



Snare Central
Unifying Log Management.
Enhancing Cyber Resilience.

Why Snare Central?

Snare Central is the secure, scalable, and purpose-built centralized log management platform for organizations that demand full visibility, compliance, and actionable insights. As the core of the Snare Suite, it empowers teams to collect, analyze, and manage logs across hybrid environments with unmatched efficiency and reliability.

Whether you're meeting compliance mandates, hunting threats, or optimizing performance, Snare Central delivers

Key Capabilities

Feature	Description
Centralized Log Aggregation	Collect logs from thousands of endpoints across Windows, Linux, Mac, and cloud environments.
Role-Based Access Control (RBAC)	Granular permission management to protect sensitive data and meet internal policies.
Custom Parsing & Filtering	Tailor how data is collected, processed, and forwarded to suit your SIEM or analytics needs.
Real-Time Alerting	Trigger alerts based on predefined rules to detect anomalies or suspicious activity.
Agent Management	Seamless deployment, configuration, and health monitoring of Snare Agents across the enterprise.
Dashboards & Reporting	Out-of-the-box dashboards and customizable reports for compliance (PCI-DSS, ISO 27001, GDPR, etc.).
Log Forwarding	Native support for forwarding logs to SIEMs including Securonix, IBM QRadar, Elastic, Devo, and more.
High Availability & Scalability	Built to grow with your environment—supports clustered setups and large-scale log ingestion.

USE CASES & BUSINESS OUTCOMES

Compliance & Audit Readiness

Use Case: Meet evolving industry regulations with comprehensive, auditable log trails.

Outcome: Reduced risk of fines and audit failures through centralized, compliant log storage.

Threat Detection & Forensics

Use Case: Detect malicious behaviour with real-time alerts and investigate incidents with historical logs.

Outcome: Faster incident response and stronger cybersecurity posture.

IT Operations & Troubleshooting

Use Case: Gain visibility into system performance and troubleshoot configuration or service issues.

Outcome: Decreased downtime and improved service reliability.

Customer Snapshot:

Global Financial Services Company

Challenge:

Lacked centralized log visibility across multiple regions and platforms.

Solution:

Deployed Snare Central alongside Snare Agents across 5 countries.

Outcome:

- 100% compliance with APRA and PCI-DSS within 90 days
 - Reduced SIEM ingestion volume by 35%
- Cut incident investigation time from days to hours

IEM Optimization

Use Case: Pre-process, filter, and enrich logs before sending to your SIEM to reduce ingestion costs.

Outcome: Lower SIEM license fees and better data quality for threat analysis.

Hybrid Environment Visibility

Use Case: Collect and analyze logs from on-prem, cloud, and remote endpoints in a single pane of glass.

Outcome: Consistent visibility and control across diverse IT infrastructures.



How Snare Central Works in the Suite

Snare Central acts as the secure command center of the **Snare Suite**, complementing:

- **Snare Agent:** Lightweight endpoint agent for secure, reliable log collection.
- **Snare Reflector:** Real-time log forwarding, load balancing, and SIEM optimization.

Together, they deliver a powerful, end-to-end solution for enterprise-grade log management.



Snare Agents
Secure, forensic-grade
log collectors.



Snare Reflector
Intelligent routing
and transformation



Snare Central
Secure, cost effective
storage and compliance

Who Uses Snare Central?

- Financial Services & Insurance
- Government & Defence
- Healthcare
- Critical Infrastructure
- Retail & Telecommunications
- Education & Research

Why Choose Snare?

- Proven in over 4,000 organizations worldwide
- 24/7 global support with unlimited technical assistance
- Trusted by military and intelligence agencies
- Vendor-neutral, SIEM-agnostic
- Simple licensing. No hidden costs.



Coming Soon in v8.7

Powerful Enhancements

Snare Central 8.7 takes things to the next level with exciting new capabilities:

01

Native API Integration with Azure Sentinel

Streamlined, secure delivery of logs directly into Microsoft Sentinel.

02

ASIM Mapping Support

Ensures normalization of data for improved analytics and compliance in Microsoft ecosystems

03

Expanded Integration Ecosystem

Enhanced compatibility with QRadar, Taegis, and upcoming support for Splunk, Microsoft Sentinel and other platforms.

04

UI & Performance Enhancements

Improved usability and speed across core admin functions.

Let's Talk About Your Log Management Strategy

Whether you're upgrading from legacy systems or consolidating multiple tools, Snare Central offers the visibility, compliance, and peace of mind you need.

www.snaresolutions.com/snare-central

