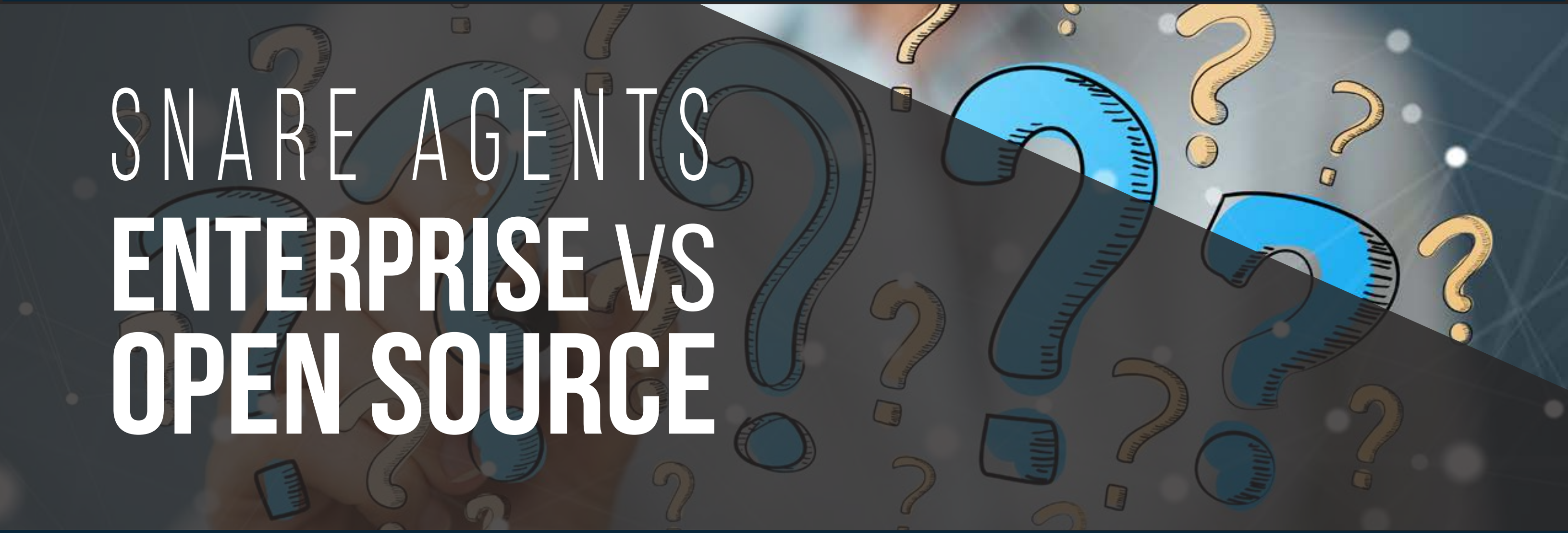
snare
A PROPHECY SOLUTION

# Snare Agents
# Enterprise vs Open Source

Whitepaper

snare
A PROPHECY SOLUTION

WHITEPAPER



# SNARE AGENTS ENTERPRISE VS OPEN SOURCE

## WHY COMPANIES AROUND THE WORLD ARE UPGRADING TO SNARE ENTERPRISE

### What Are Snare Agents?

Snare Enterprise Agents are the go to event logging agents for digital security experts around the world. That is why you find them used in conjunction with most SIEM servers, MSSPs and recommended by consultants around the world. They are easy to install and upgrade, provide objective based filtering and greatly enhance the three pillars of information security: Confidentiality, Integrity and Availability.

The Snare Agents are issued as both a free open source download, Snare Lite, as well as a commercially supported Enterprise Edition. There are three critical reasons why any serious organization needs to be using Enterprise Agents in their solution no matter the architecture:

- Support – If you need a supported security platform, as many compliance standards require, then you need to use the Enterprise Agent. The open source agent is provided to the open source community free of charge and as issued. The Enterprise Agents include maintenance, upgrades, bug fixes and full access to customer support.

- Dependability – If your organization needs to know that every log will be captured and forwarded with 100% certainty, then you need to use the Enterprise Agents. The open source agents does not support TCP, caching, custom event logs, UTC or registry audits.

- Compliance – The Snare team keeps Snare ahead of compliance standard such as PCI. The open source version has a number of vulnerabilities that will continue to grow overtime as support has been discontinued to ensure the Enterprise Edition is a s strong as it can possibly be.

For a more granular understanding we have provided a feature comparison on the following page to help you and your organization understand why we prefer our users leverage the Enterprise version of our Snare Agents over the antiquated open source versions.

| FEATURES | ENTERPRISE | OPEN SOURCE |
|---|---|---|
| Regulatory Compliance (NISPOM, PCI, SOX) | ✓ | ✗ |
| Windows 8 and Later | ✓ | ✗ |
| Guaranteed Message Delivery (TCP) | ✓ | ✗ |
| Encryption Using TLS | ✓ | ✗ |
| Event Log Caching | ✓ | ✗ |
| Log Message Simulcasting | ✓ | ✗ |
| Dynamic DNS Support | ✓ | ✗ |
| Centralized Configuration management | ✓ | ✗ |
| Custom Windows Event Log Sources | ✓ | ✗ |
| Enhanced Event Throttling | ✓ | ✗ |
| Agent Heartbeat | ✓ | ✗ |
| UTC | ✓ | ✗ |
| USB Device Monitoring | ✓ | ✗ |
| Group Policy Support | ✓ | ✗ |
| Truncation of Verbose Event Text | ✓ | ✗ |
| Single MSI for Windows Platforms | ✓ | ✗ |
| Vendor Product Support | ✓ | ✗ |
| Alt Syslog Destination Options (RFC5424) | ✓ | ✓ |
| Syslog Destination Options (RFC3164) | ✓ | ✓ |
| UDP Destination Options | ✓ | ✓ |
| Easy to Use Installer | ✓ | ✓ |
| Filter for Events of Interest | ✓ | ✓ |
| Remote Control Interface | ✓ | ✓ |
| View Local and Network Users and Groups | ✓ | ✓ |
| View Local Registry Configuration | ✓ | ✓ |
| Non-GUI Install Option | ✓ | ✓ |
| Upgrade Option to Preserve Settings | ✓ | ✓ |
| Debug Mode | ✓ | ✓ |