snare
A PROPHECY SOLUTION

The Log Strategy Reset

A Practical Guide for CISOs & MSSPs Entering 2026

Because more logs don't mean better security. Better strategy does.

Executive Summary

By the end of 2025, most security leaders reached the same conclusion:

"We have more logs than ever — and less confidence than we should."

SIEM costs exploded. Investigations stalled. Compliance pressure increased.

And AI-driven systems added **volume without context.**

The Log Strategy Reset is designed to help CISOs and Managed Security Service Providers (MSSPs) rethink logging from the ground up — shifting from log accumulation to log intent.

This guide shows you:

- Which logs actually matter
- Where volume should be controlled
- How to reduce cost **without losing evidence**
- How to build a logging strategy that scales into 2026 and beyond

1. Why Traditional Logging Failed in 2025

Most logging architectures were built on one flawed assumption:

"We'll collect everything and decide later."

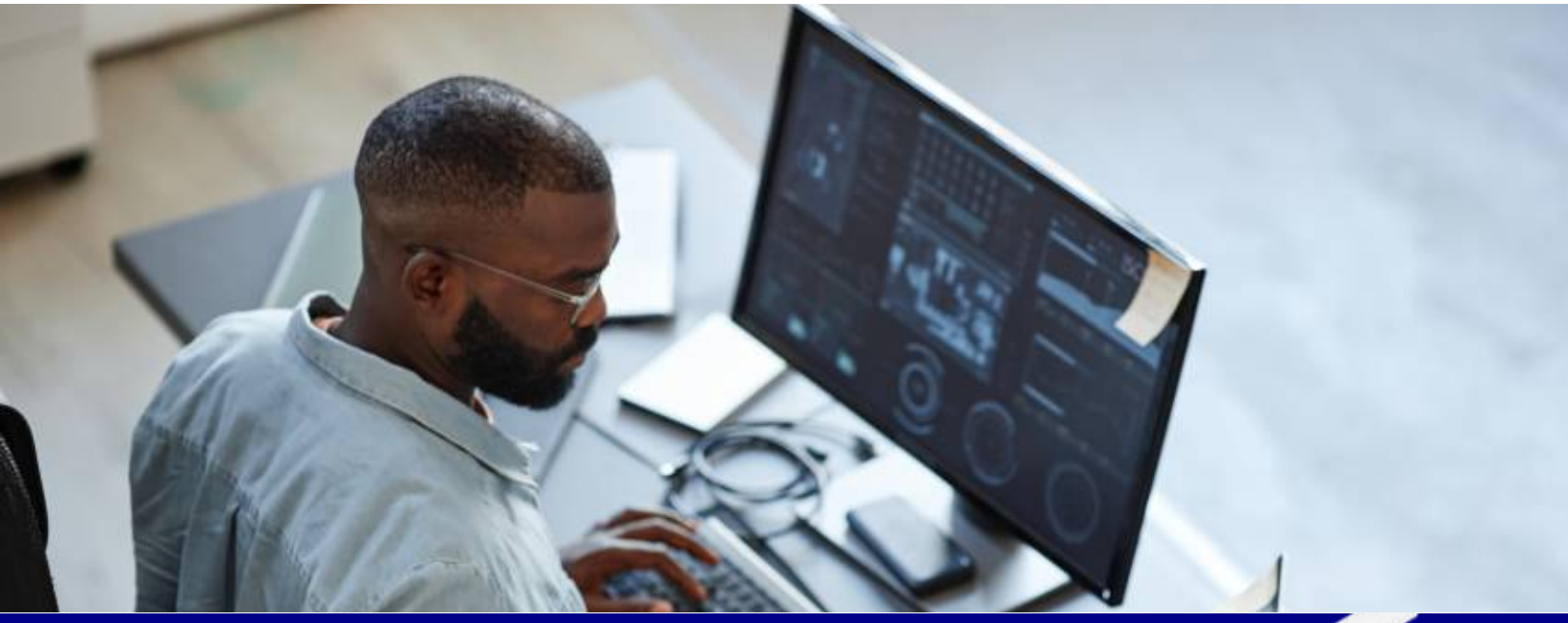
In 2025, that model broke.

What went wrong:

- **SIEM pricing penalised visibility**
- **Retention windows shrank**
- **Critical logs rolled off first**
- **Noise drowned investigation signals**
- **Teams feared turning logs off**

The result?

Organisations paid more — and knew less.



2. The New Reality: Logs Are Evidence, Not Exhaust

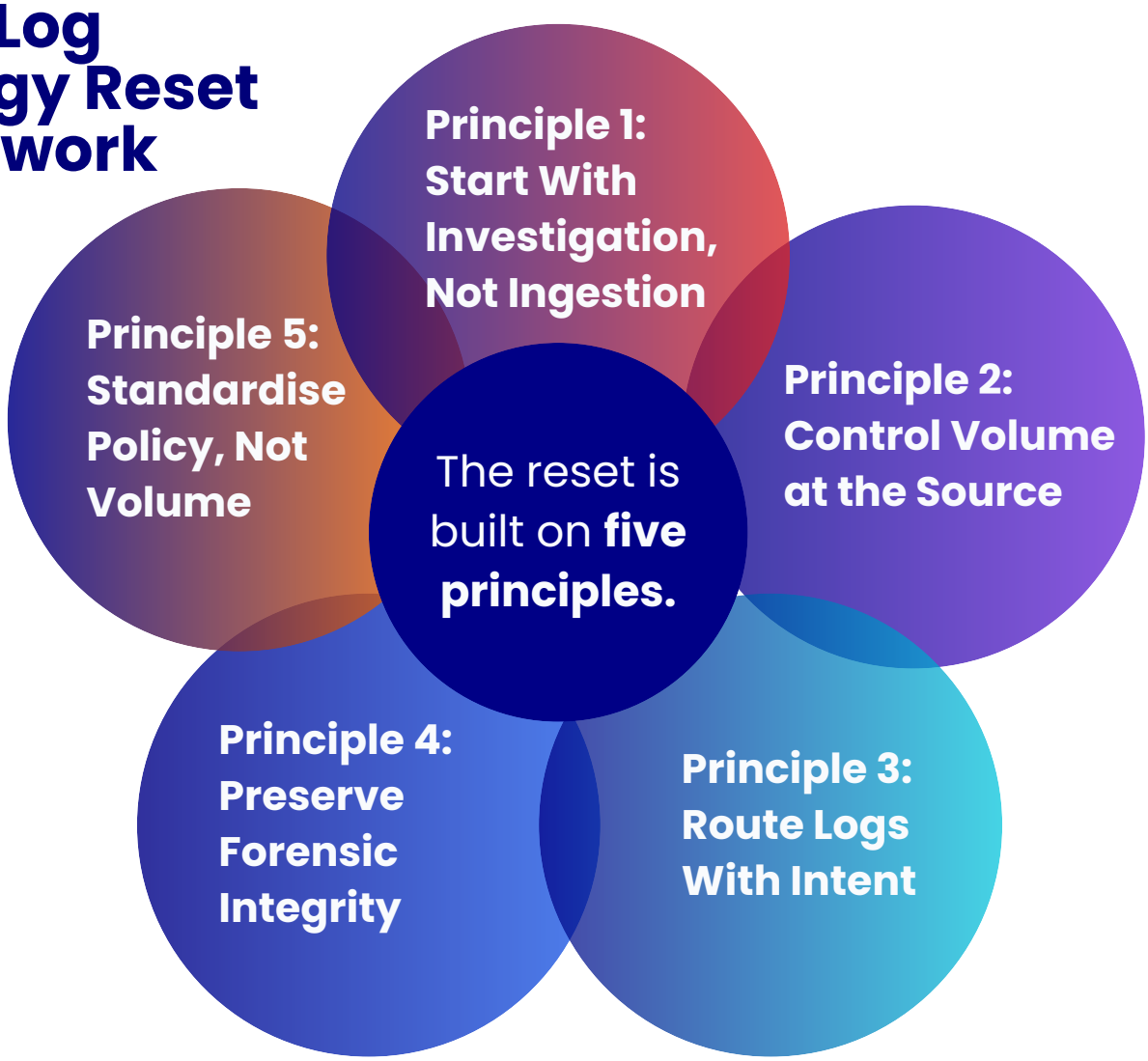
In modern security operations, logs serve three critical purposes

1. **Detection** – identifying suspicious activity
2. **Investigation** – reconstructing what actually happened
3. **Proof** – demonstrating compliance, diligence, and response

If a log doesn't clearly support at least one of these outcomes, it shouldn't exist — or it should be filtered, summarised, or routed elsewhere.

---

3. The Log Strategy Reset Framework



Principle 1: Start With Investigation, Not Ingestion

Ask first:

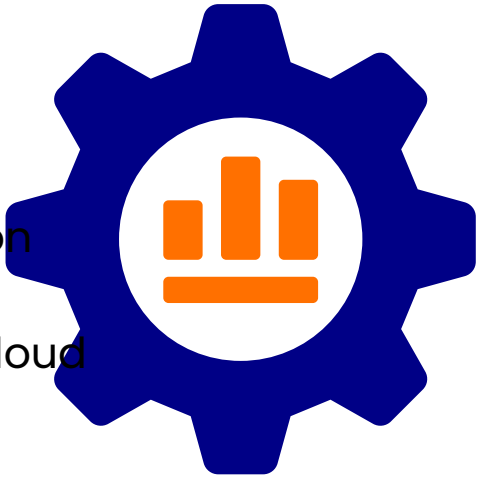
- What questions do we need to answer during an incident?
- What evidence will regulators ask for?
- What timelines matter?

Then design logging backwards from those needs.

Principle 2: Control Volume at the Source

The most expensive place to manage logs is after they hit your SIEM.

Modern strategies:

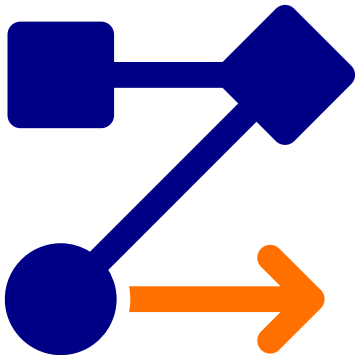


- Filter events **before ingestion**
- Apply the policy at the source of collection
- Translate and normalise early
- Drop noise at the endpoint — not in the cloud

This is where organisations using **Snare** consistently regain control — applying policy-based filtering and routing before costs spiral.

Principle 3: Route Logs With Intent

Not all logs belong in the same place.
Best-practice architectures:



- High-value security logs → SIEM
- Compliance & audit logs → Long-term archive
- Operational telemetry → Analytics platforms
- Debug / noise → Discarded or summarised

One destination does not fit all.

Principle 4: Preserve Forensic Integrity

Filtering must never mean:

- Losing timestamps
- Breaking chain-of-custody
- Altering original meaning

Your logging strategy should:

- Preserve raw evidence where required
- Ensure logs remain defensible
- Support replay and reconstruction
- Use correct timestamps on logs and NTP in the network

If logs can't stand up in an investigation or audit, they have no value.

Principle 5: Standardise Policy, Not Volume

High-performing teams standardise:

- What gets logged
- Why it's logged
- Where it goes
- How long it's retained

They do not standardise on "everything."

This is especially critical for:

- MSSPs supporting multiple customers
- Organisations operating across regions
- Hybrid and multi-cloud environments

4. The 10 Most Valuable Logs in Any Investigation

If you only reset one thing in 2026, start here:

1. **Authentication & privilege escalation events**
2. **Account creation, deletion, and modification**
3. **Process execution and command-line activity**
4. **File creation, modification, and deletion**
5. **Scheduled tasks and service changes**
6. **Policy and configuration changes**
7. **Remote access activity**
8. **Failed access attempts and anomalies**
9. **System startup, shutdown, and time changes**
10. **Log tampering or logging service interruptions**

Everything else is context — useful, but secondary.

5. A CISO's Log Strategy Reset Checklist

Use this to pressure-test your current approach:

- ☐ Can we explain why each log type is collected?
- ☐ Are we filtering before SIEM ingestion?
- ☐ Do we know our cost per log type?
- ☐ Can we reconstruct an incident 90 days later?
- ☐ Can we reconstruct an incident 6 months later?
- ☐ Can we reconstruct an incident 12 months later?
- ☐ Are logging policies consistent across endpoints?
- ☐ Can we prove logs weren't altered?

If you answered "no" to more than two — a reset is overdue.

6. MSSPs: The Reset Is a Commercial Advantage

For MSSPs, logging strategy is no longer just technical — it's competitive.

Leaders in 2025:

- Reduced SIEM infrastructure costs
- Offered predictable pricing **models**
- **Delivered faster investigations**
- **Standardised onboarding across customers**

The shift:

From "we collect everything"
To "we collect what matters — and prove why."

7. What a Modern Logging Architecture Looks Like in 2026

By 2026, leading organisations are converging on a common logging architecture — one designed for **investigation, cost control, and resilience**, not just ingestion.

At the centre of this shift is a move **upstream**.

Instead of relying on SIEM platforms to do all the heavy lifting, organisations are enforcing logging policy **at the point of collection** — where volume, fidelity, and intent can be controlled before costs escalate.

This is where platforms like **Snare** play a critical role.

Snare enables modern logging architectures by:

- **Collecting high-fidelity endpoint logs** across Windows, Linux, Unix, and macOS
- **Filtering events at the source,** before they reach expensive downstream platforms
- **Routing different log types to different destinations** based on policy and purpose
- **Preserving forensic integrity,** ensuring logs remain defensible and replayable
- **Standardising logging policies** across environments, regions, and customers

The result is an architecture that looks very different from the “send everything to SIEM” model of the past.

Key characteristics of a 2026-ready logging architecture

- Endpoint-first log collection
- Policy-driven filtering and routing
- Multiple destinations aligned to use case
- SIEMs reserved for high-value security signals
- Long-term retention without runaway storage costs

Logging designed around investigations, not alerts

This approach doesn't reduce security visibility — it **restores** it, by ensuring that the logs that arrive are the logs that matter.

Modern logging architectures aren't defined by the tools at the end of the pipeline.

They're defined by the control applied at the beginning.

That's the architectural shift 2025 made unavoidable — and the one 2026 will reward.

How Snare Enables This Architecture

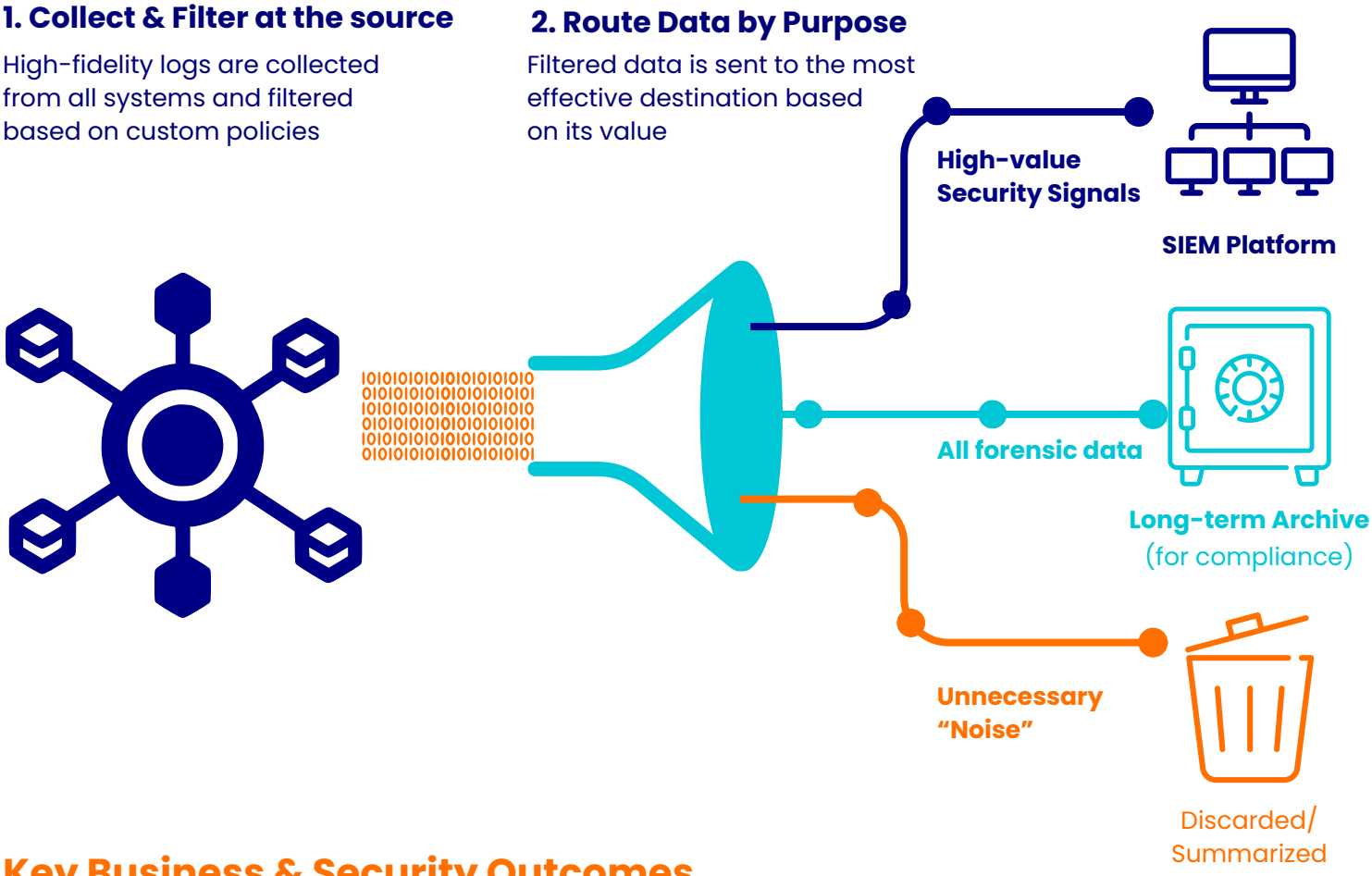
Investigation-Led Logging: A Smarter Data Flow

1. Collect & Filter at the source

High-fidelity logs are collected from all systems and filtered based on custom policies

2. Route Data by Purpose

Filtered data is sent to the most effective destination based on its value



Key Business & Security Outcomes

Faster Investigations
Analysts work with high-value security signals, not distracting noise

Predictable Costs & Reduced SIEM Pressure
Filtering data first significantly lowers expensive SIEM and storage fees

Defensible Audit Trails
Forensic integrity is preserved, ensuring data is available for compliance and audits

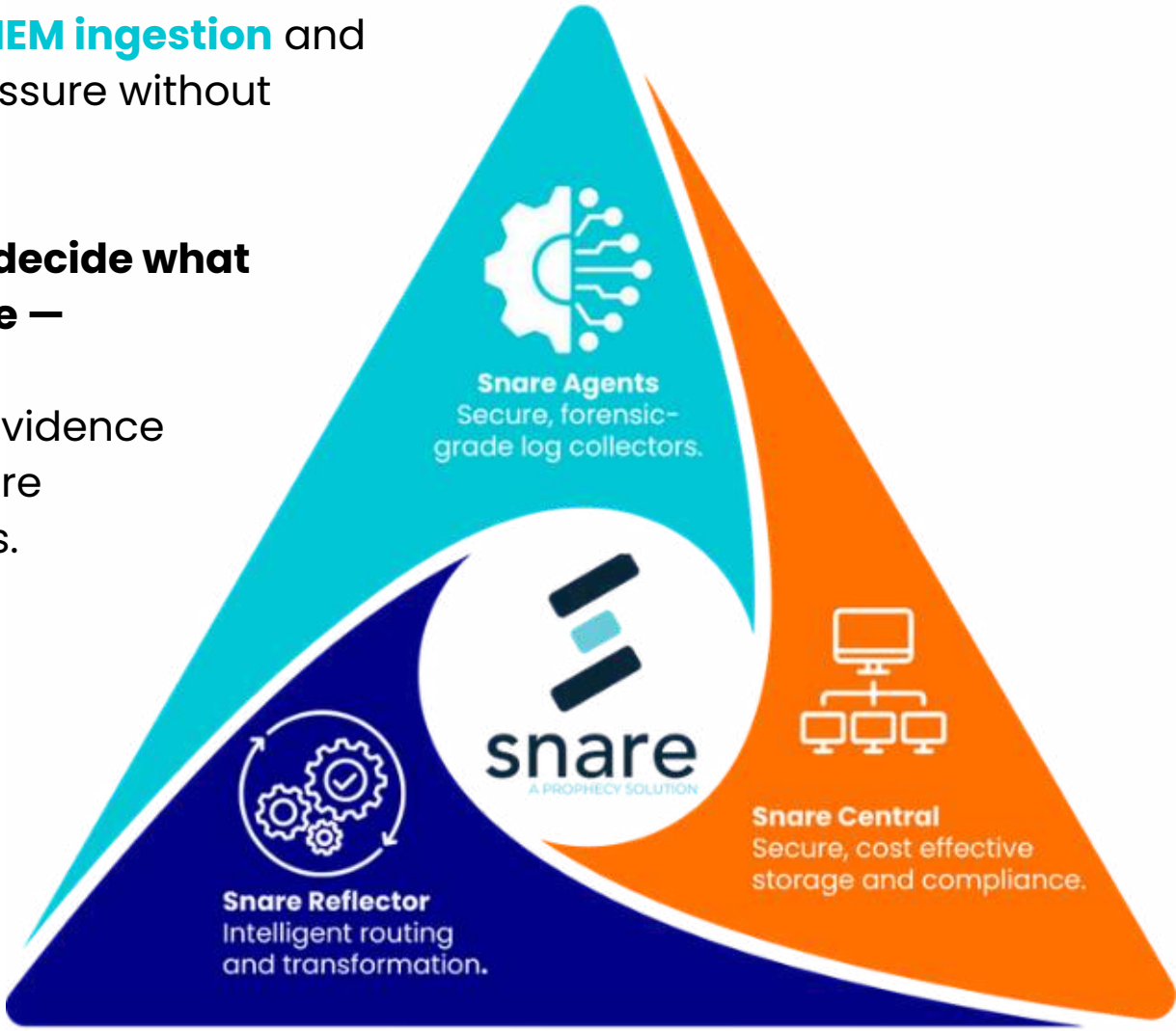
Snare acts as the control plane for enterprise logging.

Instead of forcing organisations to choose between cost and visibility, Snare enables logging strategies that scale by:

- Applying **policy-based filtering at the endpoint**
- **Routing different events to different destinations** based on purpose
- Preserving **forensic-grade logs** for investigations and compliance
- Supporting **centralised policy management** across environments
- **Reducing SIEM ingestion** and storage pressure without blind spots

Snare doesn't decide what you investigate —

It ensures the evidence you need is there when it matters.



Section 7A: What This Means for CISOs

For CISOs, modern logging architecture directly supports three board-level priorities:

Risk

- Investigation-ready evidence
- Reduced blind spots
- Stronger audit defensibility

Cost

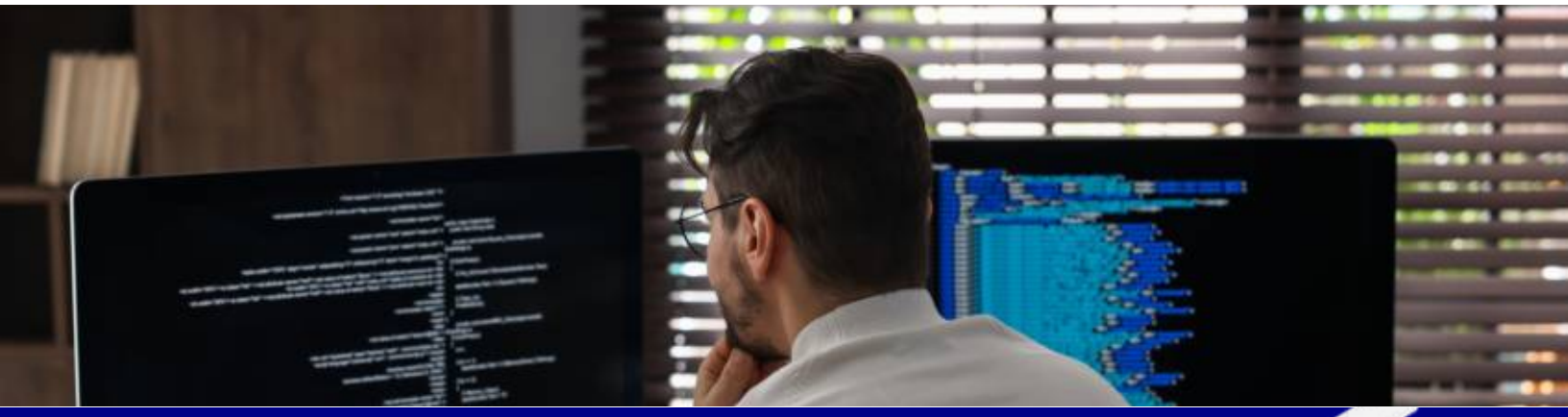
- Controlled SIEM spend
- Transparent cost drivers
- Fewer surprise overruns

Resilience

- Logging that works under pressure
- Consistency across environments
- Confidence during incidents

A 2026-ready logging strategy allows CISOs to answer:

"Yes — we can prove what happened, when it happened, and that our controls worked."



Section 7B: What This Means for MSSPs

For MSSPs, logging architecture has become a **commercial differentiator**.

Leading MSSPs are using endpoint-first logging strategies to:

- Standardise onboarding across customers
- Deliver predictable pricing models
- Reduce SIEM infrastructure costs
- Accelerate investigations
- Scale without linear cost growth

Instead of selling “all the logs,” they sell:

Clarity, speed, and confidence.

Modern MSSP logging architectures separate:

- **Security value** from **data volume**
- **Customer outcomes** from **platform cost**

That separation is what allows MSSPs to grow profitably in 2026.

Why This Matters

Modern logging architectures aren't defined by the tools at the end of the pipeline.

They're defined by:

- Where control exists
- How intent is enforced
- Whether evidence survives pressure

2025 exposed the limits of log accumulation.
2026 rewards **log strategy**.

8. Logging Shouldn’t Be the Hard Part

Security teams already operate under pressure — responding to incidents, managing risk, supporting audits, and explaining outcomes to executives and regulators. Logging should *support* that work, not complicate it.

When logging becomes difficult, it’s usually a sign that:

- Volume is unmanaged
- Cost controls are misaligned with security goals
- Policies have grown organically instead of intentionally
- Investigation requirements were never clearly defined

A strong logging strategy removes friction by design.
Well-architected logging:

- Operates quietly in the background
- Delivers consistent, trustworthy evidence
- Scales without constant tuning
- Holds up during investigations and audits
- Doesn’t surprise finance teams or security leaders

This is the outcome the **Log Strategy Reset** is designed to deliver — not fewer logs, but *less effort* required to rely on them.

When logging is done right, teams stop thinking about it — until they need it.

Take Action

Read : *A 30-Minute Log Strategy Session*

Final Thought

2025 taught us that **volume without control is risk**.

2026 is the year to reset.

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

snare
A PROPHECY SOLUTION