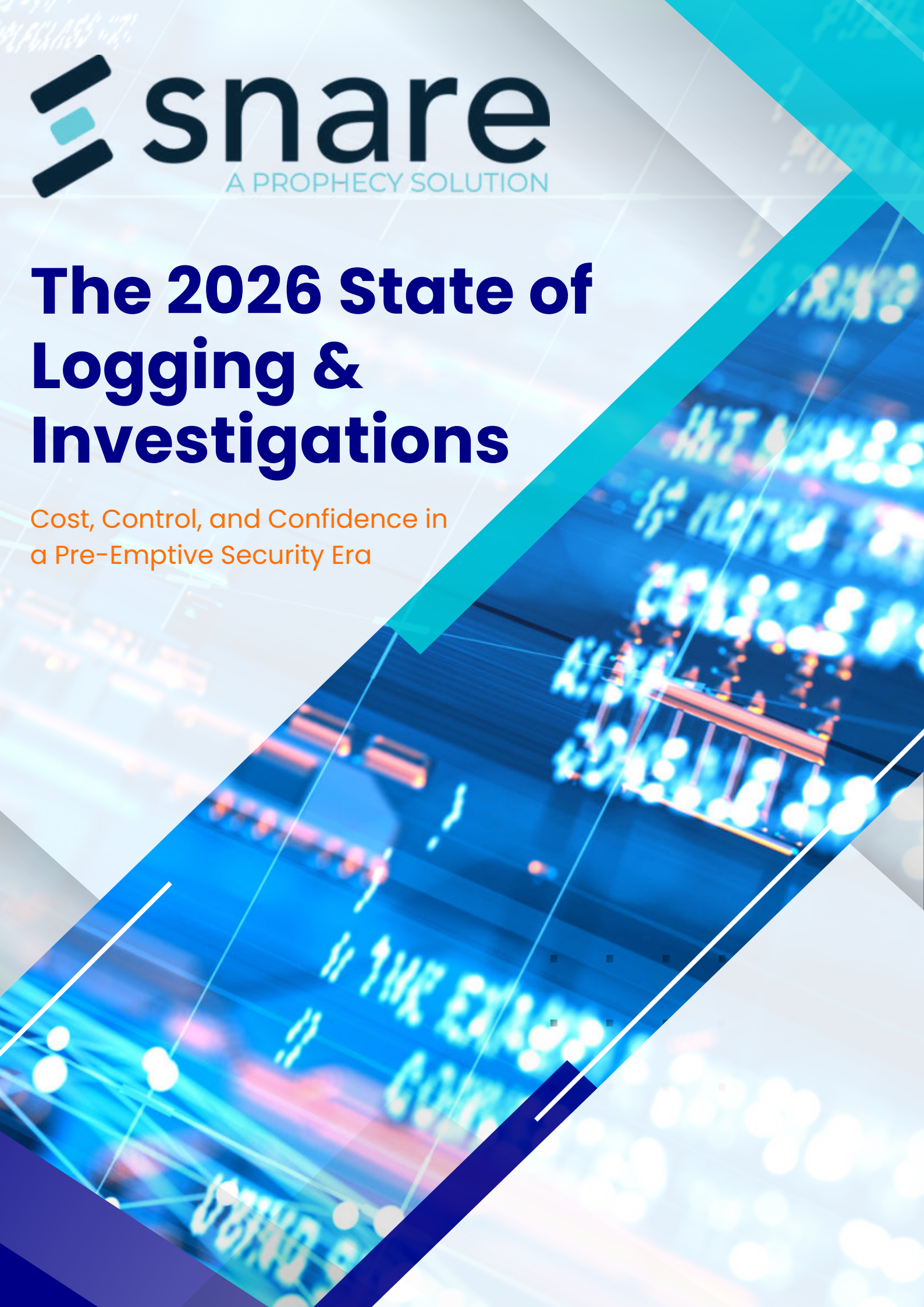
snare
A PROPHECY SOLUTION

The 2026 State of Logging & Investigations

Cost, Control, and Confidence in a Pre-Emptive Security Era



Executive Summary

As organisations enter 2026, one conclusion is broadly accepted across security leadership:

Logging has become one of the largest hidden risks in cybersecurity.

Not because logs are unimportant — but because:

- Volumes are growing faster than budgets
- SIEM cost models punish visibility
- Investigations depend on logs that are often missing, filtered, or unavailable
- AI and automation are generating more telemetry than legacy architectures can handle

Industry analysts, including **Gartner**, have consistently highlighted two converging pressures:

1. **SIEM cost inflation driven by data ingestion and retention**
2. **A strategic shift toward pre-emptive, resilience-led cybersecurity**

This report examines how these forces are reshaping logging and investigations — and where platforms like **Snare** fit into a modern, investigation-led security architecture.

1. 2025 Was the Breaking Point for Traditional SIEM Models

For over a decade, SIEM platforms sat at the centre of security operations. The model was simple:

Collect everything → store it centrally → search when needed.

By 2025, that model stopped scaling.

What changed:

- **Cloud, SaaS, and hybrid environments multiplied log sources**
- **AI systems increased machine-generated events**
- **Compliance retention periods expanded**
- **SIEM pricing models tied cost directly to ingestion and storage**

Gartner has repeatedly warned that SIEM cost growth is now **outpacing security budget growth**, forcing organisations to choose between:

- Cost control
- Investigation readiness

This is not a tooling failure — it's an architectural one.

2. Gartner's Signal: From Reactive Detection to Pre-Emptive Security

One of Gartner's most important strategic signals heading into 2026 is the move toward **pre-emptive cybersecurity.***

Rather than reacting to alerts after compromise, Gartner describes a future where organisations:

- Anticipate attack paths
- Reduce exposure before exploitation
- Design controls that limit blast radius and investigation complexity

In this model, logs are no longer just ***alerts-in-waiting*.**
They are **evidence, telemetry, and proof of control.**
Pre-emptive security requires:

- Clean, reliable signals
- High confidence in log integrity
- Reduced noise before analytics and automation are applied

This fundamentally changes how logging must be designed.

*Gartner-top-technology-trends-2026

3. The New Role of Logs: Evidence First, Alerts Second

High-performing security teams are reframing logs around three outcomes:

Logs as Evidence: A New Strategy for Security

1. Meaningful Detection

Logs should support strong signals instead of creating overwhelming alert storms

2. Rapid Investigation

Enable fast reconstruction of what happened, how it spread, and who was involved

3. Demonstrable Proof

Provide clear evidence of control effectiveness, compliance, and incident response diligence

If a log does not clearly support at least one of these outcomes, its value should be questioned.

4. Why Logging Strategy Is Now a Board-Level Issue

In 2026, logging decisions increasingly surface in:

- Breach reviews
- Regulatory inquiries
- Cyber insurance assessments
- Board and audit committee discussions

Boards are no longer asking:
“Do we have logs?”

They are asking:
“Can we prove what happened — and trust the answer?”

This elevates logging from an operational concern to a **risk, cost, and governance discipline.**

5. Where Snare Fits in the 2026 Logging Architecture

Modern organisations are recognising that the most expensive place to manage logs is **after ingestion.**

This has driven a shift toward **upstream control** — enforcing policy at the point of collection.

This is where **Snare** plays a critical architectural role.

Snare's Position in the Stack

Snare sits **between endpoints and downstream platforms,** acting as a **log control and enforcement layer.**

Snare enables organisations to:

- Collect **high-fidelity endpoint logs** across Windows, Linux, Unix, and macOS
- Apply **policy-based filtering at the source,** before SIEM costs are incurred
- **Route logs to different destinations** based on purpose (SIEM, archive, analytics)
- Preserve **forensic integrity,** timestamps, and chain-of-custody
- Standardise logging policies across environments, regions, and customers

Snare does not replace SIEM.
It ensures SIEM is fed **only the logs that matter.**

6. SIEM in 2026: Still Critical — But No Longer Central

SIEM remains essential for:

- Correlation
- Detection logic
- Response orchestration

However, its role is evolving from **data lake** to **precision analytics engine.**

Leading organisations now:

- Reserve SIEM for high-value security events
- Offload compliance and long-term retention elsewhere
- Eliminate noise before ingestion

This aligns directly with Gartner guidance around **data tiering** and **cost-aligned telemetry strategies.**

7. Investigation Readiness Is the New Benchmark

Security maturity in 2026 is increasingly measured by:

- Time to investigation
- Confidence in findings
- Ability to replay events accurately

Teams with upstream log control consistently demonstrate:

- Faster root-cause analysis
- Lower investigation costs
- Stronger audit outcomes

This is not about collecting fewer logs —
It's about collecting **the right logs, consistently.**

8. What This Means for CISOs

CISOs entering 2026 should expect to be accountable for:

- Logging cost governance
- Investigation readiness
- Evidence defensibility

Key actions:

- Define logging strategy around investigations, not ingestion
- Implement endpoint-level policy enforcement
- Separate security value from data volume
- Ensure logging decisions can be explained at board level

9. What This Means for MSSPs

For MSSPs, logging strategy is now a **commercial differentiator**.
Mature providers are using platforms like Snare to:

- Standardise customer logging baselines
- Offer predictable pricing
- Reduce SIEM infrastructure overhead
- Deliver faster, higher-confidence investigations

The market is shifting from:

"We ingest everything"
to
"We prove what matters."

10. The 2026 Outlook

Looking ahead, three trends are clear:

1. The rise in **AI applications will increase log volume — not reduce it**
2. **Regulators will demand stronger evidence, not more alerts**
3. **Cost-blind logging architectures will continue to fail**

The winners in 2026 will be organisations that treat logging as:

- A strategic control
- An investigation enabler
- A cost-governed discipline

Conclusion

The state of logging and investigations in 2026 is defined by **intentional design.**

SIEM remains important — but control must move upstream.
Evidence must be preserved.
Costs must be predictable.

Platforms like Snare exist to make that balance possible.

Because in modern security, confidence doesn't come from how much you log — it comes from knowing you logged the right things.

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