snare
A PROPHECY SOLUTION

MSSP Logging Baseline Template

Policy + Architecture for Scalable, Profitable Security Services

Purpose:

This template provides MSSPs with a repeatable, defensible logging baseline that balances security outcomes, investigation readiness, and commercial scalability.

It is designed to be:

- Customer-agnostic by default
- Customisable per tenant
- Aligned to modern SIEM cost models
- Investigation- and evidence-led

This baseline reflects what high-performing MSSPs converged on through 2025 — and what will be expected as table stakes in 2026.

Part 1: MSSP Logging Policy Baseline

1. Policy Objectives

The MSSP logging policy must achieve five outcomes:

1. Enable rapid, accurate investigations
2. Preserve forensic-grade evidence
3. Control ingestion and storage costs
4. Standardise onboarding and operations
5. Support customer audit and compliance needs

Policy principle:

Logs are collected with intent — not by default.

2. Log Classification Framework

All logs must be classified before ingestion.

Log Class	Purpose	Default Destination
Security-Critical	Detection & investigation	SIEM
Audit & Compliance	Proof & regulatory response	Long-term archive
Operational / Telemetry	Trends & performance	Analytics platform
Low-Value / Noise	Context only	Filtered / summarised

Rule: If a log does not clearly map to a class, it must be reviewed before ingestion.

3. Mandatory Log Categories (Baseline)

These logs are non-negotiable across all customers unless contractually excluded.

Identity & Access

- Authentication events
- Privilege escalation
- Account lifecycle changes

System Activity

- Process execution
- Service and scheduled task changes
- System start/stop and time changes

Configuration & Policy

- Security policy changes
- Logging service interruptions
- Agent or control-plane modifications

File & Object Activity

- Create / modify / delete events on sensitive paths

4. Filtering & Noise Reduction Policy

Filtering must occur at the source wherever possible.

Allowed filtering:

- Verbose informational events
- Repetitive low-risk system messages
- Known benign activity patterns

Prohibited filtering:

- Authentication events
- Privilege changes
- Log tampering indicators
- Timestamp or source metadata

Non-negotiable rule:
Filtering must never compromise forensic reconstruction.

5. Retention Standards (Baseline)

Log Type	Minimum Retention
Security-Critical	90–180 days (SIEM)
Audit & Compliance	1–7 years (archive)
Investigation Evidence	Case duration + policy
Operational Logs	Customer-defined

Retention is **policy-driven,** not platform-driven.

6. Customer-Specific Policy Overrides

Customers may request:

- Additional log classes
- Extended retention
- Alternate destinations

All overrides must be:

- Documented
- Costed
- Approved

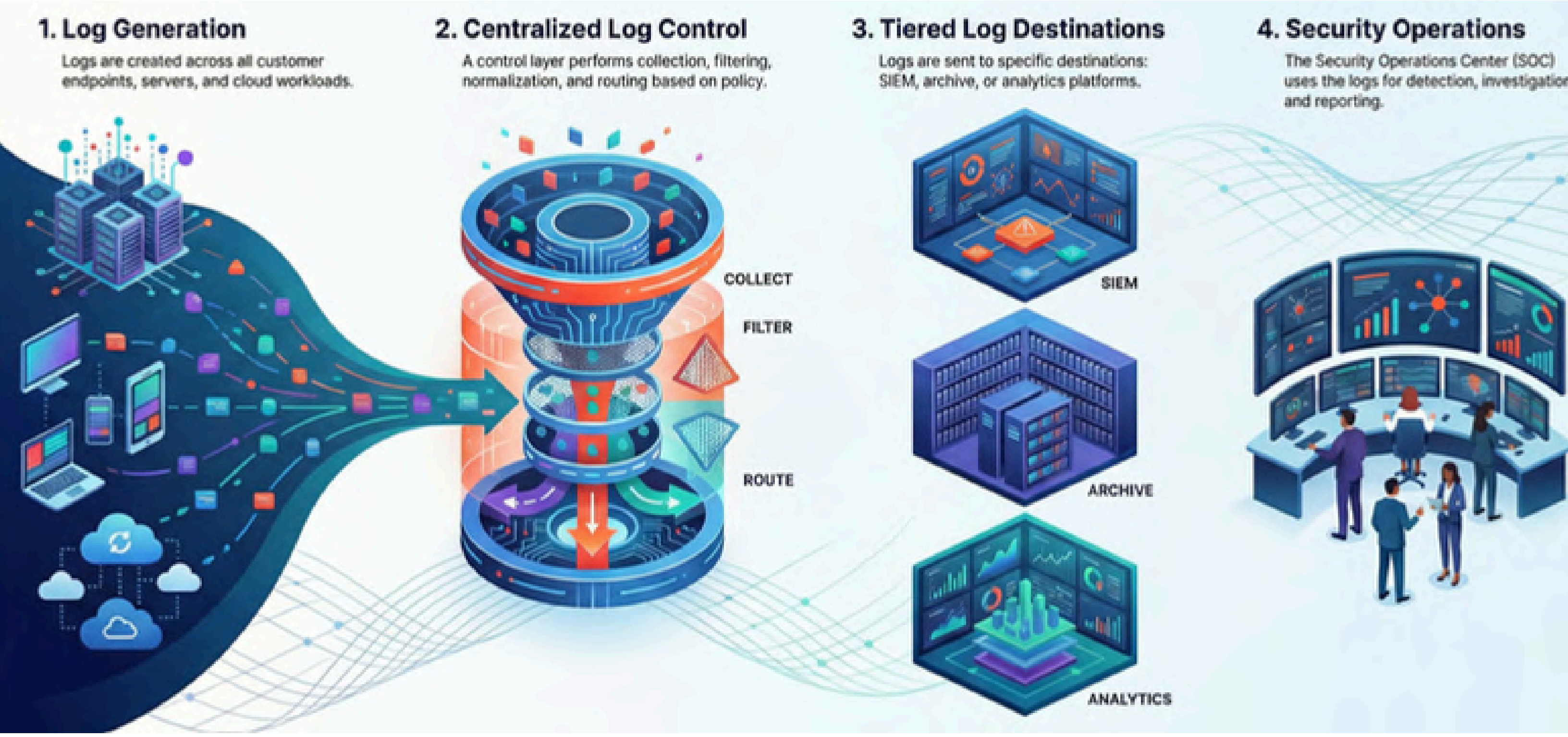
This prevents silent margin erosion.

Part 2: MSSP Reference Logging Architecture

1. Architectural Principles

- Control upstream, not downstream
- Separate security value from data volume
- Design for investigation first
- Keep SIEM focused on high-value signals

2. Reference Architecture Overview



1. Log Generation

Logs are created across all customer endpoints, servers, and cloud workloads.

2. Centralized Log Control

A control layer performs collection, filtering, normalization, and routing based on policy.

3. Tiered Log Destinations

Logs are sent to specific destinations: SIEM, archive, or analytics platforms.

4. Security Operations

The Security Operations Center (SOC) uses the logs for detection, investigatio and reporting.

3. Multi-Tenant Design Requirements

- Logical separation per customer
- Policy inheritance with override capability
- Tenant-specific routing rules
- Cost attribution per tenant
- This enables predictable pricing and clean onboarding.

4. Investigation & Evidence Handling

For every incident, the architecture must support:

- Timeline reconstruction
- Log replay
- Evidence preservation
- Export for legal or regulatory review

If evidence cannot be reconstructed independently of the SIEM, the architecture is incomplete.

Part 3: Operational Governance

1. Policy Ownership

- MSSP Security Architecture team owns the baseline
- SOC teams enforce and validate
- Sales cannot override policy without approval

2. Review Cadence

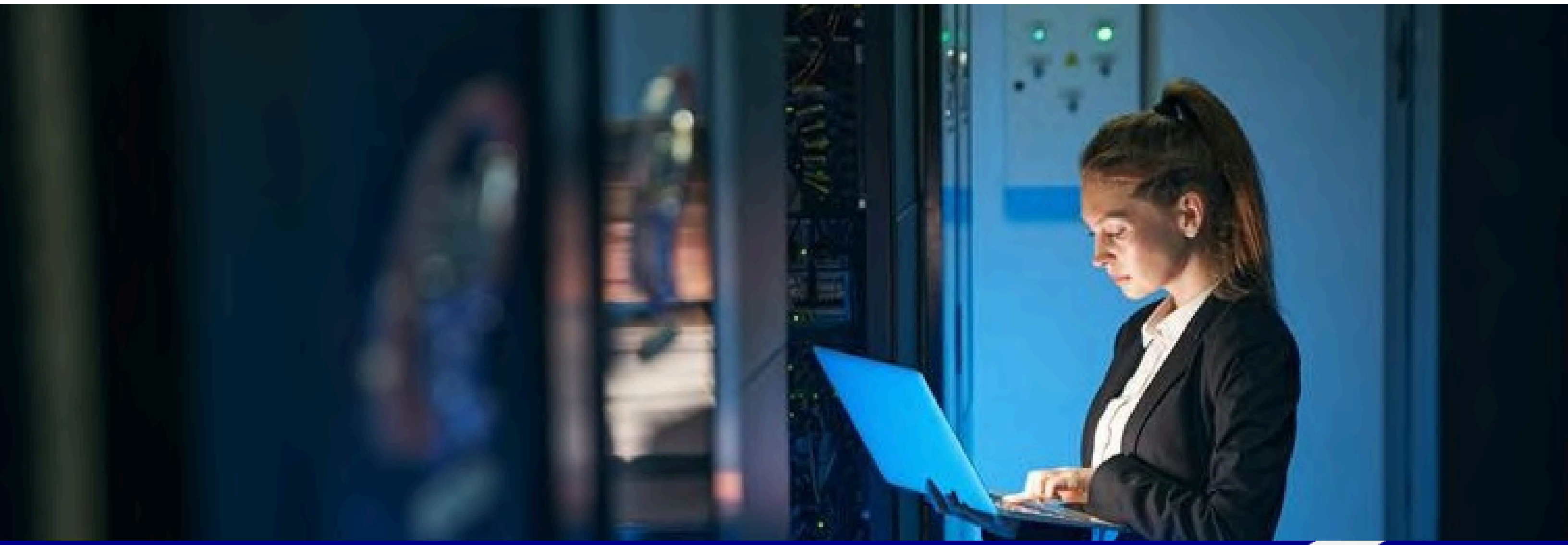
- Quarterly policy review
- Post-incident validation
- Annual customer attestation

3. Metrics That Matter

Track:

- SIEM ingestion per customer
- Cost per log class
- Investigation time-to-answer
- Logs missing during investigations

These metrics protect both security outcomes and margins.



Part 4: Commercial Alignment

A strong logging baseline enables MSSPs to:

- Offer tiered service plans
- Price predictably
- Avoid SIEM-driven margin erosion
- Differentiate on investigation quality

Shift the conversation from:
“How many logs do you ingest?”

To:

“How fast can you prove what happened?”

Part 5: How Snare Enables the MSSP Logging Baseline

The MSSP logging baseline defined in this template is deliberately tool-agnostic at the policy level.

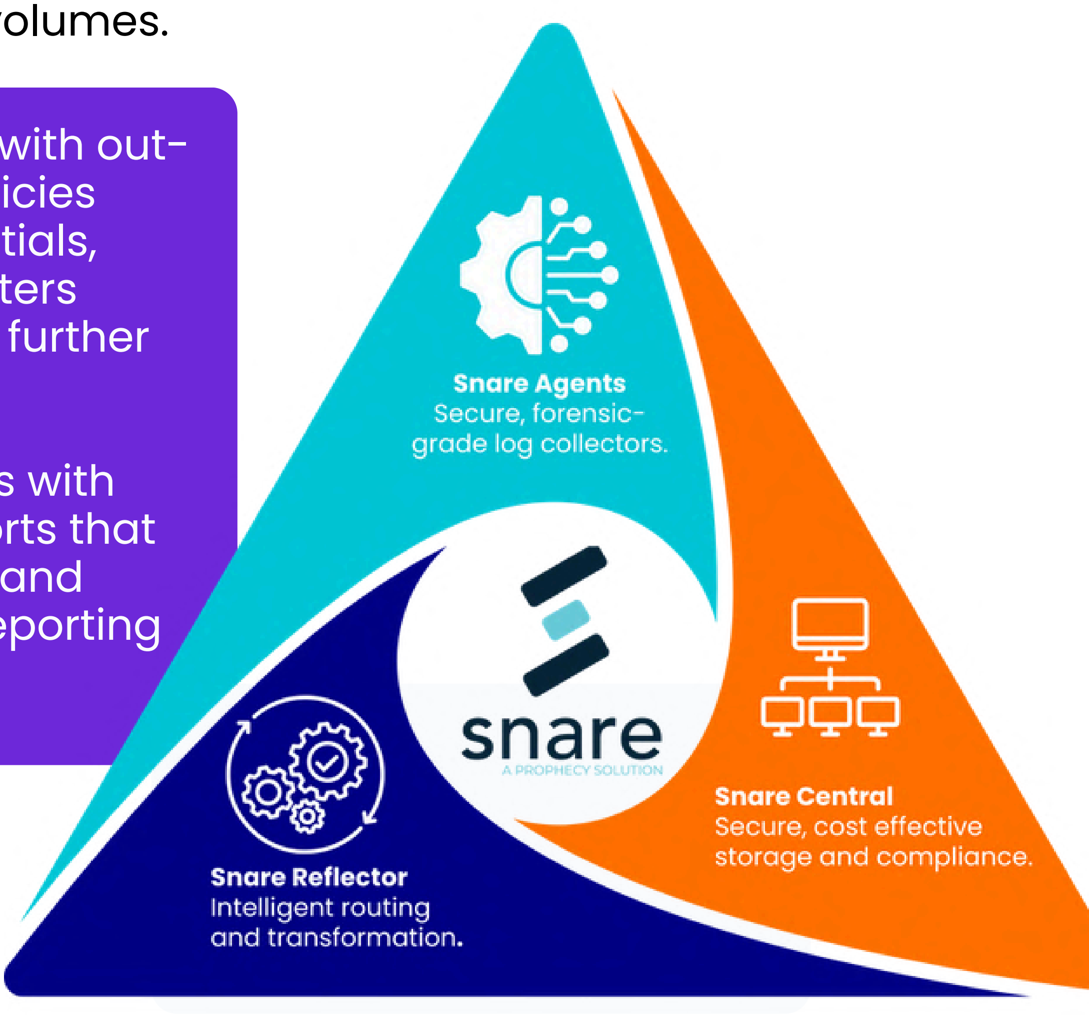
However, executing it consistently at scale requires a control layer that operates before logs reach downstream platforms.

This is where Snare fits into the MSSP architecture.

Snare acts as the enforcement and control plane that turns logging policy into operational reality — across customers, environments, and volumes.

Snare Agents come with out-of-the-box audit policies that cover the essentials, and have efficient filters applied, that can be further customised.

Snare Central comes with out-of-the-box reports that cover essential logs and make compliance reporting easy.


Snare Agents
Secure, forensic-grade log collectors.
snare
A PROPHECY SOLUTION
Snare Central
Secure, cost effective storage and compliance.
Snare Reflector
Intelligent routing and transformation.

1: Snare’s Role in the MSSP Stack

Snare sits between customer systems and destination platforms, enabling MSSPs to:

- Enforce logging policy at the point of collection
- Control volume before SIEM ingestion costs are incurred
- Maintain forensic-grade evidence independent of downstream tools
- Standardise logging across customers without losing flexibility

Snare does not replace SIEM, SOAR, or analytics platforms.

It ensures those platforms receive only the logs they are meant to handle.

2. Policy Enforcement at Scale

Snare enables MSSPs to operationalise the baseline policy by:

- Applying policy-based filtering aligned to log classes
- Mapping log type → destination (SIEM, archive, analytics)
- Enforcing non-negotiable log categories consistently
- Preventing unauthorised or accidental policy drift

This allows MSSPs to maintain a single baseline policy, with controlled, documented customer overrides.

3. Multi-Tenant Consistency Without Rigidity

For MSSPs, the challenge is not defining policy — it's enforcing it consistently across tenants.

Snare supports:

- Centralised policy management
- Tenant-specific routing rules
- Environment-specific tuning (without breaking the baseline)
- Clear separation of customer data and controls

This enables:

- Faster onboarding
- Predictable pricing
- Reduced operational overhead

4. Investigation & Evidence Assurance

Snare directly supports the investigation and evidence requirements defined earlier by:

- Preserving timestamps, metadata, and event fidelity
- Capturing log tampering and logging service interruptions
- Supporting log replay and timeline reconstruction
- Maintaining evidence integrity even when SIEM retention expires

For MSSPs, this means:

- Investigations are not constrained by SIEM retention windows
- Evidence can be produced independently of detection platforms
- Customer and regulator confidence is strengthened

5. Commercial Impact for MSSPs

When used as the logging control layer, Snare enables MSSPs to:

- Decouple security value from data volume
- Offer tiered service models with confidence
- Reduce SIEM infrastructure growth
- Protect margins as customers scale
- Compete on investigation quality, not ingestion volume

This directly supports the commercial alignment goals defined in Part 4.

6. What Snare Enables That Policy Alone Cannot

Requirement	Policy Only	Policy + Snare
Source-level filtering	❌	✅
SIEM cost control	❌	✅
Forensic replay	⚠️	✅
Tenant policy enforcement	⚠️	✅
Scalable onboarding	❌	✅
Evidence independence from SIEM	❌	✅

Why Snare Matters in the Baseline

The MSSP Logging Baseline defines what should happen.
Snare ensures it actually happens — every time, at scale.

It turns logging from:

A cost risk and operational burden

Into:
A controlled, defensible, and scalable service capability.

Appendix:
MSSP Logging Baseline – Quick Start Checklist

□ **Log classes defined**

□ **Filtering rules documented**

□ **Retention standards approved**

□ **Architecture validated**

□ **Customer override process defined**

□ **Cost attribution enabled**

Final Thought

MSSPs don’t fail because they lack tools.

They fail when logging grows faster than control.

A strong baseline fixes that — once, and at scale.

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