snare
A PROPHECY SOLUTION

A SNARE SOLUTIONS PLAYBOOK

The Intelligent Log Management Playbook

From forensic-level collection to AI-assisted investigation: how to build a security evidence architecture that improves visibility, right-sizes SIEM costs and keeps critical evidence available for as long as an investigation needs it.

EXECUTIVE SUMMARY

From more telemetry to evidence you can trust

Security teams have access to more telemetry than ever, from endpoints, servers, identity systems, cloud platforms, applications, network infrastructure and security controls. The opportunity is to turn that telemetry into usable evidence: collected deliberately, protected from tampering and available the moment an investigation needs it.

That means deciding what evidence must be collected, how it is protected, what deserves premium analytics processing, what must be retained independently, and how analysts can interrogate it quickly during an incident.

Time makes those decisions urgent. IBM's *Cost of a Data Breach Report 2026* puts the average breach lifecycle at **247 days**, and breaches that run past 200 days cost more. Gartner describes log management as an important but undervalued tool for threat detection, investigation and response. Forrester argues for data pipeline management that reduces, routes and manages telemetry before it reaches high-cost analytics platforms.

This playbook treats logging as a security evidence discipline, not a transport mechanism. It shows how a resilient collection, retention, routing and investigation layer can support the SIEM investments you already have, right-size ingestion, preserve historical evidence and give AI-assisted investigation a stronger foundation.

> **The question is no longer "How do we collect more logs?" It is "How do we build a security evidence architecture we can trust, for as long as an investigation needs it?"**

Inside this playbook

Section	Topic	Covers
01–02	**Foundations**	Why logs are evidence, and how the security data problem has changed
03–05	**The evidence chain**	Eight links from event to action, five decisions before technology, and why time changes the plan
06–07	**Architecture**	Four deployment pathways and where Snare fits
08	**Use cases**	Ten security scenarios, from compromised credentials to missing telemetry
09	**AI-assisted investigation**	AskSnare, and why AI still depends on evidence
10–12	**Economics and maturity**	Data tiers, the maturity model and an architecture checklist
13–15	**Next steps**	Independent guidance, bringing it together and assessing your architecture

01 · SECURITY STARTS WITH THE EVIDENCE

Investigations are only as complete as the evidence behind them

When an incident occurs, security teams reconstruct what happened from evidence spread across operating systems, identity platforms, infrastructure, applications and security controls:

- Authentication and logon events
- Privilege and group membership changes
- Configuration and policy changes
- Application and cloud control-plane events
- Endpoint and process activity
- Network connections and remote services
- Administrative activity
- Security-control events and alerts

NIST defines a log as a record of the events occurring within an organisation's computing assets, and log management as the process of generating, transmitting, storing, accessing and disposing of log data. It ties log management directly to investigating cybersecurity incidents and keeping records for the required period.

> **Logs are not simply machine data. In an investigation, they are evidence.**

Reference: NIST SP 800-92 Rev. 1 (initial public draft), Cybersecurity Log Management Planning Guide.

02 · THE MODERN SECURITY DATA PROBLEM

More sources, more volume, more choices to make

Cloud adoption, SaaS, hybrid work, distributed infrastructure and expanding security tooling have increased both the number of sources and the volume of events security teams manage.

Endpoint & identity	Cloud & applications	Network & security
Windows, Linux, macOS and Unix; authentication, directory and privilege events	Control-plane operations, SaaS, APIs, databases and business systems	Firewalls, DNS, proxies, EDR/XDR, vulnerability and other security controls

The challenge has moved beyond collection. It is now about balancing visibility, cost, retention, performance and portability. Joint guidance from ASD's ACSC and international partners recommends considering filtering before logs reach SIEM or XDR platforms, so those platforms receive the most valuable data while cost and capacity pressure stay manageable.

Reference: ASD's ACSC and partners, Best practices for event logging and threat detection (22 August 2024).

Eight links from event to action

Every investigation relies on an unbroken chain. Each link is a design decision, and each maps to a specific part of the Snare architecture.

1 Collect

Capture the security-relevant activity needed to detect, investigate and reconstruct events.

Snare: Snare Agent on Windows, Linux, macOS and Unix, including Event Tracing for Windows; syslog, NetFlow and cloud audit sources direct to Snare Central

2 Protect

Reduce the risk that an attacker can erase, alter or suppress the only copy of critical evidence.

Snare: TLS 1.2/1.3 with mutual TLS, an encrypted local agent buffer, off-host retention and hash verification on archive ingestion and retrieval

3 Normalise

Represent events consistently for downstream search, correlation and analytics.

Snare: Snare Central brings sources into one pipeline; Reflector remaps fields to Splunk CIM or Microsoft Sentinel ASIM

4 Optimise

Aggregate, de-duplicate or transform telemetry by security and economic value.

Snare: Central aggregation keeps original event detail in metadata; Reflector de-duplication and truncation apply to what is forwarded

5 Route

Send the right data to the right SIEM, archive, MSSP or analytics destination.

Snare: Snare Reflector, with per-destination rules, formats and independent queues

6 Retain

Keep historical evidence for as long as risk, regulation and policy require.

Snare: Snare Central retention from 90 days to 7+ years on local, NAS, SAN or S3-compatible storage

7 Investigate

Make evidence searchable for incident response, threat hunting and forensics.

Snare: Central search, 600+ pre-built compliance reports, Event Replay and AskSnare

8 Act

Contain, remediate, escalate, tune controls or strengthen future detections.

Snare: Your SIEM, SOC and response tooling, fed with the evidence they need

A chain is only as strong as its weakest link. Detection depends on collection; investigation depends on retention; response depends on both. Designing the chain end to end means a gap at one stage does not quietly undermine every stage after it.

Decide what the evidence must do, then design for it

Settling these five decisions first keeps every technology choice that follows anchored to security outcomes.

1	**What must we collect?** Start with the threats, assets and investigations that matter, then map those outcomes to the telemetry required to observe them.	**With Snare:** Agent policies set what is captured at each source, consistently across Windows, Linux, macOS and Unix.
2	**What must enter the SIEM?** Separate evidence that must be collected from evidence that needs continuous premium analytics processing.	**With Snare:** Reflector sends each destination only the events its detections use. Filtering shapes what is forwarded, never what is retained.
3	**What must we retain?** Define retention by investigation window, regulation, business risk and forensic need, not only by SIEM storage cost.	**With Snare:** Central retains the full record independently of the SIEM, for 90 days to 7+ years.
4	**Where can the data reside?** Account for on-premises, cloud, hybrid, sovereign, isolated and restricted environments.	**With Snare:** Four deployment pathways, including fully on-premises and separated zones.
5	**How will we investigate?** Decide how SIEM search, retained logs, threat hunting and AI-assisted investigation work together.	**With Snare:** Central search, Event Replay and AskSnare complement the SIEM.

Design collection around detection and investigation goals. MITRE ATT&CK v18 introduced detection strategies that connect adversary techniques to observable telemetry through data components such as Logon Session Creation (DC0067). They are a practical starting point for the first decision: which evidence each technique needs.

Reference: MITRE ATT&CK, Detection Strategies and Data Components.

Your evidence has to outlast the breach

Retention decisions are usually made around storage cost. They should be made around how long an investigation actually takes to begin.

183
days, on average, to identify a breach

247
days, on average, to identify and contain it, up from 241 a year earlier

12%
increase in average cost, to USD 5.65 million, for breaches lasting more than 200 days

By the time a typical breach is contained, the activity that started it is eight months old. Breaches resolved in under 200 days averaged USD 4.32 million, so lifecycle length is a cost driver as well as an investigation problem.

What that means for each decision

Moment	Evidence the investigation needs
Day 0: initial access	Authentication, remote access, edge-device and identity events from the first foothold
Day 183: identification	Six months of endpoint, server, privilege, SaaS and cloud activity, much of it never alerted on
Day 247: containment	The full timeline from first access to response, with proof the historical record is unaltered

> **The planning rule:** retention for investigation evidence should comfortably exceed your realistic breach lifecycle, not your SIEM's hot-storage window. Joint guidance from ASD's ACSC, CISA and partners recommends retaining administrative and security event logs for at least a year, and PCI DSS v4.0.1 requirement 10.5.1 requires 12 months, with the latest three months immediately available.

Reference: IBM, Cost of a Data Breach Report 2026 (research conducted by Ponemon Institute), p. 15, Figure 5 and p. 30, Figure 17; ASD's ACSC, CISA et al., Implementing SIEM and SOAR Platforms (May 2025); PCI DSS v4.0.1.

Choice is part of the architecture

There is no single correct deployment model. Some teams need complete on-premises control; others run hybrid estates or want to add AI-assisted investigation. Every Snare pathway is built from the same Snare Agent, Snare Central and Snare Reflector, so you can start where you are and evolve.

PATHWAY 1

Fully on-premises

Environments that need local collection, management and retention, with no dependency on cloud or AI.

- Snare Agent, syslog and NetFlow into Snare Central
- Archive retained inside your network
- Reflector routes to on-premises or cloud SIEMs

PATHWAY 2

On-premises + AskSnare

Teams that keep collection and retention on-premises and add AI-assisted investigation.

- Everything in pathway 1
- The evidence layer feeds selected security data to AskSnare
- Natural-language questions over retained evidence

PATHWAY 3

Unified on-premises + cloud

Mixed estates that need one collection and retention layer across on-premises and cloud.

- Adds Microsoft 365, Azure, AWS and Oracle Cloud sources
- One retention and routing policy across both
- The widest context for AskSnare

PATHWAY 4

Hybrid / separated

Organisations that must keep protected zones isolated while modernising elsewhere.

- Separate Snare Central instances per zone
- Protected logs never leave their zone
- The connected zone can add cloud sources and AskSnare

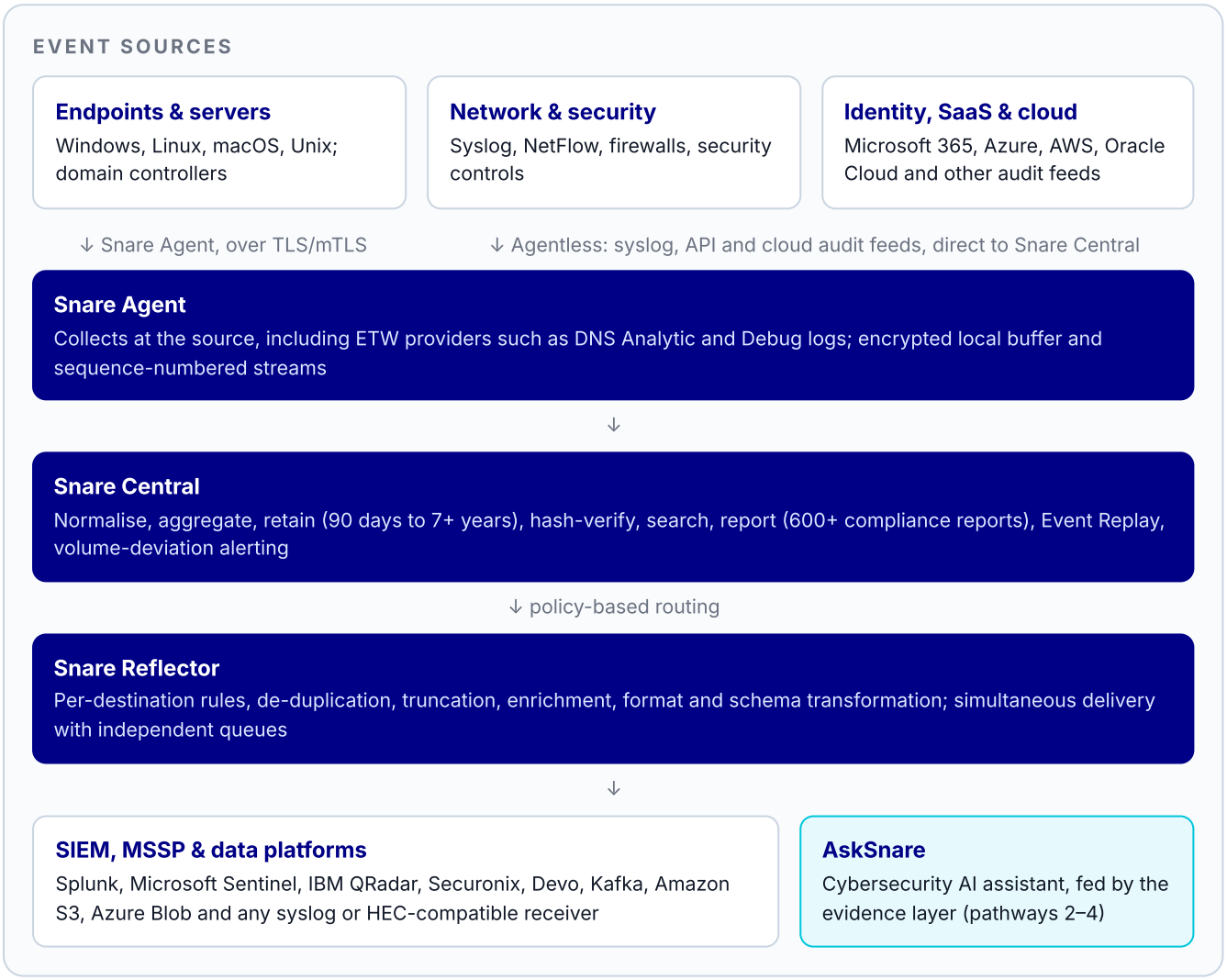
Keep data where it needs to live, and add capabilities where they create value.

The on-premises pathway remains a complete security architecture. Cloud and AI are additional options, not prerequisites for strengthening logging and evidence management. Customers can move between pathways as requirements change, without replacing collection.

07 · WHERE SNARE FITS

An evidence layer between your sources and your analytics

Snare sits between event sources and downstream platforms, separating the collection and evidence layer from whichever analytics destination you use today.



Snare Agent	Snare Central	Snare Reflector	AskSnare
Collects security telemetry at the source	Management, policy, retention and investigation	Routes the right data to each destination	AI-assisted investigation over security evidence

Snare complements the SIEM. It makes the security data feeding it more controllable, portable and investigation-ready.

Ten use cases, mapped to the evidence lifecycle

Each use case that follows covers the security challenge, the evidence required, how the Snare architecture supports it, example questions to ask of the evidence, and the resulting operational value.

#	Use case
01	Compromised credentials and abnormal authentication
02	Insider threat and unusual user behaviour
03	Privilege escalation and privileged account abuse
04	Lateral movement across the environment
05	Ransomware and post-compromise investigation
06	Proactive threat hunting across historical logs
07	Compliance, audit and forensic evidence
08	Right-sizing SIEM ingestion and storage costs
09	Changing SIEM without rebuilding log collection
10	Finding gaps in visibility and missing telemetry

Collect
Snare Agent and agentless sources

Retain and optimise
Snare Central archive and aggregation

Route
Snare Reflector

Investigate
Central search, reports, Event Replay

AI assist
AskSnare (pathways 2–4)

Act
Your SIEM, SOC and response tooling

Read the use cases as a set. Most investigations touch several at once. A credential compromise becomes lateral movement, which becomes a ransomware investigation. The same evidence layer supports all of them, which is why it pays to design it once and well.

01 Compromised credentials and abnormal authentication

Valid credentials make malicious activity look legitimate. The challenge is recognising authentication that is unusual for the account, system, location or surrounding activity, and linking it to what happened next.

EVIDENCE REQUIRED

- Authentication successes and failures (4624, 4625, 4648)
- Account and group changes
- Privileged logons (4672)
- Process creation and command lines (4688)
- Identity provider sign-ins

HOW SNARE SUPPORTS IT

Snare Agent captures Windows, Linux and macOS security events at the source, and identity audit sources feed Snare Central directly. Central retains them off-host and makes them searchable. Reflector routes the detection-relevant subset to the SIEM, and AskSnare lets analysts interrogate the evidence without starting every investigation with a complex query.

ASK THE EVIDENCE

"Show failed logins followed by a successful privileged login for the same account in the last 24 hours."

"Which accounts accessed systems they have not used before?"

"Build a timeline for this account across the affected systems."

Faster validation of suspected compromise	**Authentication correlated with endpoint behaviour**	**Clearer reconstruction after access**

Reference: MITRE ATT&CK, Logon Session Creation (DC0067)

02 Insider threat and unusual user behaviour

Insiders already have authorised access, so a single event is rarely suspicious on its own. Investigations depend on changes in behaviour and on activity that differs from a user's role or history.

EVIDENCE REQUIRED

- Authentication and sessions
- Privileged or administrative actions
- File and application access (file integrity monitoring)
- Removable-media events where available
- Process and command execution

HOW SNARE SUPPORTS IT

By retaining detailed endpoint and system activity in Snare Central, Snare preserves the history needed to compare current behaviour with past behaviour. AskSnare helps analysts pose exploratory questions and narrow the investigation step by step.

ASK THE EVIDENCE

"Show unusual administrative activity for this user in the last seven days."

"Has this account accessed resources it has not used before?"

"Show privilege changes followed by unusual file access or commands."

More context around legitimate-but-risky activity	**Faster prioritisation for human review**	**Historical evidence for internal investigations**

03 Privilege escalation and privileged account abuse

Attackers seek elevated privileges soon after initial access. Detecting it needs visibility of account changes, elevated sessions, service creation, admin tools and follow-on execution, often across several hosts.

EVIDENCE REQUIRED

- Group membership and role changes (4728, 4732)
- Privilege assignment and privileged logons
- Service and scheduled-task creation (7045, 4698)
- Process creation
- Security-policy changes (4719)

HOW SNARE SUPPORTS IT

Snare provides the operating-system evidence that links initial access to elevated execution. Snare Central retains it off-host with hash verification, so the investigation does not depend on the compromised machine. AskSnare helps correlate privilege changes with the sessions and processes that followed.

ASK THE EVIDENCE

"Show accounts added to privileged groups in the last 48 hours."

"Which privilege changes were followed by remote access or process execution?"

"Show services or scheduled tasks created by newly privileged accounts."

Earlier visibility of attacker progression | **Better evidence for containment decisions** | **Complete privilege-abuse timelines**

04 Lateral movement across the environment

Once attackers have a foothold, lateral movement exposes more systems, credentials and data. Living-off-the-land techniques can look like normal administration, so defenders need detailed histories correlated across hosts.

EVIDENCE REQUIRED

- Authentication events and Kerberos tickets (4768, 4769)
- RDP, SMB and remote-service activity
- PowerShell and command execution
- Process creation
- Remote-administration events

HOW SNARE SUPPORTS IT

Snare preserves host-level evidence across the estate, so analysts are not limited to a single endpoint view. Retained logs in Snare Central can be searched alongside SIEM detections, and AskSnare helps trace a user or host across many systems.

ASK THE EVIDENCE

"Show systems accessed by this account after the suspected compromise."

"Identify remote administrative activity originating from this endpoint."

"Build a timeline of authentication and process activity across these systems."

Faster incident scoping | **Better identification of affected systems** | **Stronger evidence for containment**

Reference: ASD's ACSC and partners, Best practices for event logging and threat detection (living-off-the-land detection)

05 Ransomware and post-compromise investigation

Ransomware is an outcome, not the start of the incident. Investigators must reconstruct what came before encryption: initial access, execution, privilege escalation, discovery, lateral movement, persistence and possible exfiltration.

EVIDENCE REQUIRED

- Authentication and identity events
- Process and command execution
- Privilege changes
- Remote-service activity
- File, system and policy events

HOW SNARE SUPPORTS IT

Snare Central retains historical evidence outside the compromised endpoints, often well beyond the SIEM's retention window, so the full sequence can be reconstructed. Event Replay can return that history to Microsoft Sentinel or Splunk, and AskSnare helps build a cross-system timeline.

ASK THE EVIDENCE

"What happened on this endpoint before the encryption event?"

"Which other systems show the same sequence of behaviour?"

"Summarise the timeline from initial access to encryption."

Faster incident reconstruction	**More accurate scope assessment**	**Evidence that pre-dates the SIEM window**

Reference: IBM, Cost of a Data Breach Report 2026: 183 days on average to identify a breach

06 Proactive threat hunting across historical logs

Monitoring asks whether a rule has fired. Threat hunting asks what may be happening that no rule has recognised yet, which needs accessible historical telemetry and the ability to search for behaviour, not just known indicators.

EVIDENCE REQUIRED

- Historical endpoint and server events
- Authentication activity
- Process and command execution
- Administrative activity
- DNS activity, including ETW DNS Analytic logs

HOW SNARE SUPPORTS IT

Retained evidence in Snare Central supports hypothesis-driven hunting whether or not an alert fired at the time. Event Replay can send a historical slice back into Splunk or Sentinel for analysis with existing content, and AskSnare lets analysts start with a question and refine it.

ASK THE EVIDENCE

"Show PowerShell activity that is unusual for each endpoint."

"Find sequences of failed logons, privilege change and remote execution."

"Which hosts exhibit similar suspicious behaviours?"

Find activity that never raised an alert	**Faster hunting iterations**	**Better use of retained history**

07 Compliance, audit and forensic evidence

Security logging must do more than real-time detection. Organisations may need historical records for compliance, audits, internal investigations, incident response, legal processes and cyber-insurance requirements.

EVIDENCE REQUIRED

- User and system activity for each control
- Administrative and privileged actions
- Configuration and policy changes
- Authentication and access records
- Logs retained for the required period

HOW SNARE SUPPORTS IT

Snare's forensic logging heritage supports collection and multi-year retention independent of the analytics platform, with hash verification on archive ingestion and retrieval. More than 600 pre-built compliance reports cover frameworks including PCI DSS, HIPAA, GDPR and ISO 27001, so an expired SIEM retention window does not become an evidence gap.

ASK THE EVIDENCE

"Show all privileged changes on these systems during the audit period."

"Retrieve the security events for this incident date range."

"Show the sequence of administrative actions for this account."

Evidence ready for audits and investigations	**Retention decoupled from SIEM economics**	**Less reliance on evidence left on endpoints**

Reference: NIST SP 800-92 Rev. 1 (initial public draft); PCI DSS v4.0.1, Requirement 10.5.1

08 Right-sizing SIEM ingestion and storage costs

Ingest-based pricing makes "send everything to the SIEM" hard to sustain, yet discarding data can leave investigation gaps. The architectural answer is to separate collection from destination.

EVIDENCE REQUIRED

- Full-fidelity record of collected events
- Detection requirements per platform
- Event volumes by source and type
- Retention requirements by data class
- Format needs of each destination

HOW SNARE SUPPORTS IT

Snare acts as the control layer before the SIEM. Snare Central aggregates repeated events while keeping the original detail, and retains the full record. Snare Reflector applies per-destination rules, de-duplication, truncation and format transformation. You keep the evidence and pay premium analytics rates only for what detections use.

ASK THE EVIDENCE

"Which sources contribute the most SIEM volume?"

"Which event types are never used by a detection?"

"What would retention cost outside the SIEM?"

Lower premium ingestion	**Evidence preserved, not discarded**	**Predictable growth as sources increase**

Reference: Forrester, data pipeline management for security and IT; ASD's ACSC guidance on filtering before SIEM/XDR

09 Changing SIEM without rebuilding log collection

Organisations consolidate vendors, adopt cloud SIEM, change MSSPs, merge environments or run several analytics platforms at once. The logging layer should not turn every analytics decision into a collection project.

EVIDENCE REQUIRED

- Consistent collection across all sources
- Destination-specific formats and schemas
- Parallel delivery during transition
- Historical data for the new platform
- Per-tenant routing for MSSPs

HOW SNARE SUPPORTS IT

Snare Reflector delivers to all configured destinations simultaneously, with independent queues and failover, so old and new SIEMs can run in parallel during migration. Field remapping aligns data to Splunk CIM or Sentinel ASIM, Event Replay can seed the new platform with history, and Central retains everything regardless of destination.

ASK THE EVIDENCE

"Today: Snare → existing SIEM"

"Transition: Snare → existing SIEM + new SIEM"

"Future: Snare → new SIEM, or customer + MSSP platforms"

Change the destination, not the collection

Lower-risk parallel running

Freedom to choose analytics on merit

10 Finding gaps in visibility and missing telemetry

An often-overlooked risk is missing telemetry. An agent can stop reporting, logging can be disabled, configuration can drift, a new system can appear outside policy, or a source can suddenly send far fewer events.

EVIDENCE REQUIRED

- Expected host and source inventory
- Event-flow and volume history
- Audit policy changes and log clearing (4719, 1102)
- Agent and collector health
- Log-clearing attempts (ATT&CK T1070)

HOW SNARE SUPPORTS IT

Snare monitors the evidence pipeline itself. Sequence-numbered agent streams make gaps detectable, and Snare Central alerts when an agent's event volume deviates from its normal pattern, with sensitivity set at 1σ, 2σ or 3σ. Activity around logging changes is preserved, and AskSnare can help answer which sources stopped reporting.

ASK THE EVIDENCE

"Which systems stopped sending security logs in the last six hours?"

"Which sources are sending materially less telemetry than normal?"

"Show activity around the time logging stopped on this host."

Faster detection of blind spots

Less risk of silent logging failure

Assurance analytics see expected data

Reference: MITRE ATT&CK, Indicator Removal (T1070)

AskSnare: from a security question to the evidence that answers it

The value of AI in investigation is reducing the friction between an analyst's question and the evidence that answers it, so they can move from a broad question to specific steps without starting over.

An investigation as a conversation

1	*"Show failed logins followed by successful privileged authentication in the last 24 hours."*
2	*"Which of those accounts have never logged into those systems before?"*
3	*"Show process activity from those sessions."*
4	*"Which behaviour is unusual compared with prior activity?"*
5	*"Summarise the evidence and the investigation timeline."*

Queries in place

AskSnare queries data where it resides. Nothing is replicated or centralised, so evidence doesn't cross sovereignty boundaries.

Explainable

Every insight comes with a clear rationale analysts can check against the source evidence.

Analysts stay in control

AskSnare is a cybersecurity AI assistant. It recommends and explains; your team decides and acts.

> **The goal is not to replace analyst judgement. It is to make evidence easier to interrogate, correlate and explain.**

Why AI still depends on evidence

Good security AI starts with good security telemetry. AI makes the quality and availability of telemetry more important, not less. An assistant can only reason over what has been captured, retained and made available to it.

MIT Lincoln Laboratory research published in March 2026 examined automated analysis of large-scale host-based logs, reducing hundreds of raw fields to informative dimensions to surface coordinated deviations that are not obvious in individual log streams. Scalable analytics depend on rich, well-structured telemetry.

Reference: Schofield, Jananthan and Kepner, AI for Scalable Defensive Cyber Log Analysis, MIT Lincoln Laboratory (20 March 2026).

10 · SIEM ECONOMICS AND DATA TIERS

Separate analytics needs from retention needs

A sustainable strategy treats security data by how urgently it must be queried, how often it is used and how long it must remain available.

Tier	Primary purpose	Typical destination	With Snare	Retention
Hot	Immediate detection and active investigation	SIEM or high-performance analytics	Reflector sends each SIEM the events its detections need	Hours to weeks
Warm	Investigation context not queried continuously	Searchable lower-cost repository	Snare Central archive on local, NAS or SAN storage, searchable and reportable	Weeks to months
Historical	Forensic, audit and long-range evidence	Economical retained storage	Snare Central on S3-compatible object storage, hash-verified; Event Replay when needed	Months to years

ASD's ACSC guidance similarly distinguishes readily searchable "hot" data from more economical "cold" storage, weighing capacity against forensic value. Snare reports up to 90% lower SIEM storage costs by retaining evidence outside the SIEM; results depend on ingestion volumes, storage policies and log sources.

11 · SECURITY LOGGING MATURITY MODEL

Five levels, from collecting to intelligent investigation

1 · Collect

Security events are captured from key systems.

Outcome: a baseline, often with evidence gaps and source-by-source administration.

2 · Control

Policies, collection and retention are centrally managed.

Outcome: greater reliability, governance and integrity.

3 · Optimise

Telemetry is aggregated, remapped and routed intentionally.

Outcome: lower downstream cost and better signal quality.

4 · Investigate

Historical evidence supports hunting, search and attack reconstruction.

Outcome: faster response and stronger forensics.

5 · Intelligent

AI helps analysts ask, refine and summarise investigations.

Outcome: less investigation friction and wider access to evidence.

Reference: ASD's ACSC and partners, Best practices for event logging and threat detection (22 August 2024).

The questions to ask in your next working session

Work through it with security operations, infrastructure, architecture and risk teams. Unticked boxes are not a failure: each one points to a specific link in the Security Evidence Chain, and most can be closed without replacing the tools you already rely on.

Collection

- [ ] Do we know which security events are collected?
- [ ] Have we mapped key threat techniques to the telemetry needed to investigate them?
- [ ] Are endpoint, identity, server, infrastructure and cloud sources covered?
- [ ] Do we know which critical systems are not logging?

Integrity

- [ ] Are logs protected from unauthorised modification or deletion?
- [ ] Could an attacker erase the only copy of evidence by compromising an endpoint?
- [ ] Can we prove historical evidence has not been altered?
- [ ] Are access and admin actions on the logging environment auditable?

Retention

- [ ] Are retention periods set by investigation and regulatory needs?
- [ ] Does retention exceed our realistic breach lifecycle (IBM's average is 247 days)?
- [ ] Can evidence be retained independently of premium SIEM storage?

SIEM optimisation

- [ ] Does every collected event need to enter the SIEM?
- [ ] Can unnecessary or duplicate events be reduced before ingestion?
- [ ] Can different event sets go to different destinations?
- [ ] Can events be reformatted for each downstream platform?

Portability

- [ ] Can we change SIEM without replacing endpoint collection?
- [ ] Can we send telemetry to several platforms during migration?
- [ ] Can we support on-premises, hybrid and cloud destinations?

Investigation

- [ ] Can analysts search historical logs without a restore project?
- [ ] Can they replay a historical window into analytics?
- [ ] Can they reconstruct a cross-system attack timeline?
- [ ] Can AI help analysts interrogate evidence, with reasoning they can check?

Independent guidance points in the same direction

These sources are cited as independent evidence of the industry challenge. They are not endorsements of Snare.

IBM / Ponemon Institute

The average breach takes 247 days to identify and contain, and breaches lasting more than 200 days cost 12% more than a year earlier.

Cost of a Data Breach Report 2026

Gartner

Log management is important but often undervalued when planning threat detection, investigation and response operations.

Adopt Log Management for Security Operations Use Cases (27 Oct 2025)

Forrester

SIEM ingestion is expensive, and data pipeline management can help control what reaches high-cost analytics platforms.

If You're Not Using Data Pipeline Management for Security and IT, You Need To (12 Nov 2024)

NIST

Log management spans generation, transmission, storage, access and disposal, and supports both investigation and required retention.

SP 800-92 Rev. 1 (initial public draft)

ASD's ACSC and international partners

Effective logging centralises access, protects integrity, supports relevant detections and considers filtering before SIEM/XDR to manage cost and capacity.

Best practices for event logging and threat detection (22 Aug 2024)

MITRE ATT&CK

Detection strategies map adversary techniques to observable telemetry, reinforcing the need to design collection around detection and investigation goals.

ATT&CK Detection Strategies

MIT Lincoln Laboratory

Large-scale host telemetry can support automated, interpretable analysis when it is structured and reduced into informative dimensions.

AI for Scalable Defensive Cyber Log Analysis (20 Mar 2026)

14 · BRINGING IT TOGETHER

One requirement stays constant: reliable evidence

SIEM platforms will evolve, organisations will change vendors and operating models, AI will become part of everyday investigation, and threat actors will keep adapting. Through all of it, security teams need evidence they can rely on.

Collect once	**Protect the evidence**	**Control what goes where**
Retain what matters	**Route to any platform**	**Investigate when needed**

Modern logging should not simply "send logs to the SIEM". It should maintain a security evidence architecture that stays useful when the SIEM changes, the investigation starts 247 days late, a system has been compromised, or analysts need to ask questions nobody anticipated when the data was first collected.

15 · ASSESS YOUR SECURITY EVIDENCE ARCHITECTURE

Six steps to a clear picture

Establish where evidence is generated, how it is protected and routed, what it costs to analyse, how long it is kept and how quickly analysts can interrogate it.

1 Map your current logging architecture

Sources, collectors, destinations and owners.

2 Identify evidence gaps and high-risk sources

Where collection, integrity or retention fall short.

3 Review what enters the SIEM and why

Volume by source against detection use.

4 Model retention and ingestion economics

Hot, warm and historical tiers, against your realistic breach lifecycle.

5 Assess portability across SIEM and MSSP

How hard it would be to change destination.

6 Find where AskSnare can accelerate investigations

The questions analysts ask most.

Start with your logging architecture, not another security tool. Our team can run the assessment with you.

REFERENCES AND FURTHER READING

Sources cited in this playbook

Independent research and guidance referenced throughout. These sources describe the industry challenge and are not endorsements of Snare.

IBM / Ponemon Institute	Cost of a Data Breach Report 2026: The AI tipping point. 602 organisations breached March 2025 to February 2026. p. 15, Figure 5; p. 30, Figure 17. ibm.com/reports/data-breach
Gartner	Adopt Log Management for Security Operations Use Cases, 27 October 2025. gartner.com/en/documents/7114630
Forrester	If You're Not Using Data Pipeline Management for Security and IT, You Need To, 12 November 2024. forrester.com/blogs/if-youre-not-using-data-pipeline-management-dpm-for-security-and-it-you-need-to
NIST	SP 800-92 Rev. 1 (initial public draft): Cybersecurity Log Management Planning Guide, 11 October 2023. csrc.nist.gov/pubs/sp/800/92/r1/ipd
ASD's ACSC and partners	Best practices for event logging and threat detection, 22 August 2024; Implementing SIEM and SOAR Platforms: Practitioner Guidance, May 2025. cyber.gov.au
MITRE ATT&CK	Detection Strategies; Logon Session Creation (DC0067); Indicator Removal (T1070). attack.mitre.org/detectionstrategies
MIT Lincoln Laboratory	Schofield, Jananthan and Kepner, AI for Scalable Defensive Cyber Log Analysis, 20 March 2026. dspace.mit.edu
PCI Security Standards Council	PCI DSS v4.0.1, Requirement 10.5.1. pcisecuritystandards.org

About the Snare capabilities in this playbook. Capabilities described reflect Snare Agent v5.11 and Snare Central v8.8. Deployment pathway availability, supported platforms and destinations vary by configuration; check the Snare support matrix or speak with our team about your environment. Cost figures are Snare's own and depend on ingestion volumes, storage policies and log sources.

NEXT STEPS

Start with the evidence. Build from there.

Snare gives security teams a collection, retention and routing layer that stays useful when the SIEM changes, an investigation starts late or analysts need to ask questions nobody anticipated.

Collect once

Snare Agent for Windows, Linux, macOS and Unix, plus syslog, NetFlow and cloud audit sources.

Protect the evidence

TLS 1.2/1.3 with mutual TLS, an encrypted local buffer and hash-verified archives, retained off-host.

Route to any platform

Simultaneous delivery to multiple SIEMs and data platforms, so the SIEM can change without re-collecting.

Investigate faster

Forensic search, 600+ compliance reports, Event Replay and AskSnare.

Assess your security evidence architecture. Book a technical session with our team to map your sources, retention requirements, SIEM destinations and the deployment pathway that fits your environment. **snaresolutions.com**

Snare is a Prophecy International solution. © 2026 Prophecy International. Analyst and research references are not endorsements of Snare.