DATA SHEET

Cribl Search™

Cribl Search is a unique, vendor-agnostic analytics service that performs search-in-place queries.

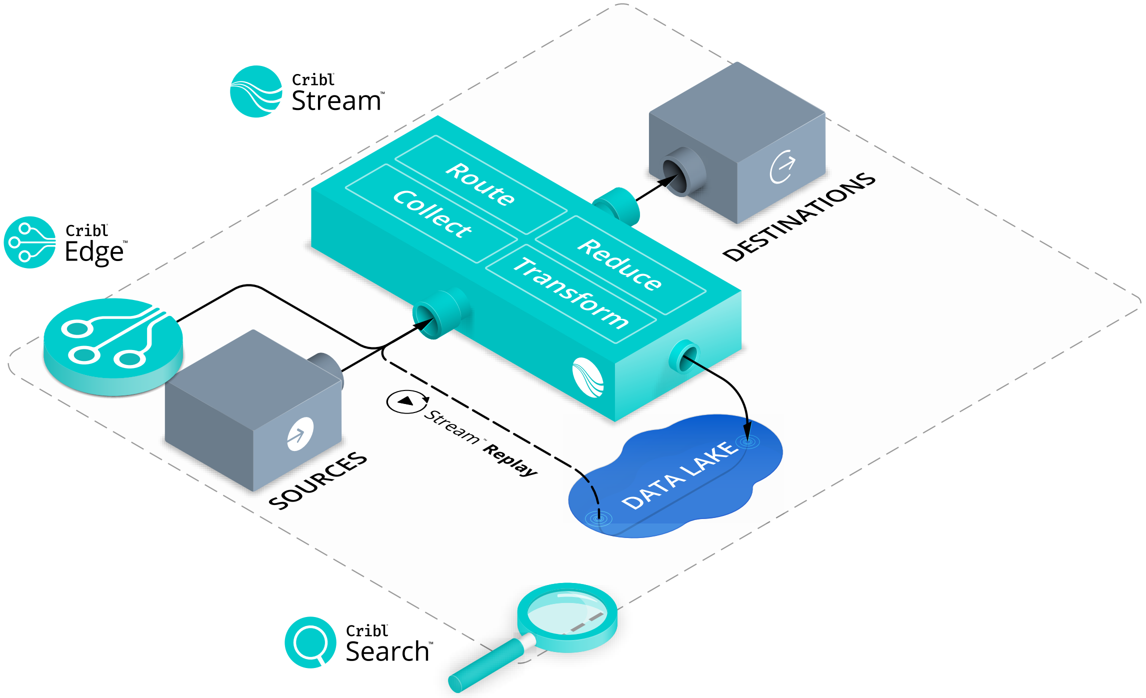
Cribl Search flips the traditional search process on its head; no longer must administrators collect, move and store data prior to searching. Now users can search data at the edge, moving through an observability pipeline, stored in a data lake, or even stored in their existing solutions like TSDBs or log stores.

Benefits

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 types and multiple data stores.

Eliminate risk & uncertainty with a 'search then forward' model instead of the legacy 'forward then search' approach



NO NEED TO MOVE DATA FIRST
Search data without first having to move it

NO RIP & REPLACE
Complements your existing systems of analysis

NO COMPLEX QUERY LANGUAGE
Simple, user-friendly query configuration

NO RESTRICTIVE LICENSING
Self-service sign up and pay for what you use via Cribl Cloud

Product Features

SERVICE

- *Federated search service allows users and administrators to query multiple data stores and sources. Works in conjunction with existing search and analysis tools.*
- *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 in flight through an observability pipeline.*
- *Allow administrators to simply identify the targeted data to be searched, via datasets, and launch the query.*
- *Simple query language that is intuitive, ergonomic and powerful; fits the requirements of all personas.*
- *Out of the box integration with other the Cribl.Cloud suite of products as well as Amazon S3, Amazon Security Lake, Azure Blob, Google Cloud Storage and more Integration with Cribl Edge allows for direct teleporting from search results into endpoints.*
- *Allows administrators to also run searches against live API endpoints, such as AWS, Okta, Zoom, Microsoft Graph, GCP, Google Workspace and more.*
- *Inbound API allows seamless integration with existing 3rd 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. Available to use from day one.*
- *Ability to search into any text-based files, as well as specified binary file formats, including Parquet, JournalD, and Splunk index files.*
- *Ability to search data from Cribl Stream (using a customer-owned S3 bucket as storage).*
- *Ability to send Search Results to any Cribl Stream destination.*

MANAGEMENT

- *Dataset partitions in S3 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 (eg 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 Local Filesystems*

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: 20+ operators and >200 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.*

TECHNICAL REQUIREMENTS

System

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

Browsers Supported:

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