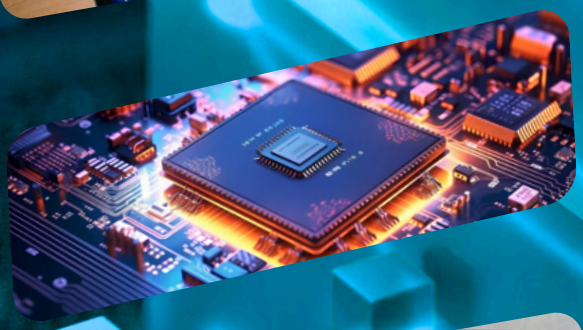


snare
A PROPHECY SOLUTION

Do I Really Need a Full-blown Siem?

Do I Really Need a Full-blown Siem?

Security information and event management systems (SIEMs) are expensive. Their value depends on how well an organization's cyber posture, resources, and deployment are managed. While feature-rich, many organizations fail to utilize them fully, making it difficult to realize the expected return on investment (ROI).

Organizations often face high upfront costs and increasing expenses for data ingestion, storage, and retention. This has led many to question whether the value justifies the cost, especially if the SIEM's full potential is not leveraged. Some turn to managed services to reduce strain; however, this raises data sovereignty concerns as data can be stored in off-site, third-party silos, leaving organizations without direct control.

For many, a full-blown SIEM is neither financially viable nor necessary. These organizations need to collect, store, and retain log data for compliance and audit purposes yet must do so with limited financial and operational resources.

What a Solution Could Look Like

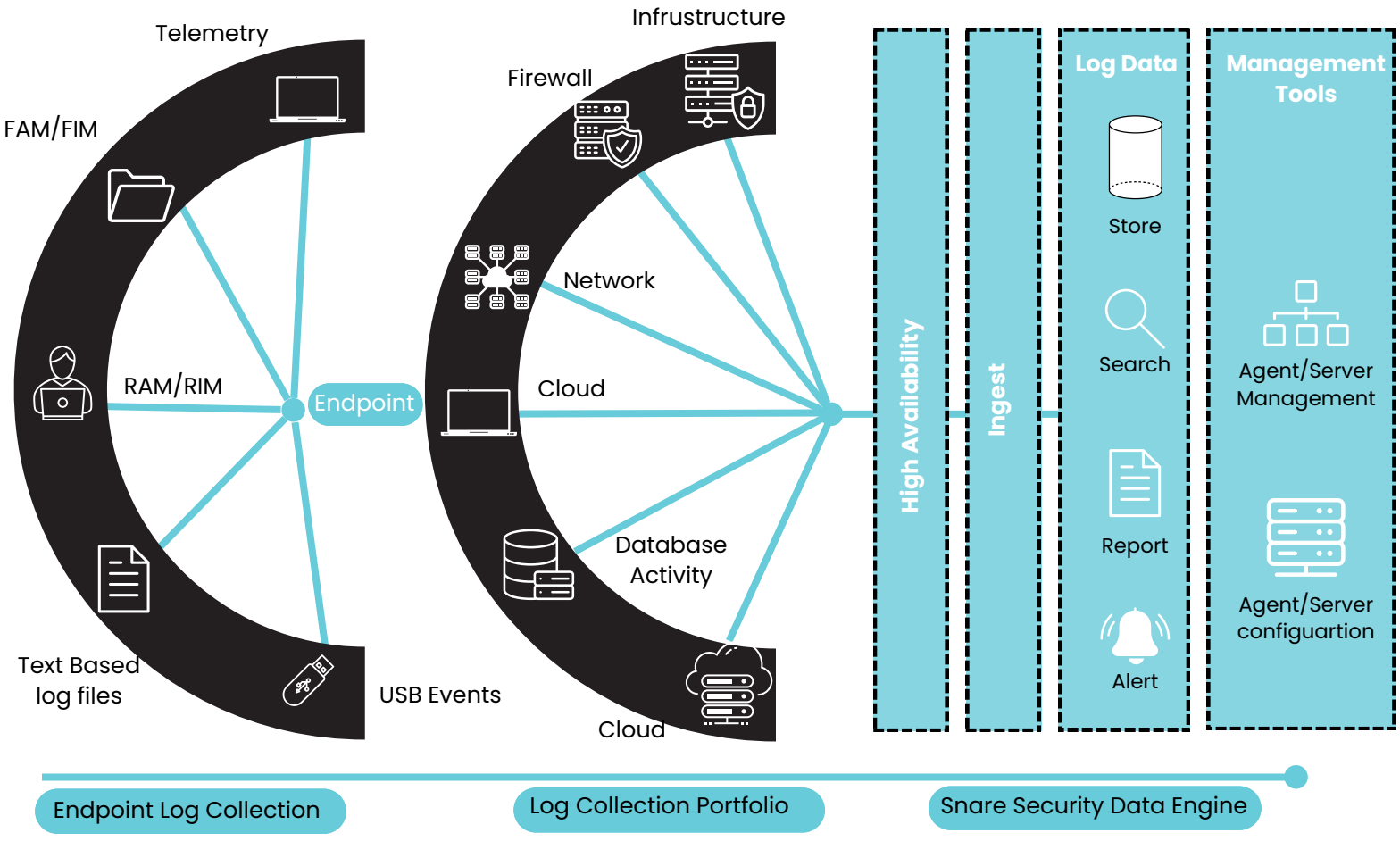
Recognizing the need to collect, store, and retain log data is the first step. Next, you must determine what data to collect, where to store it, and how long to keep it, all in line with compliance and audit governance requirements. This depends largely on the market sector your organization operates in and how its compliance needs map to these requirements. During a cyber incident, you also need to ensure that the data provides evidential support to identify the "what," "when," and "how" of the event.

This leads to the critical issue of SIEM justification: What do I need to do with the collected data? What capabilities and visibility do I require, and for how long? Answering these questions involves defining dashboards, searches, reports, and alerts while determining retention periods, which may vary based on log type. For many organiza tions, these basic requirements are sufficient, making the case for a full SIEM difficult to justify.

The solution lies in deploying a 'SIEM Light' approach. This provides the essential capabilities—data collection, visibility, searchability, and retention—needed to manage critical information while adhering to organizational policies. It achieves this without the usual SIEM ingestion, storage, and retention costs, offering a more practical and cost-effective alternative

Initial discussion and technical evaluation → Proof of concept (POC) and technical walkthrough → Deployment

Snare Architecture



Reduce Data Ingestion, Storage and Retention Costs

Snare's approach delivers core functionality without the ongoing costs of ingestion, storage, and retention.

Snare's approach to data management through a Security Data Engine (SDE) provides several key benefits:

- Retain data sovereignty, maintaining full control over your organizational data.
- Achieve complete visibility of your collected data for as long as needed.
- Set data retention times to align with compliance and audit guidelines.
- Access all evidential support required in the event of an incident.
- Eliminate significant ingestion, storage, and retention costs.
- Avoid paying for SIEM features that your organization does not need or use.
- Benefit from default policies, reports, searches, and alerts based on best practices.
- Reduce the mean time to detect and resolve incidents.
- Ensure full compliance with audit and governance requirements.
- Upstream critical data to a corporate platform when necessary.