A new way to SIEM

Turn telemetry into **defense**

Cribl
The **AI Platform** for Telemetry

Cribl Detect™

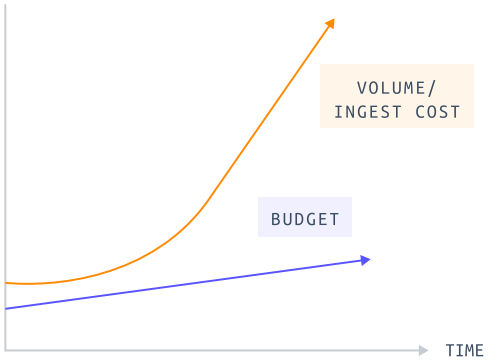
Cribl Detect goes beyond monolithic or so-called "SIEM-less" approaches. It is a complete solution for detection, response, and investigation, with posture management that shows your coverage gaps, and open architecture that gives you choice and control.

The challenge

Existing SIEM models are buckling under AI-era data growth. Data volumes are rapidly outpacing security budgets, and current approaches force tradeoffs.

30%
[1]Source: IDC
CAGR of telemetry data creating massive implications for storage and analysis.[1]

7%
IT budget growth rate; IT budgets are vastly outpaced by data growth

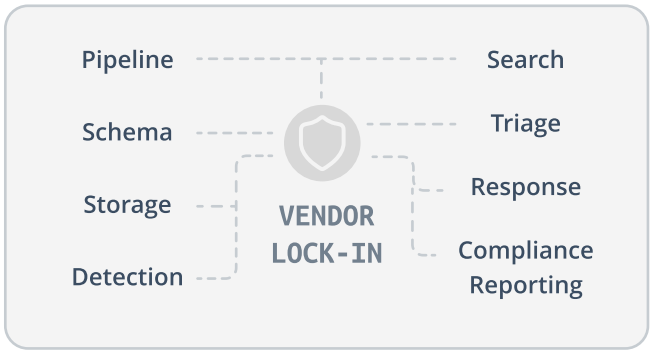


Existing approaches

Existing SIEM models are buckling under AI-era data growth. Data volumes are rapidly outpacing security budgets, and current approaches force tradeoffs.

Legacy SIEM

Monolithic — no choice

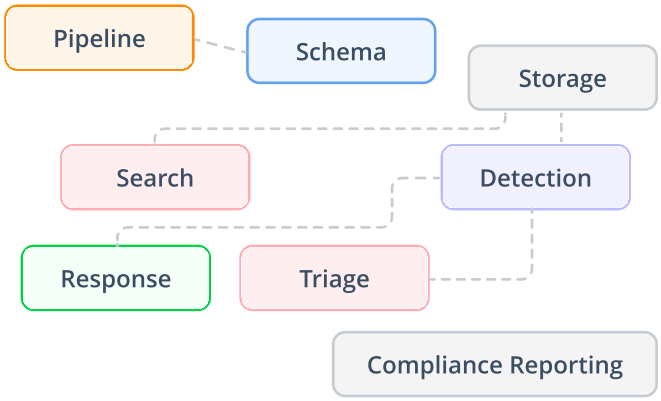


Tradeoff: cost for visibility

Monolithic SIEMs ingest and centralize all your data. The functional components–pipeline, schema, storage, analytics, and reporting–are tightly coupled, locking you into the vendor's architecture. It's priced per GB, so cost-prohibitive economics force tradeoffs between budget and visibility.

"SIEM-less"

Components cobbled together from multiple vendors



"SIEM-less" approaches require you to assemble the components from multiple vendors–and manage multiple formats, schemas, and contracts. You get choice and flexibility, but you are the integrator. The end result still looks very much like a SIEM.

The solution

Cribl Detect charts a new way forward, breaking down the monolith and giving you the flexibility of "SIEM-less" approaches, without the integration hassles. It shows you where you're covered and pinpoints gaps. Detection shifts upstream, decoupling pipeline, storage, and analytics, so you can expand coverage without expanding costs.

KEY BENEFITS

Detect before storage

Analytics run in the pipeline, so telemetry is evaluated for threats in stream, no waiting for indexing. Using the broader Cribl platform, signals can be generated on data routed to Cribl Lake, or outside Cribl entirely. Detection isn't limited by what you can afford to index.

Know exactly where you're exposed

Posture management maps your coverage to ATT&CK, shows where you're missing detections (or the telemetry to power them), and surfaces rules that have silently broken–before a threat goes undetected. Prioritized recommendations tell you what to fix first.

Expand coverage without expanding cost

Not all telemetry carries the same value, so it all shouldn't cost the same. With the Cribl platform, high-value data goes to high-performance storage; full-fidelity telemetry is retained in economical storage for hunting, investigation, and compliance. You pay based on security value, not a flat ingest price.

Investigate the whole estate

Federated search reasons across telemetry wherever it lives—in Cribl or other data lakes and object stores—without rehydration or migration. Results land in one unified view, and an AI copilot helps analysts move quickly from alert to explanation to containment.

Product overview

Detection and correlation

Security analytics are embedded in the pipeline for real-time detection. Correlations chain findings to uncover slow-burn threats that isolated alerts miss. Start from a catalog of 8,000+ rules, or build your own in Detection Lab, an AI-assisted rule builder.

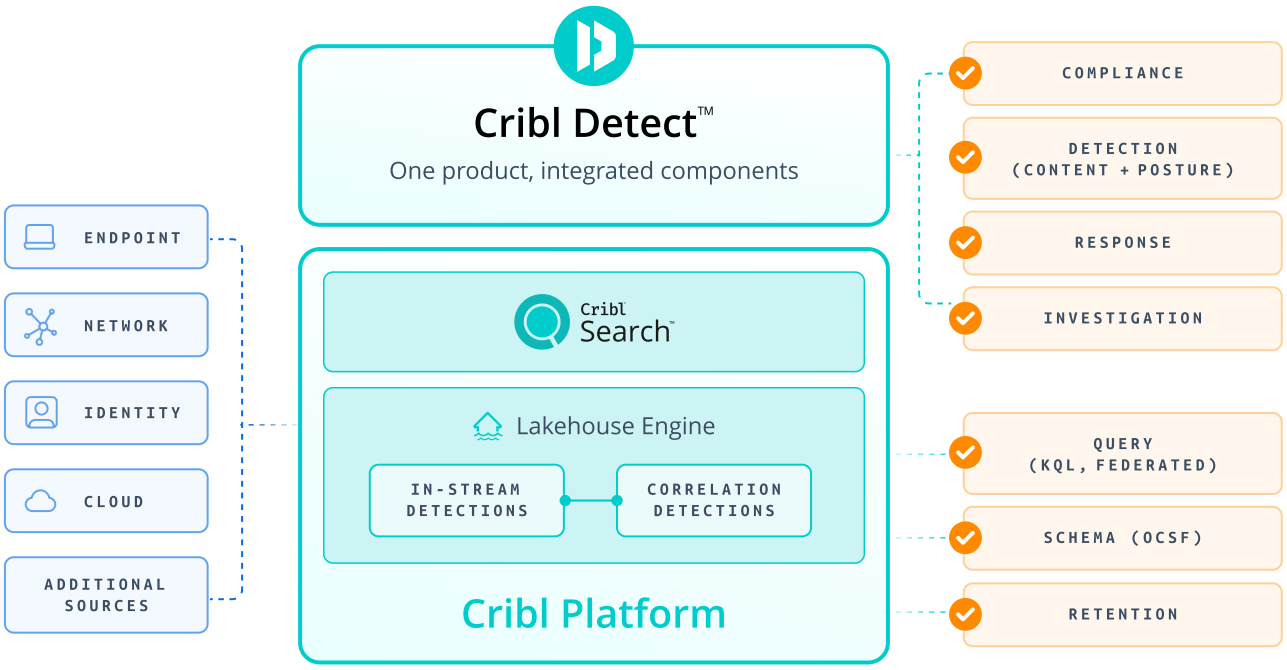
AI-powered investigation

Analysts query sources directly—no re-indexing, no data movement—and get aggregated results in a single interactive view. Natural language search removes the query-language barrier, while notebooks turn searches, findings, and notes into collaborative investigation records.

Alerting and response

AI-driven triage separates threats from noise, escalating what matters. Signals are grouped into detailed alert views rather than raw events, each carrying the threat intel, identity, and asset context analysts need. Manage findings as cases, sync with ticketing systems, and trigger runbooks through existing SOAR workflows.

Open architecture for choice, control, and flexibility



Platform-first, solution-ready

Cribl Detect extends Cribl's AI Platform for Telemetry into a complete security analytics solution, integrating core functional SIEM components to enable compliance, detection, response, and investigation.

Security logs flow from endpoints, network, identity, cloud, and other sources into an embedded pipeline for real-time detection. With the broader Cribl platform, tiered routing separates signal from noise. High-value data goes into Lakehouse Engine for correlation-based detection and search. Low-value data goes to Cribl Lake for low-cost storage. Searches are in KQL, and federation powers investigations across your entire estate.

Open *SIEMs* at Every Layer

Cribl Detect is designed around openness and extensibility. Each functional layer is Cribl-native, but none of it is mandatory. You can bring or keep your own object stores or data lakes. Lakehouse engine normalizes data into OCSF, an open, consistent schema for easy export to other platforms. KQL is a widely used language, so other systems can target our infrastructure for federation. We also support integrations with your existing response workflows with SOAR integrations.

Cribl | The **AI Platform** for Telemetry

Learn more at cribl.io | Try Cribl Sandboxes | Join our Slack community | Follow us on LinkedIn and X

OPG-0036-EN-1-0926