snare
A PROPHECY SOLUTION

Snare in High-Volume Environments

Real-World Customer Use Cases for Scalable, Controlled Logging

High-volume environments

expose the cracks in traditional logging strategies faster than any other setting.

In 2025, organisations operating at scale learned a hard lesson:

Volume without control doesn't just increase cost, it increases risk.

This use-case collection shows how organisations are using Snare to regain visibility, protect investigations, and keep SIEM costs predictable in the most demanding environments.

Use Case 1: Global Financial Services Organisation

Reducing SIEM Costs Without Sacrificing Audit Readiness

Environment:

- Tens of thousands of endpoints across regions
- Strict regulatory and audit requirements
- Centralised SIEM with ingestion-based pricing

Challenge:

The organisation faced runaway SIEM costs driven by:

- Verbose endpoint logging
- Long retention requirements
- Inability to selectively ingest logs without creating audit gaps

Security teams were forced to choose between:

- Cost control
- Compliance confidence

How Snare Helped:

- Implemented **endpoint-level filtering** to remove low-value noise
- Preserved **forensic-grade audit** logs at full fidelity
- Routed high-value security events to SIEM
- Archived compliance logs separately for long-term retention

Outcome:

- SIEM ingestion reduced by **~40%**
- Storage requirements reduced by **~85%**
- Audit posture strengthened with defensible evidence
- No loss of investigation capability

Use Case 2: National Government Agency

Ensuring Evidence Integrity Across Critical Systems

Environment:

- Highly regulated public-sector environment
- Sensitive systems requiring defensible audit trails
- Long-term log retention mandates

Challenge:

During internal investigations, teams discovered:

- Critical endpoint logs missing due to retention limits
- Inconsistent logging policies across agencies
- Difficulty proving chain-of-custody

How Snare Helped:

- Standardised logging policies across endpoints
- Ensured **immutable, timestamp-accurate log capture**
- Enabled **log replay** for post-incident reconstruction
- Centralised policy management without centralising raw data

Outcome:

- Improved investigation confidence
- Faster response to regulator and auditor queries
- Reduced operational risk during incident reviews

Use Case 3: Large-Scale MSSP

Scaling Customers Without Linear Cost Growth

Environment:

- Hundreds of customer environments
- Multi-tenant SIEM platform
- Pressure to deliver predictable pricing

Challenge:

The MSSP's SIEM costs grew linearly with customer growth.

Each new customer increased:

- Ingestion volume
- Infrastructure overhead
- Margin pressure

How Snare Helped:

- Deployed Snare as a **standardised log control layer**
- Created **baseline logging policies** for all customers
- Applied **customer-specific routing** rules
- Reduced noise before SIEM ingestion

Outcome:

- Improved investigation confidence
- Faster response to regulator and auditor queries
- Reduced operational risk during incident reviews

Use Case 4: Utilities & Critical Infrastructure Provider

Maintaining Visibility Across OT and IT Systems

Environment:

- Mix of legacy systems and modern platforms
- High event volumes during operational peaks
- Zero tolerance for investigation blind spots

Challenge:

Operational spikes generated massive log bursts, overwhelming:

- SIEM ingestion
- Storage capacity
- Analyst workflows

How Snare Helped:

- Applied **policy-based filtering** during high-volume periods
- Prioritised security-relevant events
- Preserved raw logs for forensic replay
- Reduced alert fatigue during peak activity

Outcome:

- Stable security operations during peak load
- Reduced alert noise
- Faster post-incident analysis

Use Case 5: Enterprise with Rapid Cloud & AI Expansion

Preparing Logging for AI-Driven Volume Growth

Environment:

- Hybrid cloud infrastructure
- AI-enabled applications generating new telemetry
- Expanding attack surface

Challenge:

Operational spikes generated massive log bursts, overwhelming:

- SIEM ingestion
- Storage capacity
- Analyst workflows

How Snare Helped:

- Controlled log volume **before downstream ingestion**
- Normalised multi-source events into consistent formats
- Routed AI telemetry to analytics platforms instead of SIEM
- Preserved security-critical logs for investigations

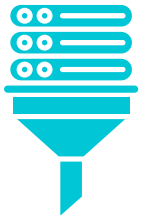
Outcome:

- Logging architecture future-proofed for AI growth
- SIEM costs stabilised
- Investigation readiness maintained

Common Patterns Across High-Volume Environments

Across all use cases, successful teams shared the same approach:

Control logs at the source



Filter before cost is incurred

Route logs based on purpose

Preserve forensic integrity

Design for investigation, not ingestion

Snare consistently acts as the **control plane** that enables this model.

Why Snare Works in High-Volume Environments

Snare is purpose-built for scale:

- Handles millions of events per day
- Supports granular, policy-based filtering
- Maintains evidentiary integrity
- Integrates cleanly with SIEMs and analytics platforms
- Reduces operational and financial risk

It doesn't reduce visibility, It **restores control, while still ensuring that we have the visibility required.**

Next Steps

Book: *A High-Volume Log Strategy Session*

Assess: *Is Your Logging Architecture Ready for 2026?*

Toll Free US: 1(800) 834 1060
Asia/Pacific: +61 8 8213 1200
UK/Europe: +44 (800) 368 7423

AMERsales@prophecyinternational.com
APACsales@prophecyinternational.com
EMEAsales@prophecyinternational.com

snare
A PROPHECY SOLUTION