Snare Central

Snare Central is a flexible centralized logging solution that is SIEM agnostic and easily scalable.

It can be physical or virtual and is used to manage your agents, control the type and size of logs you send to your SIEMs, SOCs, and/or MSSP. Central receives logs from a wide array of sources such as servers, desktops, databases, network devices (firewalls, routers, switches, etc) text-based log files and other endpoints.

Key Central Features

1. Ingest syslog feeds from any device
2. We have LDAP integration and RBAC capabilities
3. SNMP trap alerts from network devices
4. Batch bulk uploads of archived data

We have lightweight agents for MSSQL, Epilog, WEC Windows Server and Desktops, Linux, Solaris and MacOS.

Plus Central supports your **security** and **compliance** needs!

- Our agents provide point-to-point encryption of log data using TLS.
- Data is not encoded in a proprietary closed format and can be exported for forensics as needed.
- We support password complexity rules for user accounts for better security.
- Support PCI, SOX, HIPAA, NISPOM and other regulatory requirements.
- Up to 50:1 compression on log storage.

Central Has 3 Major Components

Agent Management, Snare Reflector and Snare Repository

Agent Management

Snare Central includes the ability to manage and upgrade your agents from a central location. From agent updates to policy configuration and management for select groups or all agents based on security and compliance needs.

- Use one or more policy master templates for different systems (Domain Controllers, Application servers, desktops, database servers etc)
- Use different policies for different times of the day using schedules
- Support for all v5 and later agents
- Status indicators of when agents are online or if systems are down and not reporting logs
- EPS rate changes via the healthchecker

Snare Reflector

The Reflector can send data in real-time to one or more destinations, using UDP or TCP with TLS encryption enabled. We send logs in any of major formats including both syslog types 3164 and 5424. The reflector can also reflect the received format such as if the original system or Snare agent was sending in that format. The reflector also has some smart syslog formats for when sending to QRadar and RSA Envision. One major benefit of our reflector is its ability to parse logs based on the destination's purpose.

- Only send critical logs to each destination
- Or a different set of logs to each destination
- Filter out logs you don't need, reducing SIEM costs
- Cache logs when network flow is interrupted

For environments that need to manage sensitive data the reflector can **mask sensitive data** using its regex parsing before its reflected to the other destination.

Snare Repository

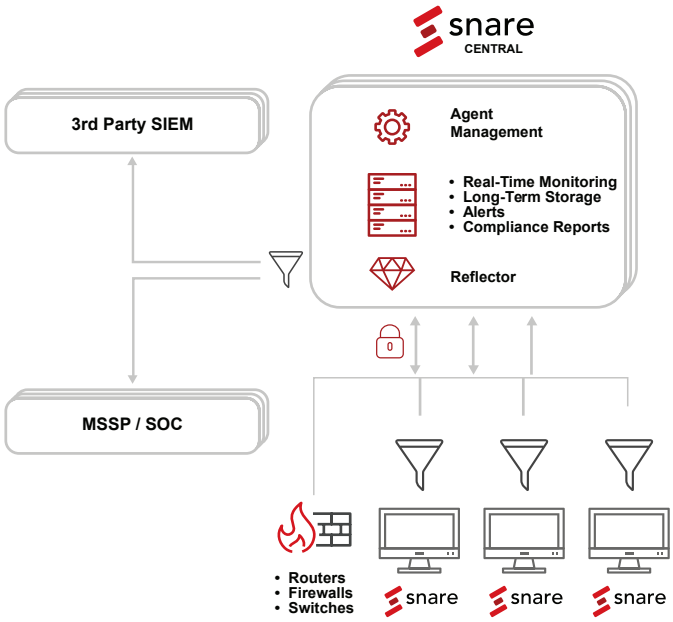
The Snare Repository is where you'll find critical capabilities, including the following features:

- Real-Time Monitoring
- Long-Term Storage
- Alerts
- Compliance Reports
- End to End Encryption

Network File System and packages (NFS) are included in the base operating system to allow for custom configuration of NFS as needed. NFS can be used to connect to popular NAS systems to expand the usable disk or to allow archiving or data backups to another location. This allows organizations to keep as much data as needed, without compromising performance or increasing licensing costs.

Snare Central helps address forensic needs, giving you the ability to store logs based on your compliance requirements, generally between 3 to 7 years, but can be as long or short as your organization requires.

The Snare Repository is also where all 200+ out-of-the-box reports, including ones for compliance and audits, are found. Any of these reports can be customized to your specific needs. Repository users also love the fact that our Alerts are intelligent as they can be configured to alert only when multiple security events happen at the same time using our threshold reporting feature.



Central comes with over 200 out-of-the-box reports and dashboards to help with your security and compliance needs.

Contact us

Toll Free US: 1 (800) 834 1060
Denver Office: 1 (303) 771 2666
Asia Pacific: +61 8 8213 1200
UK/Europe: +44 (797) 090 5011

US Headquarters

8480 E Orchard Rd. Suite 4350
Greenwood Village, CO 80111

Corporate Headquarters

Level 1, 76 Waymouth Street
Adelaide, South Australia 5000, Australia

ABN: 84 151 743 976