>SOLUTION BRIEF_

Cribl Search

THE CHALLENGE

Turning raw data into answers is traditionally expensive and slow. Teams have to onboard massive volumes of data, manually apply schemas to make it searchable, store it, and constantly rebuild queries just to keep up.

THE SOLUTION

For incident responders—DevOps, threat hunters, platform engineers, security analysts, and SREs—Cribl Search delivers a faster, simpler, and more collaborative way to investigate logs. Bringing ingest, storage, and high-speed analysis together in a single solution, with the ability to also search data at rest, Cribl Search helps teams collaborate with full context and use AI to get to answers fast.

THE BENEFITS

- Get fast time to value with data onboarding
- Cut legacy log management costs
- Run 10x faster investigations with AI
- Consolidate tools and reduce context switching
- Lower operational overhead with an intuitive experience

Cribl Search is a unified log search and investigation platform that delivers a faster, simpler, and more collaborative way to investigate logs. Security and IT teams can ingest data in minutes, collaborate in shared Notebooks, and use AI-assisted workflows to move from questions to answers—fast. When performance matters, 10x faster investigations make all the difference.

The challenge

Today's data environments are more fragmented than ever. Security and IT teams rely on logs spread across clouds, data lakes, and multiple tools, making investigations slow, manual, and expensive. Finding answers often means rehydrating data and moving it between systems. Costs for SIEM, observability, and storage continue to rise while budgets shrink.

At the same time, AI is fundamentally changing the scale of the problem. Modern AI workloads generate 10–100× more queries than humans ever could, pushing legacy architectures past performance limits. With more data than ever, too few skilled analysts, and constant manual toil just to keep systems running, teams struggle to gain context, collaborate effectively, and get answers when speed truly matters.

The Cribl Solution

Cribl Search began by letting teams search data where it lives—without rehydration delays or vendor lock-in—giving them flexibility, control, and lower costs through federated, search-in-place technology. Today, Cribl Search has evolved to support AI-scale workloads with new capabilities that unify ingest, storage, and high-speed search. Teams can search data in-place when it makes sense, or ingest data and investigate immediately when speed and simplicity matter most.

Ultimately, Cribl Search delivers a unified, high-performance search experience across all your data—hot or cold, in place or ingested—so you can investigate faster while reducing cost, complexity, and vendor lock-in.

Search Data on Ingest: Lakehouse Engine

Cribl Search makes it fast and easy to onboard data in minutes, so searches can be run immediately. Search computes where the data is, then AI-powered parsing and extraction stores the data in the format required, for rapid, real-time analysis.

This unified ingest-to-investigate architecture eliminates tool sprawl complexity, bringing all the telemetry into a single workspace where humans and AI agents work side by side to generate answers. Built to handle the massive telemetry volumes of AI-driven workloads, Cribl Search delivers faster investigations, streamlined workflows, and lower operational overhead, making advanced analysis accessible to all analysts.

Unified: One System from Ingest to Investigation

Juggling multiple tools to ingest, store, and query data slows down investigations, is error-prone, and increases overhead. Cribl Search unifies these workflows: go from ingest to analysis with no extra pipelines or handoffs. A single interface brings together ingest, storage, exploration, and investigation, while all essential capabilities—collection, normalization, storage, search, and dashboards—live in one integrated system, reducing complexity and speeding up investigations.

Context is fragmented across tools and scattered across endless tabs. Cribl Search brings data, context, and workflows into a single investigation experience.

Streamlined: Fast, Frictionless Workflows

Turning raw data into searchable insights can take 10–15 steps with traditional pipelines. Cribl simplifies ingestion with automatic parsing, AI-assisted guidance, and streamlines workflows, making data ready for analysis in minutes. Teams can explore data instantly, understand dataset characteristics, give analysts immediate insight and help reduce the manual toil of building queries.

Agentic AI: Increases Speed, Democratizes Access

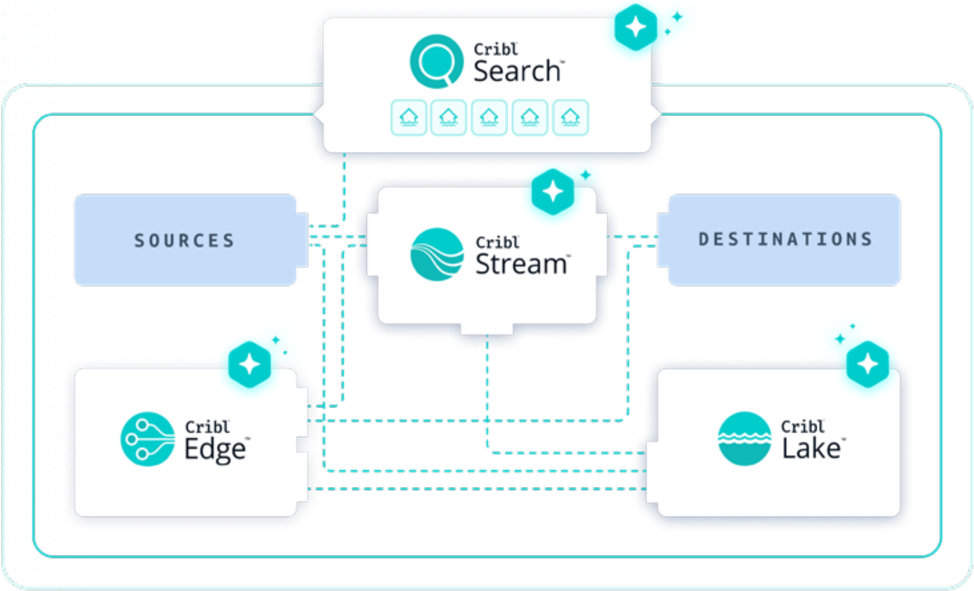
Investigators spend too much time collecting data, then piecing together associated context, and tracking down owners. Cribl Search automatically taps operational context from systems like ServiceNow, leverages enterprise knowledge via AI/LLMs, and guides analysts toward likely root causes. By surfacing “who to talk to” and “what to do next,” Cribl dramatically accelerates investigations and responses. Combined with Cribl Copilot and Notebooks, teams can ask questions of their data and let agentic AI drive exploration and collaboration.

Search Data at Rest: Federated Engine

Cribl Search’s federated search-in-place approach lets teams query data where it lives—across data lakes, object stores, API endpoints, cloud services, and more—without first moving or centralizing it. This eliminates the time, cost, and complexity of traditional ingestion and rehydration workflows, giving analysts access to previously unreachable telemetry with a single query interface.

By searching data directly at its source, Cribl Search provides real-time visibility into all your data stores and reduces dependency on expensive, siloed systems. Results from multiple systems are federated, aggregated, and presented in a unified view, so teams can investigate across environments without switching tools or stitching together results manually.

This federated model also supports compliance and audit requirements by enabling low-cost storage strategies that leave data in place—whether in cloud buckets or cold archives—while retrieving only what's needed for analysis. This ensures secure, long-term retention, faster access for investigations, and full visibility across your entire data landscape.



Cribl Search gives IT and Security teams the power to collect, process, and ask questions of data anywhere – whether it's in flight, in a data lake, or at the edge.

Facets of Cribl Search

Notebooks: A single workspace for faster, more collaborative investigations.

Only have one tab open to run an entire investigation. Analysts can use Notebooks to combine queries, charts, text, and search history to explore results in depth — without repeatedly querying underlying data sources — saving both time and money. Teams can refine searches, segment data for deeper insights, and apply enrichment and transformations as needed.

Built-in annotations, co-editing, presence indicators, and version control create a collaborative, auditable investigation trail. AI summarizes key results and insights that can be shared to higher-ups. Together, these capabilities deliver a clear investigation trail that improves efficiency, accuracy, and collaboration in incident response workflows.

Search Packs: Config bundles to shortcut extensive manual setup

Search Packs are predefined bundles including dashboards, saved searches, macros, lookups, and documentation tailored to specific data sources or common use cases. By providing reference examples that can be inspected, customized, or extended, Search Packs accelerate onboarding, reduce setup time, and make it easy for teams to maximize the value of Cribl Search across the organization.

Scheduled Searches & Alerts: Automate to stay ahead of issues

Scheduled searches let admins and users control when searches run and turn results into actionable alerts. Teams can automate routine analysis to detect anomalies, monitor thresholds, compare results over time, and track long-term trends—triggering alerts when conditions are met. This proactive approach helps teams stay ahead of issues, reduce manual effort, and respond faster without constantly running ad-hoc searches.

Differentiators

OPEN

Freedom to search your data—your way. Cribl Search gives teams true choice: low-cost, federated search-in-place when data should stay where it is, and high-speed ingest-based search when performance matters. Open by design, it integrates easily across agents, AI, storage, and tools—keeping data portable, interoperable, and future-proof as architectures evolve.

FOCUSED

Purpose-built for IT and security investigations. Designed for telemetry at scale—logs, events, and signals that power daily investigations. From incident response to threat hunting and troubleshooting, it's built around how IT, SecOps, SRE, and InfraOps teams actually investigate, collaborate, and resolve issues.

PERFORMANT

Engineered for AI-scale speed and reliability. Built to handle massive telemetry volumes and AI-driven workloads, Cribl Search delivers fast, predictable performance even as query volumes explode. By putting compute where the data is and optimizing for high-speed search, it enables 10× faster investigations with Notebooks to streamline collaboration.

VERSATILE

Easy to start. Powerful to scale. Teams can onboard data in minutes with automatic parsing and AI-assisted workflows, then grow into advanced investigations, alerting, Notebooks, and agentic search. Cribl Search meets users where they are—simple for beginners, powerful for experts, and flexible enough to adapt to any environment.

PROVEN

Trusted by over 50% of Fortune 100, built for real outcomes. Cribl Search is battle-tested at scale, helping teams reduce costs, consolidate tools, and move faster with fewer resources.

Cribl Search: getting started.

To get started with Cribl Search today, sign up for Cribl.Cloud or request a demo. The Cribl Slack Community is also a great place to connect with leaders from other teams utilizing the Cribl suite of products.

ABOUT CRIBL

Cribl, the AI Platform for Telemetry, empowers enterprises to manage and analyze telemetry for both humans and agents. Trusted by organizations worldwide, including half of the Fortune 100, Cribl bridges the gap between AI ambition and infrastructure reality. No lock-in. No data loss. No compromises. Cribl's vendor-agnostic platform ensures data remains portable and interoperable. By cost-effectively handling increasing data volume and variety without delay, Cribl gives enterprises the choice, control, and flexibility to build what's next.

Learn more: cribl.io | Try now: Cribl Sandboxes | Join us: Slack community | Follow us: LinkedIn and X

SB-0014-EN-8-0326