>DATA SHEET_

Cribl Search™

One search experience for all telemetry

Cribl Search is a unified 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.

Replace fragmented tools and expensive legacy logging stacks with a single search experience designed for IT and security teams working in the AI era.

CRIBL SEARCH IS POWERED BY:

1. Lakehouse engine for high-speed searches of data ingested directly into Search
   - **Low-touch data onboarding:** Ingest data in minutes, auto-detect formats with data types, and land data in investigation-ready datasets—no complex pipeline building or cross-team handoffs required.
   - **High-performance lakehouse engine:** Run fast, concurrent searches on hot and recent data ingested directly into Search, land data in bottomless, managed storage optimized for sub-second searches.
   - **AI-powered investigations:** Use Copilot and Notebooks to guide exploration, correlate context, and document end-to-end investigations in a shared, collaborative workspace.
   - **Unified ingest-to-analyze architecture:** Combine ingest, storage, search, dashboards, and alerts in one product to reduce tool sprawl, lower costs, and simplify operations.
2. Federated engine for low-cost, search-in-place capabilities for data at rest
   - **Search data where it lives:** Run queries directly against data lakes, object storage, cloud services, and live APIs—no rehydration or data movement required.
   - **Cost-optimized long-term retention:** Keep historical data in low-cost object storage while accelerating investigations on your most critical lake data.
   - **Unified, data-agnostic search:** Use a single query language to federate searches across multiple data stores and data types, both structured and unstructured, through one consistent interface.
   - **Rich API and provider support:** Query live sources such as AWS, Okta, Zoom, Microsoft Graph, GCP, and Google Workspace using built-in Dataset Providers and collectors.
   - **Works with your existing stack:** Layer federated search on top of your current SIEM, observability, and storage tools—no re-platforming, rip-and-replace, or vendor lock-in required.

Together, these engines deliver 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.

FAST TIME TO VALUE

Ingest data in just minutes, run searches immediately.

10× FASTER INVESTIGATIONS

Streamlined workflows, automatic parsing, and unified views eliminate manual toil.

TOOLS CONSOLIDATION

One architecture for ingest, storage, search, dashboards, and alerts.

CUT LOG MANAGEMENT COSTS

Move workloads off SIEM and APM tools to reduce costs.

AI-POWERED INVESTIGATIONS

Guided exploration surfaces context, next steps, and root cause faster.

Product Features

SERVICE

- **AI-Powered, Question-First Search.** Investigate with natural language while agentic AI suggests and refines queries end-to-end.
- **Direct Ingest into Search.** Send data straight into the Search lakehouse engine without requiring Stream.
- **Unified Ingest-to-Investigate Architecture.** Use one product for ingest, storage, search, and analysis with unified configuration and billing.
- **AI-Powered Investigation Experience.** Intuitive search interface enhanced with AI to accelerate exploration and reduce reliance on highly specialized query expertise.
- **High-Performance Query Engine.** Designed to handle AI-scale concurrency and query volumes, delivering fast results across large datasets.
- **Federated Search Across Analytics Platforms.** Query Snowflake, ClickHouse, Azure Data Explorer, Prometheus, and other services in place without re-indexing. Allows users and administrators to query multiple data stores and sources, and works in conjunction with existing search and analysis tools.
- **Low-touch Data Onboarding.** Easily ingest data into Search with automatic data type detection and optimized local storage for high-speed investigation.
- **Flexible Data Formats & Sources.** Supports logs, metrics, events, and structured/unstructured telemetry across hybrid and multi-cloud environments.
- **API & Search-as-Code Automation.** Automate configuration, permissions, and deployment using API credentials and manage Cribl Search as code, including a Terraform provider support.
- **Live API Search.** Run searches directly against API endpoints such as AWS, Okta, Zoom, Microsoft Graph, GCP, Google Workspace or any custom REST API.
- **Elastic Distributed Architecture.** Automatically launches the required distributed search resources to meet data volume and concurrency demands.
- **Broad File Format Support.** Search text-based files and specified binary formats, including Parquet, JournalD, and Splunk index files, and compressed files.

MANAGEMENT

- **Managed, Bottomless Object Storage with Auto-Tiering.** Retain data as long as needed in S3-backed storage that automatically tiers by access patterns.
- **Multi-Region, Multi-Cloud Lakehouse.** Run Lakehouse in multiple AWS and Azure regions to improve performance and meet data residency requirements.
- **Centralized Dataset Control.** Define, manage, and govern datasets from a unified control plane.
- **Lakehouse-Accelerated Datasets.** Run fast, cost-efficient searches on recent data while retaining full historical data in low-cost object storage.
- **Ingest-Time Retention & Storage-Aware Filtering.** Avoid hidden gaps in historical searches with retention policies and intelligent time filtering — even when timestamps are incomplete.
- **Pipeline Simplification.** Reduce ingestion complexity and pipeline sprawl with streamlined workflows.
- **Reusable Search Logic.** Save, standardize, and share searches to improve collaboration and investigation consistency.
- **Role-Based Access Control (RBAC).** Granular permissions ensure the right teams access the right data.
- **Flexible Dataset Partitioning.** Search optimized subsets of data using time-based or custom partitions (e.g., technology, geography, environment) across S3 and other storage systems.
- **Guided Setup & Out-of-the-Box Datasets.** Simple setup wizard and preconfigured datasets — including Cribl system logs, Amazon S3, Cribl Edge logs, and more — to accelerate time to value.

SECURITY

- **Secure-by-Design Architecture.** Built with encryption in transit and at rest to protect sensitive data.
- **Data Access Controls.** Fine-grained access management for datasets and search results.
- **Audit Logging.** Track activity across search sessions and administrative actions.
- **Cloud-Native Security Practices.** Supports modern cloud security frameworks and best practices.
- **Encryption-Aware Search of Stream-Encrypted Data.** Search and decrypt Stream-encrypted fields on the fly for authorized users without exposing data at rest.
- **Fine-Grained API Credential RBAC.** Scope API keys to specific datasets and actions using the same role-based model as users and teams.

DEPLOYMENT AND ARCHITECTURE

- **Unified Architecture.** Integrates ingestion, storage, and search to reduce tool sprawl and simplify operations.
- **Cloud & Hybrid Support.** Available via Cribl-managed cloud services or customer-managed deployments.
- **Elastic Scalability.** Scales to support AI-generated query volumes and growing data footprints.
- **Open & Flexible.** Designed to work within existing data ecosystems — without forcing data lock-in or costly re-platforming.
- **Bring Your Own Model (BYOM).** Point Cribl AI features at your own AI models (Anthropic or OpenAI) to meet strict privacy and compliance needs.

SEARCH INTERFACE

- **IDE-Like Search Experience.** Interactive search bar with typeahead suggestions for operators, functions, fields, and recent queries.
- **Real-Time Query Validation.** Catch errors before execution to save time and cost.
- **Local Query Preview.** Optimize queries before running them against full datasets.
- **Interactive Dashboards.** Token-aware drilldowns allow seamless transitions from charts to deep investigations or external tools.
- **Extensive Operators & Functions.** Over 250 operators and functions to shape, filter, enrich, and analyze data.
- **Built-In Documentation & History.** Access operator documentation, recent queries, and saved searches directly within the interface.

WORKING WITH RESULTS

- **AI-Assisted Investigation Notebooks with PDF Export.** Document investigations in shared notebooks and export them as PDFs for tickets, audits, and reports.
- **Rich, Interactive Results UI.** View results as events, fields, tables, timelines, or charts.
- **Advanced Visualization Options.** Create dashboards with customizable chart types, layouts, and drilldowns.
- **Field Discovery & Enrichment.** Automatically compute top values, unique counts, presence statistics, and enrich results with lookups.
- **Scheduled Searches & Alerts.** Automate recurring searches and trigger notifications via Email, SMS, PagerDuty, Webhook, and more.
- **Search Result Reuse.** Reuse prior results when underlying data has not changed to reduce redundant compute.
- **Search Packs.** Prebuilt dashboards and configuration bundles aligned to common data sources and use cases — accelerating onboarding and time to value.
- **Collaborative Investigation Notebooks.** Combine searches, charts, and detailed notes into shareable investigation workflows that can be refined and reused.

TECHNICAL REQUIREMENTS

System

- Cribl Search is available as a service at https://cribl.cloud/

Browsers Supported:

- Firefox 65+, Chrome 70+, Safari 12+, Microsoft Edge

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

DS-0003-EN-8-0326