Snare logo are registered trademarks of Intersect Alliance International 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.