snare
A PROPHECY SOLUTION

MSSP Architecture Briefing

Building a Scalable, Cost-Effective and Investigation-Ready Logging Architecture

Powered by Snare, AskSnare and ProDataIQ

Executive Summary

Managed Security Service Providers (MSSPs) face a difficult balancing act.

Customers demand comprehensive visibility, long-term retention, rapid investigations, regulatory compliance, and 24x7 monitoring.

At the same time, MSSPs must control infrastructure costs, SIEM ingestion expenses, operational overhead, and analyst workloads.

The challenge is no longer collecting logs.

The challenge is collecting the right logs, retaining them cost-effectively, and turning them into actionable intelligence.

This briefing outlines a modern MSSP logging architecture that supports:

- Multi-tenant operations
- Investigation readiness
- Long-term retention
- SIEM optimisation
- Regulatory compliance
- AI-assisted investigations
- Scalable service delivery

The MSSP Logging Challenge

Modern MSSPs typically manage:

- Multiple customers
- Multiple SIEM platforms
- Cloud and on-premises environments
- Regulatory obligations
- Large-scale log volumes
- Increasing analyst workloads

Common challenges include:

Rising SIEM Costs

Many MSSPs are seeing ingestion costs increase faster than service revenue.

Fragmented Data Sources

Logs arrive from:

- Windows
- Linux
- Cloud platforms
- SaaS applications
- Network devices
- Security products

Long-Term Retention Requirements

Customers increasingly require:

- 12 months
- 3 years
- 7 years

of retained security data.

Investigation Complexity

Analysts spend excessive time locating and correlating relevant evidence.

Reference MSSP Architecture

Layer 1: Log Collection

Snare Agent

Collects forensic-grade telemetry from:

- Windows Servers
- Linux Servers
- Workstations
- Critical Infrastructure
- Cloud Workloads

Benefits:

✔️ Forensic-level audit logging
✔️ Reduced network overhead
✔️ Secure transmission
✔️ Centralised policy management

Layer 2: Log Management

Snare Central

Acts as the operational logging hub.

Functions include:

- Collection
- Aggregation
- Normalisation
- Routing
- Retention
- Replay

Benefits:

✔️ Centralised visibility
✔️ Vendor independence
✔️ Reduced operational complexity
✔️ Investigation-ready evidence

Layer 3: Multi-Destination Delivery

Snare Reflector

Routes data to:

- Microsoft Sentinel
- Splunk
- Google SecOps
- Securonix
- Elastic
- QRadar
- Devo

Benefits:

✔️ Vendor flexibility
✔️ Multi-tenant routing
✔️ SIEM optimisation
✔️ Reduced lock-in

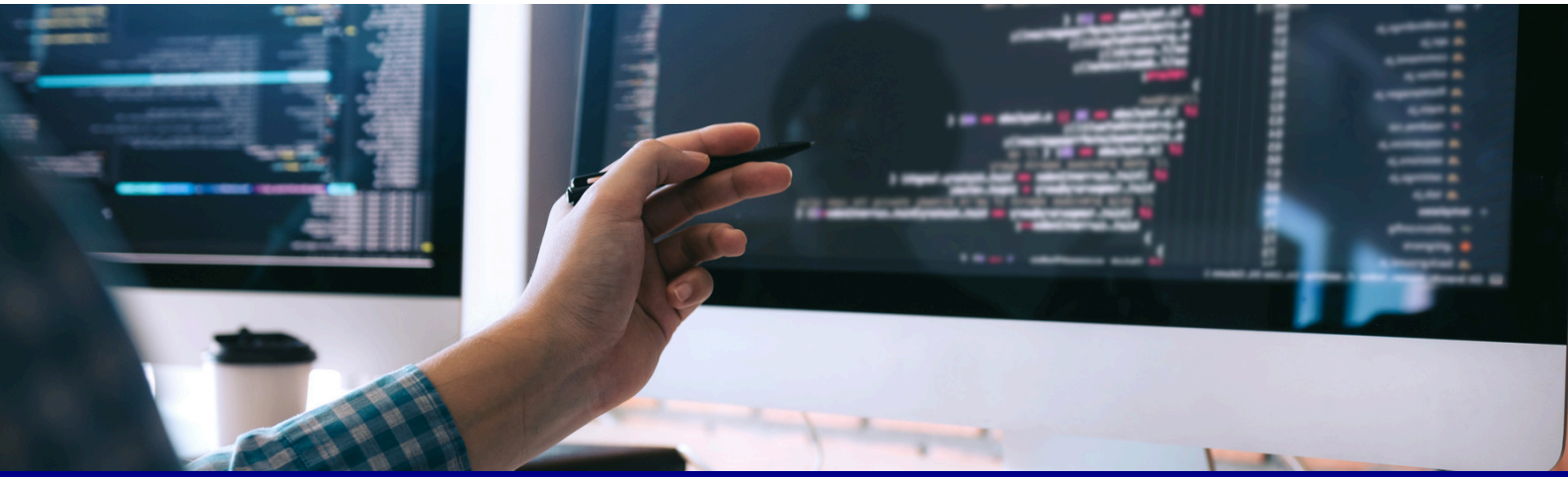
Layer 4: Long-Term Retention

SnareStore

Retains evidence while reducing storage costs.

Benefits:

✔️ Up to 90% storage reduction
✔️ Investigation readiness
✔️ Compliance support
✔️ Replay capabilities



snare
A PROPHECY SOLUTION

Layer 5: AI-Assisted Investigation

AskSnare

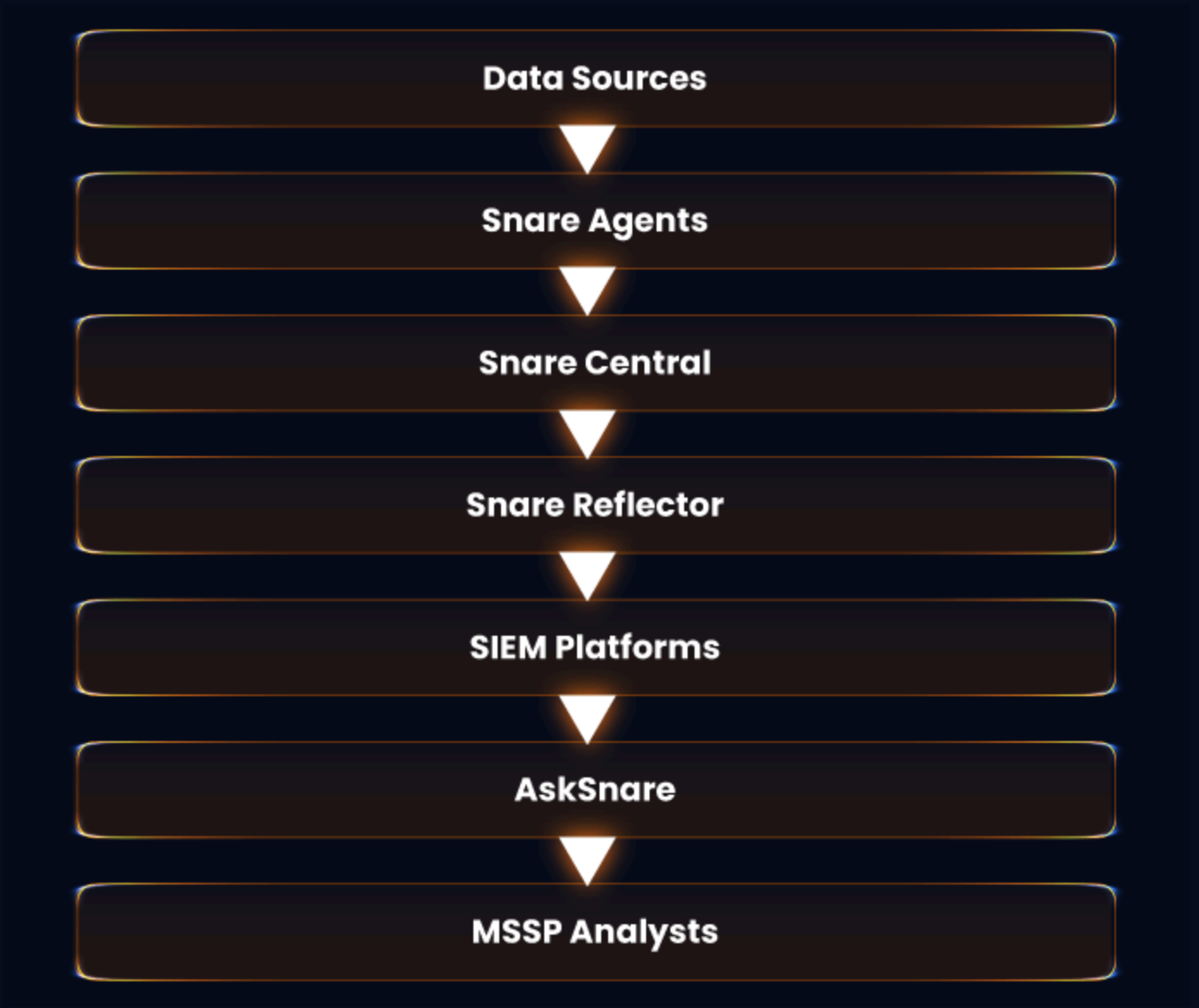
Provides natural language investigation capability.

Examples:

"What systems stopped logging?"
"What changed before this incident?"
"Show unusual authentication activity."

Benefits:

- ✔ Faster investigations
- ✔ Reduced analyst workload
- ✔ Improved customer response times
- ✔ Contextual understanding



Reference MSSP Architecture

Managed Detection & Response (MDR)

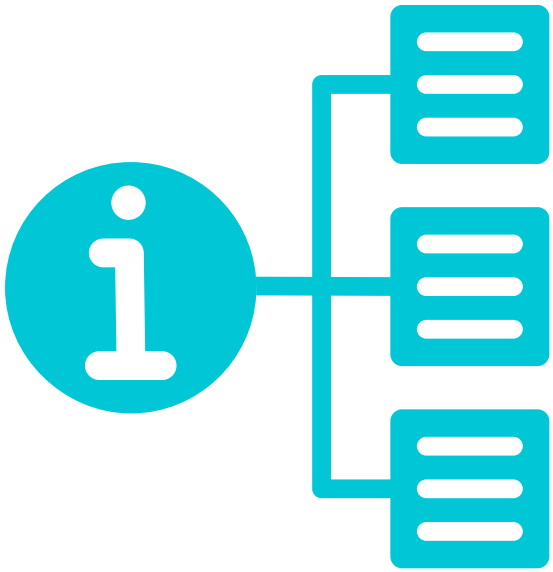
Requirements:

- High-quality telemetry
- Investigation capability
- Fast search

Snare Contribution:

✔️ Forensic-grade visibility
✔️ Centralised telemetry
✔️ Investigation-ready evidence

Compliance Monitoring

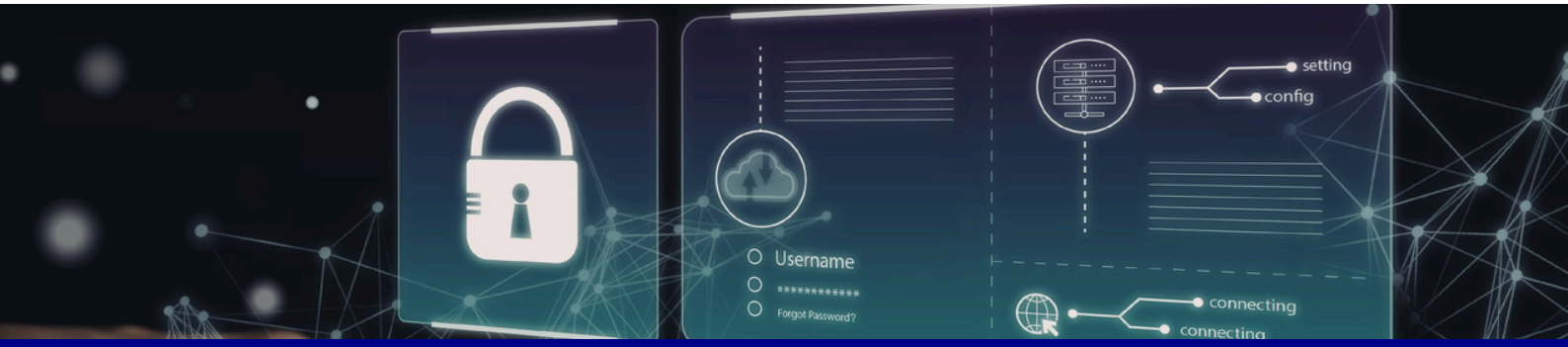


Requirements:

- Audit trails
- Long-term retention
- Evidence preservation

Snare Contribution:

✔️ Retention
✔️ Replay
✔️ Audit support



snare
A PROPHECY SOLUTION

Threat Hunting

Requirements:

- Historical visibility
- Large datasets
- Fast access

Snare Contribution:

✔️ Long-term telemetry retention
✔️ Event replay
✔️ Cross-platform visibility

Incident Response

Requirements:

- Rapid evidence collection
- Event reconstruction
- Timeline analysis

Snare Contribution:

✔️ Detailed forensic telemetry
✔️ Investigation-ready logs
✔️ AskSnare contextual insights

The Economics of MSSP Logging

Traditional architecture often results in:

- Excessive SIEM ingestion costs
- Duplicate storage
- Data loss due to retention constraints
- Limited historical visibility

A Snare-centric architecture enables:

Reduce SIEM Costs

Filter and optimise before ingestion.

Improve Retention

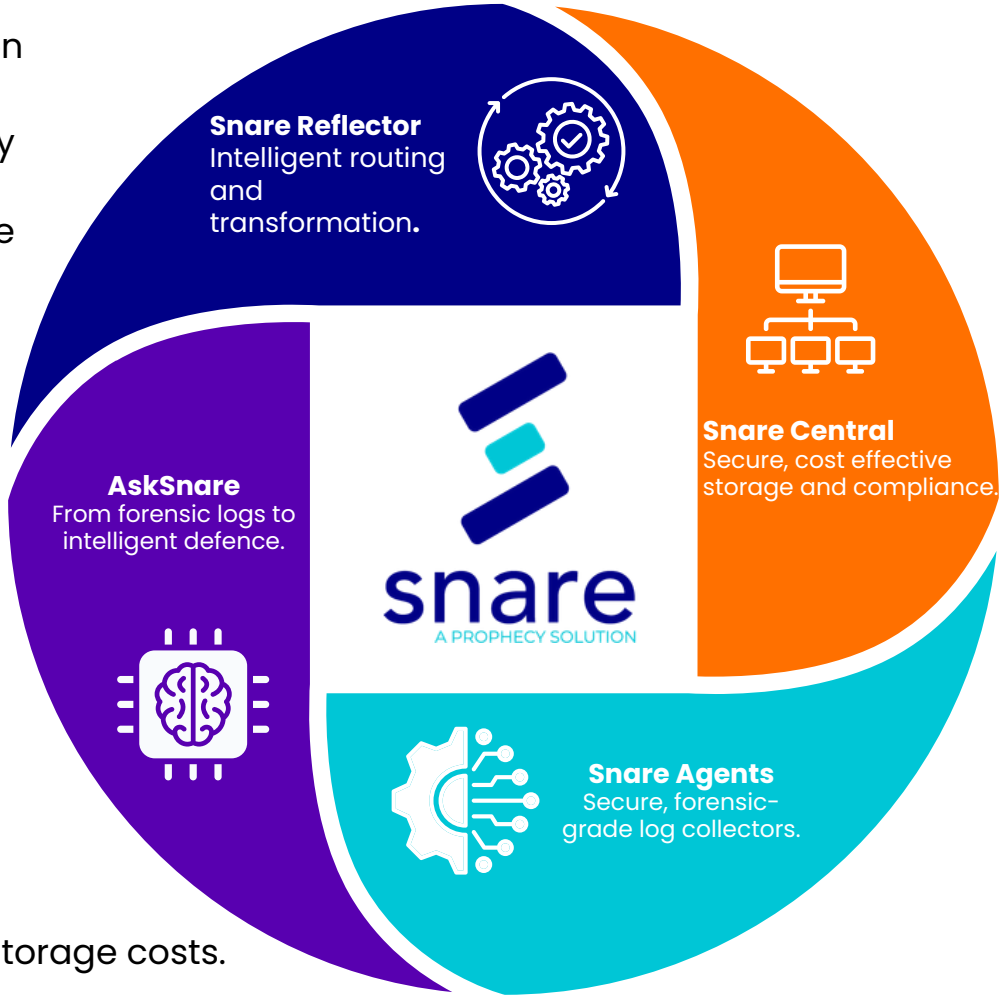
Retain years of data economically.

Increase Service Margins

Reduce infrastructure and storage costs.

Improve Investigation Outcomes

Provide analysts with better evidence and faster access.



AI and the Future of MSSP Operations

AI is rapidly changing how security services are delivered.

However, AI is only as effective as the telemetry supporting it.
MSSPs require:

- Trusted data
- Complete audit trails
- Historical visibility
- Investigation-ready evidence

This is where Snare and AskSnare become critical.

Snare provides the telemetry foundation.

AskSnare provides the intelligence layer.

Together they help MSSPs deliver:

- Faster investigations
- Improved customer outcomes
- Greater operational efficiency
- Enhanced service differentiation

snare
A PROPHECY SOLUTION

Recommended Next Steps

Building a modern MSSP logging architecture is not simply about deploying another logging tool. It is about creating a scalable telemetry foundation that supports profitable service delivery, rapid investigations, regulatory requirements, and future AI-driven operations.

Whether you are launching a new security service, modernising an existing SOC, or looking to improve margins, the following roadmap can help guide your next steps.

---

1. Assess Your Current Telemetry Architecture

Before introducing new technologies or services, understand the current state of your logging environment.

Review:

- Data sources currently being monitored
- Collection methods and coverage gaps
- SIEM ingestion volumes
- Retention periods
- Customer-specific logging requirements
- Investigation workflows
- Multi-tenant architecture design

Ask yourself:

- Are we collecting the right data?
- Are there critical blind spots?
- Can we quickly identify when telemetry stops flowing?
- Are we retaining enough data to support investigations?

Desired Outcome
A clear understanding of where visibility gaps, operational inefficiencies, and cost pressures exist.

2. Review SIEM Cost Drivers and Optimisation Opportunities

For many MSSPs, SIEM licensing and ingestion costs represent one of the largest operational expenses.

Assess:

- Duplicate data ingestion
- High-volume low-value event types
- Retention costs
- Multi-SIEM duplication
- Customer-specific data requirements

Identify opportunities to:

- Filter before ingestion
- Aggregate repetitive events
- Route only relevant data
- Retain data outside expensive SIEM storage

Desired Outcome
Lower operating costs without sacrificing visibility or investigation readiness.

3. Build a Tiered Telemetry Strategy

Not all data requires the same treatment. Classify telemetry into tiers:

Tier 1 – Critical Investigation Data

Examples:

- Authentication activity
- Privileged access
- Security alerts
- Configuration changes
- Endpoint telemetry

Recommended:
Immediate SIEM ingestion and long-term retention.

Tier 2 – Operational Visibility

Examples:

- Application activity
- Infrastructure logs
- System health

Recommended:
Selective ingestion and retained access.

Tier 3 – Historical Evidence

Examples:

- Archived security telemetry
- Compliance records
- Legacy investigation data

Recommended:
Low-cost retention with replay capability.

Desired Outcome
Desired Outcome
Lower operating costs without sacrificing visibility or investigation readiness.

4. Strengthen Investigation Readiness

Many MSSPs focus heavily on detection but discover during an incident that historical evidence is difficult to access.

Evaluate:

- Historical search capabilities
- Evidence retention
- Investigation workflows
- Event replay capabilities
- Audit reporting

Test your ability to answer:

- What happened?
- When did it happen?
- Who was involved?
- What changed?
- Can we prove it?

Desired Outcome
Faster investigations and improved customer confidence during incidents.

5. Standardise Multi-Tenant Operations

As MSSPs scale, operational consistency becomes critical.
Establish standards for:

- Collection policies
- Retention policies
- Customer onboarding
- Routing rules
- Compliance reporting
- Investigation procedures

Ensure each customer environment can be managed consistently without introducing unnecessary complexity.

Desired Outcome
Improved operational efficiency and reduced service delivery overhead.

6. Introduce AI-Assisted Investigation Workflows

Security operations centres are increasingly challenged by alert volume, staffing shortages, and investigation complexity.

Begin identifying opportunities where AI can assist with:

- Log analysis
- Event correlation
- Timeline reconstruction
- Threat investigation
- Context generation
- Governance reporting

However, AI is only effective when supported by trusted telemetry.
Ensure your logging architecture provides:

- Accurate data
- Complete audit trails
- Historical visibility
- Investigation-ready evidence

Desired Outcome
Reduced analyst workload and faster access to meaningful insights.

7. Position Logging as a Strategic MSSP Service

Many MSSPs still treat logging as a supporting capability.

Leading MSSPs are increasingly packaging logging as a standalone service offering that delivers:

- Compliance support
- Long-term retention
- Investigation readiness
- Threat hunting
- Security operations enablement
- AI governance readiness

This creates opportunities for:

- New recurring revenue streams
- Improved customer retention
- Service differentiation
- Expanded consulting engagements

Desired Outcome
Transform logging from a cost centre into a strategic revenue-generating service.

8. Build Toward an AI-Ready Security Operations Model

The future MSSP will combine:

- Trusted telemetry
- Centralised visibility
- Investigation readiness
- AI-assisted analysis
- Human expertise

This is where the combination of Snare, AskSnare, and ProDataIQ delivers long-term value.

Snare provides the forensic-grade telemetry foundation.

AskSnare accelerates investigation and understanding.

ProDataIQ provides the intelligence layer that helps turn evidence into actionable security insights.

Desired Outcome
A scalable, future-ready security operations platform capable of supporting the next generation of managed security services

MSSP Action Plan

Next 30 Days

✔️ Assess telemetry coverage
✔️ Review SIEM costs
✔️ Identify retention gaps
✔️ Evaluate investigation workflows

MSSP Action Plan

Next 30 Days
- ✔ Assess telemetry coverage
- ✔ Review SIEM costs
- ✔ Identify retention gaps
- ✔ Evaluate investigation workflows

Next 90 Days
- ✔ Implement optimisation opportunities
- ✔ Standardise collection policies
- ✔ Improve retention strategy
- ✔ Introduce replay and investigation capabilities

Next 12 Months
- ✔ Mature multi-tenant operations
- ✔ Expand threat hunting services
- ✔ Introduce AI-assisted investigations
- ✔ Develop differentiated managed logging services
- ✔ Build an AI-ready SOC

The most successful MSSPs will be those that treat telemetry as a strategic asset rather than a by-product of security operations.

The path to scalable, profitable, and AI-enabled security services begins with trusted telemetry.

Key Takeaway

The security industry is entering a new phase.

For years, MSSPs have focused on collecting more data, ingesting more logs, and deploying more detection content. However, increasing telemetry volumes, rising SIEM costs, and growing customer expectations have exposed a fundamental challenge:

More data does not automatically create better security outcomes.

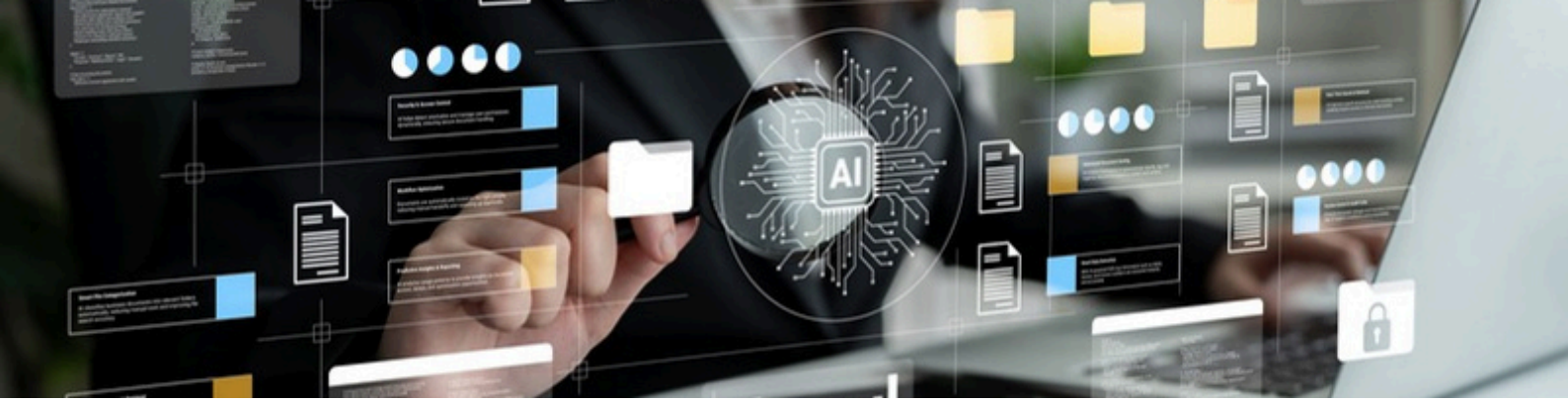
The MSSPs that will lead the next generation of managed security services will not be those with the largest data lakes or the highest ingestion volumes.

They will be the organisations that can efficiently collect, retain, route, investigate, and operationalise security telemetry at scale.

This requires an architecture that can:

- Collect forensic-grade telemetry at the source
- Maintain data integrity throughout the pipeline
- Support multi-tenant service delivery
- Reduce unnecessary SIEM ingestion costs
- Preserve long-term investigative evidence
- Accelerate incident response and threat hunting
- Enable AI-assisted investigations without sacrificing accuracy or context

As security operations evolve, telemetry is becoming more than a data source. It is becoming the foundation upon which detection, investigation, compliance, threat hunting, AI-assisted operations, and customer trust are built.



The challenge for MSSPs is no longer simply answering:

"Did we collect the logs?"

The more important questions are:

Can we trust the data?

Can we reconstruct the event?

Can we investigate at speed?

Can we retain evidence economically?

Can we scale operations without scaling costs at the same rate?

A modern MSSP architecture must balance visibility, performance, retention, and operational efficiency while preparing for a future where AI becomes a core component of security operations.

This is where Snare, AskSnare, and ProDataIQ work together.

Snare provides the telemetry foundation.

AskSnare accelerates investigation and contextual understanding.

ProDataIQ introduces intelligent analysis that helps transform security data into operational insight.

Together, they help MSSPs move beyond log management and toward a model where telemetry becomes a strategic operational asset.

The future SOC will not be defined by the amount of data it collects.

It will be defined by how effectively it can turn telemetry into evidence, evidence into intelligence, and intelligence into action.

Final Thought

The most valuable security data is not the data you collect.

It is the data you can trust, investigate, and operationalise when it matters most.

That is the foundation of a modern MSSP architecture.

Architecture Principle #1

Collect once.
Route intelligently.
Retain economically.
Investigate rapidly.

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

snare
A PROPHECY SOLUTION