Cribl

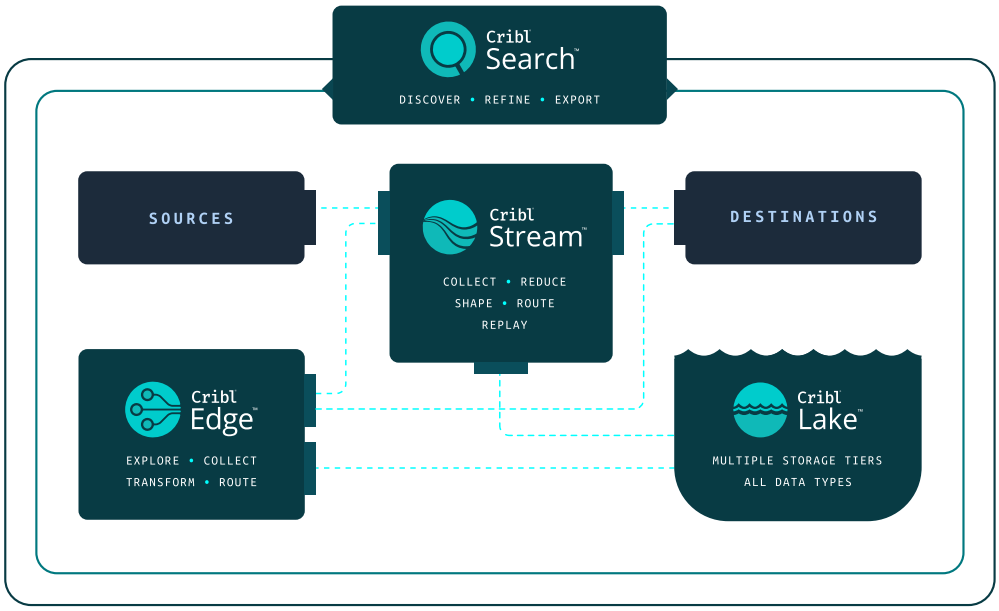
Cribl Search™

Cribl Search is an innovative new approach to finding and accessing data regardless of where it is landed and in any format.

Cribl Search flips the traditional search process on its head, delivering a federated, search-in-place processing engine that accesses data from any source or storage medium in any format using a single, intuitive query interface. Able to explore data anywhere and work with other products to forward in right format, a functionality called Schema-on-Need.

Benefits.

- Search data in place, still on the source, accessible via an API or already stored in a data lake.
- A single unified search experience reduces cost and people hours of administering and supporting each proprietary tool.
- A data agnostic search service with an ergonomic query language that federates searches across multiple data stores and multiple data types.
- Eliminate risk and uncertainty with a 'search then forward' model instead of the legacy 'forward then search' approach.
- Optimize infrastructure, data ingestion, tool performance, and people hours.



NO NEED TO MOVE DATA FIRST

Search data without first having to move it.

NO RIP AND REPLACE

Complements your existing systems of analysis.

SHAPE YOUR DATA

Take data as it comes, shape it into what you need.

NO COMPLEX QUERY LANGUAGE

Put data where it has the most value.

NO RESTRICTIVE LICENSING

Self-service sign up and pay for what you use via Cribl.Cloud.

Product Features

SERVICE

- Eliminates costs associated with first collecting and only then being able to query the data. Search options include — Search data in place (still on the source), data at rest (already stored in a data lake), or even data cloud data warehouses..
- Federated search service allows users and administrators to query multiple data stores and sources. Works in conjunction with existing search and analysis tools.
- Allow administrators to simply identify the targeted data to be searched, via datasets, and launch the query.
- Integration with Cribl Edge allows for direct teleporting from search results into endpoints.
- Ability to search data from Cribl Stream in Cribl Lake, S3 or other cloud storage options.
- Ability to send Search Results to Cribl Lake or any Cribl Stream destination.
- Simple query language that is intuitive, ergonomic and powerful; fits the requirements of all personas.
- Cribl Search comes with out of the box integration with Cribl's entire suite of products. Integration with Cribl Stream, Edge, and Lake provide a turnkey solution for storing, routing, shaping, and searching of data between the four products.
- Allows administrators to also run searches against live API endpoints, such as AWS, Okta, Zoom, Microsoft Graph, GCP, Google Workspace and a generic REST collector to allow administrators to configure any API endpoint.
- Inbound API allows seamless integration with existing third-party tools to automate operations.
- Scalable service launches the required number of distributed search resources to address searchable data volume.
- Employs the same consumption based pricing as Cribl Stream/Edge, but is CPU based vs data ingestion.
- Ability to search into any text-based files, as well as specified binary file formats, including Parquet, JournalD, and Splunk index files and even compressed files.

MANAGEMENT

- Dataset partitions in S3 (and other data stores) allow arbitrary subsets of data to be searched more optimally, including arbitrary customer-specified partitions (eg technology, location, geo) as well as time-based partitions (e.g. year, month,day,hour etc.).
- Authentication services to restrict access to searches and data based on individual or team rights.
- A simple, user-friendly wizard available at first use (or at any time) provides administrators to configure datasets and launch their first query in minutes.
- Cribl Search ships with out-of-box configurations as well as allowing user to configure their own.
- Default datasets available out of the box include: Cribl system / internal logs, Amazon S3 buckets, Cribl Edge logs, and and more.

SEARCH INTERFACE

- Interactive, user-friendly search bar provides a rich IDE-like experience.
- Typeahead assist provides recommendations for operators, functions, field names, and recently-run queries.
- Real-time query validation ensures correctness before query dispatch.
- Built-in Docs :Extensive documentation for operators and functions.
- History: Provides quick view of recent queries.
- Saved Searches: Ability to save, access, edit or rerun previous searches you have saved.
- Operators and Functions: Supporting over 250 operators and functions help users find, shape, slice and dice the data in various ways.
- Local query preview allows query optimization before incurring time or cost of execution on actual data providers.

WORKING WITH RESULTS

- Scheduled Searches allow administrators automatically run searches at predetermined times.
- Notifications can be automatically generated when a scheduled search matches a defined condition. Notifications formats include Email, SMS, PagerDuty, Webhook, and more.
- Rich, interactive, user-friendly UI for working with query results.
- Standard UI or a user defined, customizable dashboards are available.
- Results are displayed in multiple formats including events, fields, or charts.
- Interactive timeline supports drilldowns on time bins.
- Discovered and extracted fields are automatically computed for top value distribution, presence, uniques, etc.
- Results can be shaped, filtered, enriched via lookups and sorted either using the query itself or the rich UI tooling.
- Ability to display query results in standard table (text) format or an easy to view chart format with various visualization options.
- Use the rich set of chart types , color palettes, and a number of options to produce best visualization for the data.
- Search Packs are predefined configuration bundles providing a mechanism for packaging, sharing, and installing dashboards and configurations that align with a given data source or built around common use cases.
- Access is available to a growing community of Search Packs with pre-built dashboards and other out-of-the-box features to accelerate Search on-boarding and improving the time-to-value of Search.
- Ability to reuse the results of a previously-run search, avoids running the same search multiple times if the data hasn't changed.

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 Data Engine for IT and Security, empowers organizations to transform their data strategy. Customers use Cribl's vendor-agnostic solutions to analyze, collect, process, and route all IT and security data from any source or in any destination, delivering the choice, control, and flexibility required to adapt to their ever-changing needs. Cribl's product suite, which is used by Fortune 1000 companies globally, is purpose-built for IT and Security, including Cribl Stream, the industry's leading observability pipeline, Cribl Edge, an intelligent vendor-neutral agent, and Cribl Search, the industry's first search-in-place solution. Founded in 2018, Cribl is a remote-first workforce with an office in San Francisco, CA.

Learn more: www.cribl.io | Try now: Cribl sandboxes
Join us: Slack community | Follow us: LinkedIn and Twitter

DS-0003-EN-5-1024