snare
A PROPHECY SOLUTION

Event Logging Strategy Checklist

Build a smarter, cheaper, stronger logging foundation

Step 1: Map Your Critical Assets & Use Cases

□ Identified mission-critical systems (Identity, cloud APIs, privileged access, key apps, cloud services, domain controllers, databases, firewalls, network devices, endpoints.)

□ Built a logging priority matrix (impact vs likelihood)

□ Linked logs directly to business outcomes (detection, compliance, forensics)

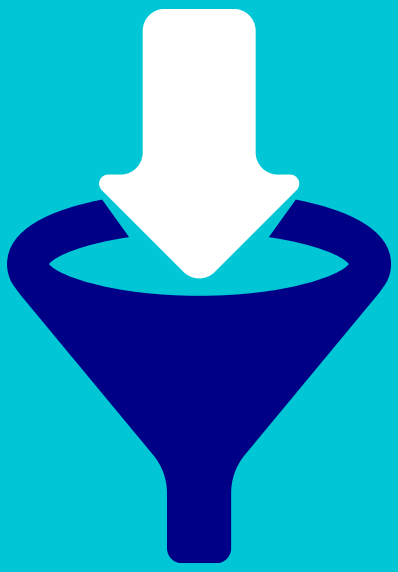
Step 2: Deploy a Trusted Collection Layer

□ Using lightweight reliable agents across all environments

□ Ensured log traffic is encrypted in transit

□ Implemented Centralized Storage, preventing local tampering or deletion

□ Coverage includes on-prem, cloud, and containers



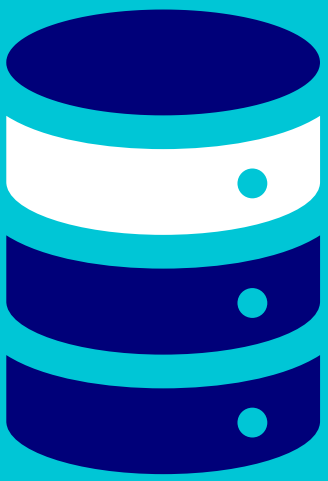
Step 3: Filter & Enrich Early

□ Filtering noise at the source to reduce SIEM costs

□ Enriching logs with context (user, device, geolocation, system role)

□ Measuring ingestion savings from smarter pre-processing

□ Sensitive data is masked



Step 4: Segment Log Tiers

□ Identified log retention period mandated by relevant industry standards

□ Implemented low-cost long-term storage

□ Implemented access controls to centralised log repository

Step 5: Ensure Integrity & Retention

□ Cryptographic checksums or hashes applied to detect tampering

□ Write-once (WORM) storage enabled for audit logs

□ Retention policies mapped to compliance (PCI DSS, GDPR, Essential 8, HIPAA, ISO/IEC 27001)

□ Access restricted, monitored, and fully auditable

Step 6: Correlate, Alert & Act

□ Correlation rules tuned across multiple sources (e.g., MFA + privilege escalation)

□ Alerts and anomalies reviewed and acted upon regularly

□ Integration with SOAR or automation workflows in place

□ Logs shared with threat intel feeds for stronger detection

Step 7: Review, Refine, Repeat

□ Quarterly logging health checks scheduled

□ SIEM costs and ingestion volumes reviewed regularly

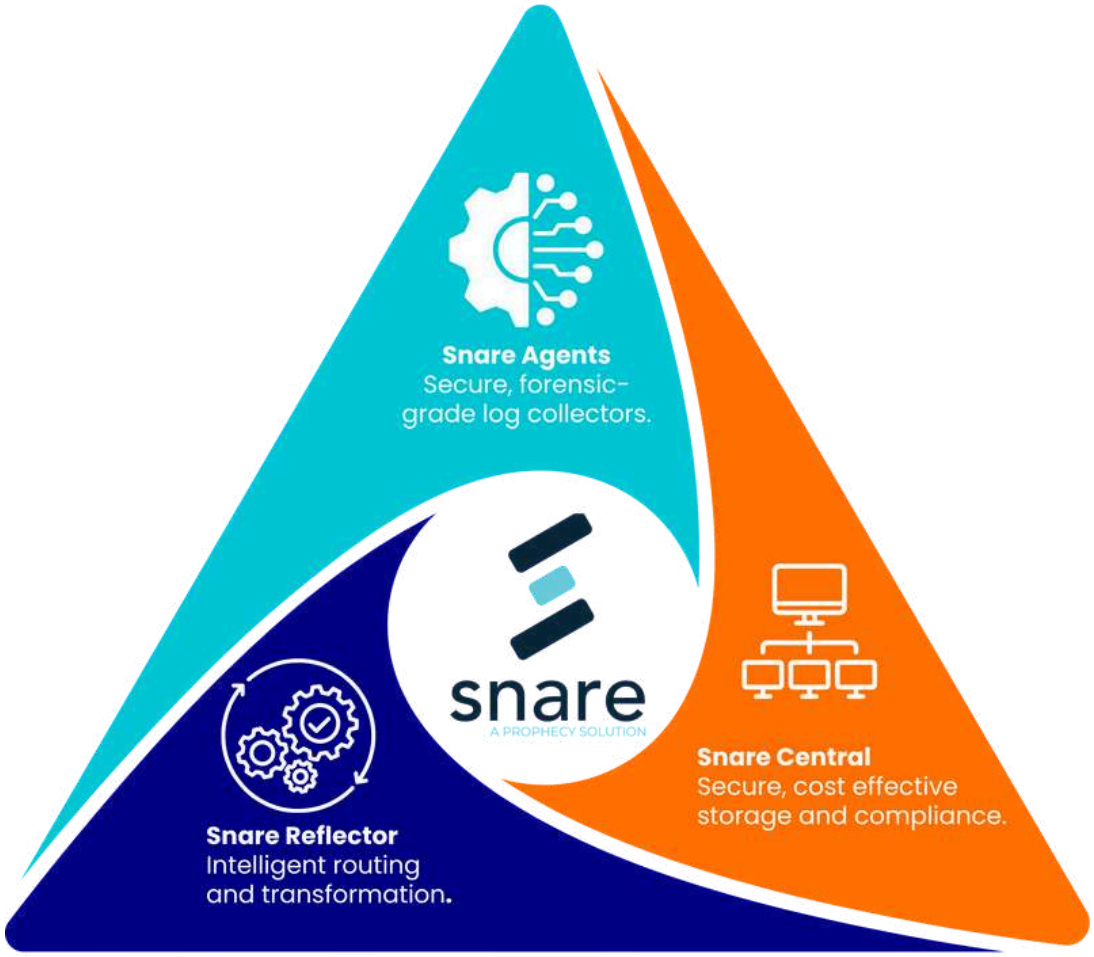
□ Controls updated for new regulations and system changes

□ Logs tested in mock forensic investigations

□ Systems and infrastructure coverage is reviewed regularly

How Snare helps build a smarter, cheaper, stronger logging strategy

- **Enterprise-grade log collection** across hybrid environments
- Up to **90% SIEM cost reduction** through smart filtering
- **85%-90% reduction in data Storage**
- **Forensic-grade integrity** to meet compliance & audit requirements
- **Vendor-Agnostic, SIEM-Ready Integration** with Splunk, Sentinel, QRadar, Securonix & more
- **Lightweight, Scalable, and Secure Architecture** including security features like encryption in motion, centralized management (SAM), and audit controls



snare
A PROPHECY SOLUTION

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