The Great Re-Architecture:
A SOC Without SIEM Dependency

RELIAQUEST

EXPONENT

The Promise vs. The Reality of the SIEM-First World

What We Were Promised

- A single pane of glass for all security data
- Centralized detection across every data source
- Faster investigations with unified context
- Complete visibility — if it's not in the SIEM, it doesn't exist

What We Actually Got

- Runaway ingestion costs that scale with every new source
- Alert noise that drowns analysts in false positives
- Latency from high-volume log pipelines slowing detection
- Architecture lock-in that makes change expensive and painful

The SIEM was never designed to be the center of everything — the industry made it that way. The result is an architecture that's brittle, bloated, and increasingly misaligned with how modern threats actually move.

The Hidden Cost of Centralizing Everything

Ingestion Tax

Noise

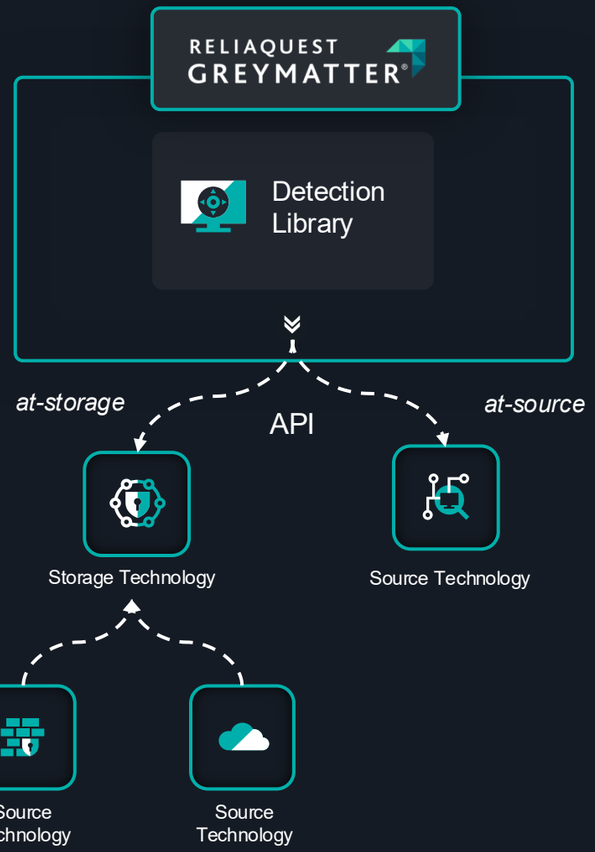
Latency

Flexibility

76%

Detection Use Cases
Don’t Need SIEM

Re-Architect: Detect Threats at the Source

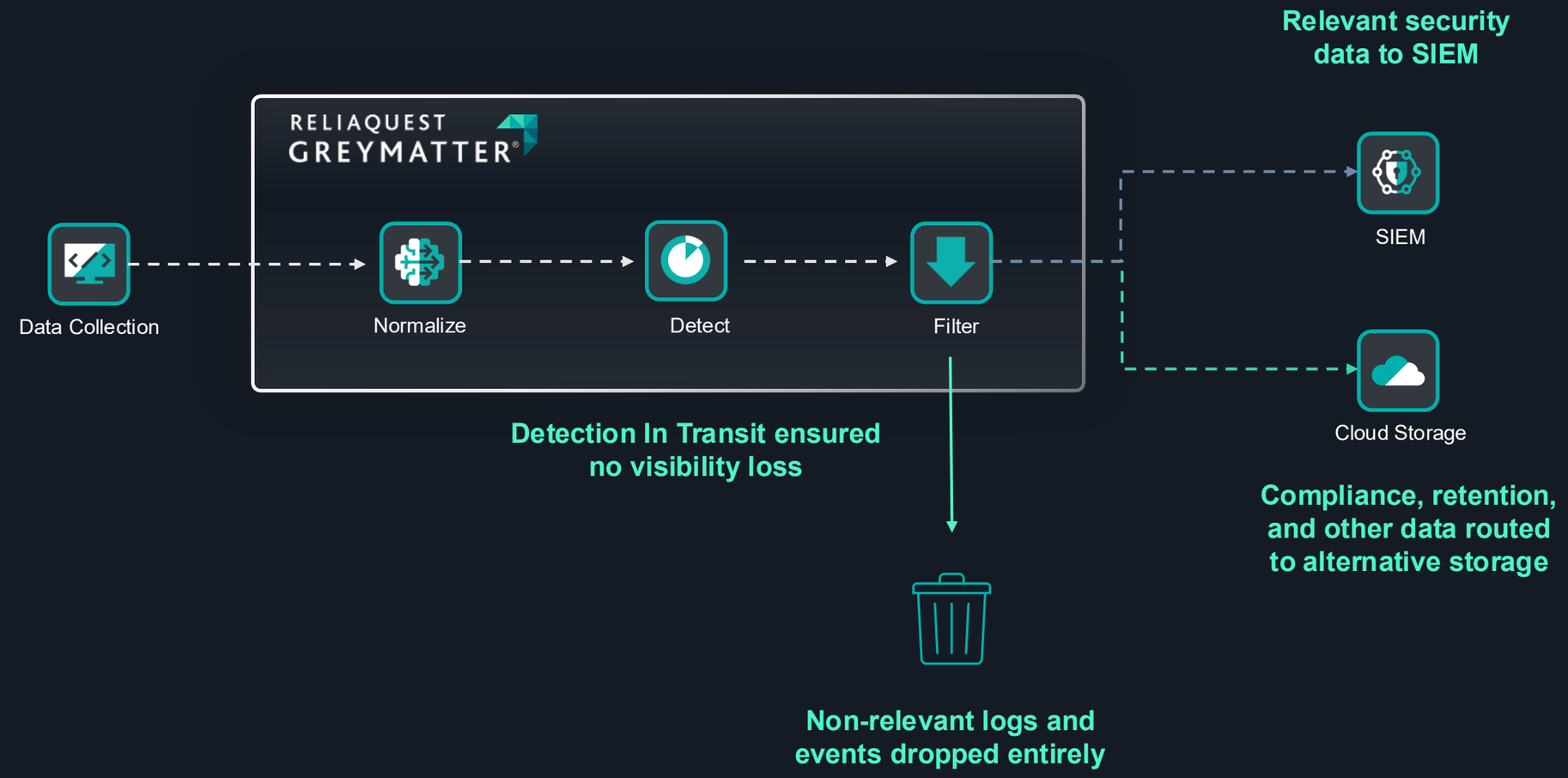


Detection at Source:

- Fire detection logic without requiring SIEM ingestion
- Reduce the volume of data going to the SIEM
- Decrease MTTD by eliminating ingestion lag
- Operate detection use cases even during SIEM outages or swapping technologies

Re-Architect: Detect Threats In Transit

- Detect threats as data moves from source to storage
- Filter and route data to the most cost-effective solution
- Only store relevant telemetry and drop what's not needed



Decoupling Your SIEM Without Losing Visibility

- **Reframe What the SIEM Is For**
- **Detect at-Source and In-Transit**
- **Implement Intelligent Data Routing**
- **Investigate and Hunt At-Source**

RELIAQUEST

EXPONENT