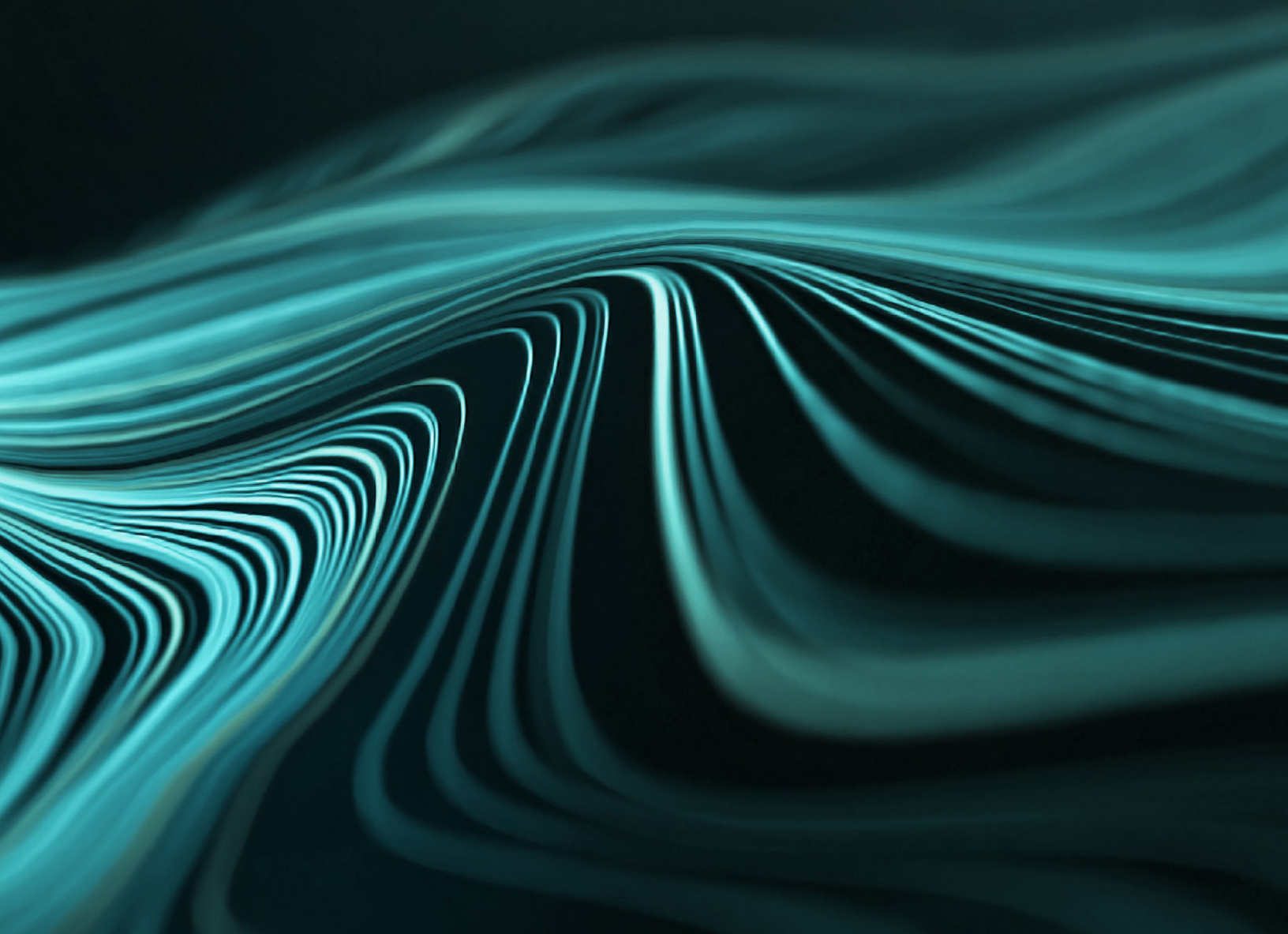


SOLUTION BRIEF

Cribl Search™





THE CHALLENGE

Traditionally, IT and security teams looking to get answers from their data had to ship, ingest, and store the data prior to querying it, leading to less data visibility, higher costs, and more logistical complexity.



THE SOLUTION

Cribl Search performs federated “search-in-place” queries on any data in any format at any location, increasing the scope of analysis without requiring the cost or complexity of first shipping, ingesting, and storing the data.



THE BENEFITS

- Get access to data that you didn't have access to before
- Deploy a single, system-agnostic search capability for ease of use
- Reduce costs and people hours needed for dedicated staff to manage each proprietary search tool
- Allows concentrated search results to be pushed back into existing analytics systems or stored for forensics or audit purposes
- Remove the mental and operational overhead of determining what to do with your data

SOLUTION BRIEF

Cribl Search™

Cribl Search performs federated “search-in-place” queries on any data in any format at any location, increasing the scope of analysis without requiring the cost or complexity of first shipping, ingesting, and storing the data.

The Challenge

Over 64 ZB of data was created in 2020, but enterprises are utilizing less than 2% of it. The vast majority of data goes unseen and unused because it's expensive and impractical to search data. Think about it: You've got to collect the data in question, pay to move and store it somewhere, and then query that data – all while praying to the deity of your choice that you find the needle in the haystack.

On top of all of that, tools today struggle with performing universal queries. Federated search isn't a new concept, but many leading search technologies are still limited to effectively querying data stored in a single vendor. Teams need a vendor-agnostic way to cost-effectively query their data regardless of where it lives.

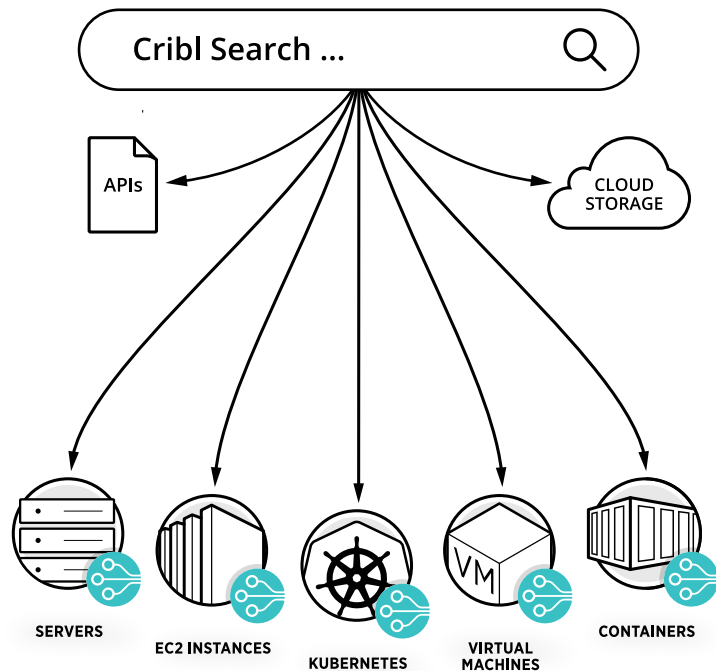
The Cribl Solution

Cribl Search performs “search-in-place” queries on any data, in any format, wherever it is — at the edge, in an observability lake, or even from an API endpoint. This increases users' scope of analysis without needing to ship, ingest, and store the data first, giving them relevant, valuable data that's only routed for further analysis if necessary.

Cribl Search leverages federated search, enabling users to query multiple data sources at once while presenting the results in a single, unified interface. Search gives you a painless and cost-effective way to query your data, so you get the insights you need at scale.

Cribl Search comes with out of the box integration with the other Cribl Suite products as well as As Amazon S3, Amazon Security Lake, Azure Blob, Google Cloud Storage and other compliant data stores. Additionally Search support searching on API Endpoints, with many default configurations. Integration with Cribl Stream and Edge allows routing, shaping and searching of data between the 3 systems. Cribl Edge also enables direct teleporting from Search results ,directly into endpoints for additional investigation.

CRIBL SEARCH'S VENDOR-AGNOSTIC APPROACH TO FEDERATED SEARCH STREAMLINES COSTS AND ENSURES YOUR TEAM HAS TIME TO WORK ON WHAT REALLY MATTERS.



Facets of Cribl Search

GET VISIBILITY INTO DATA YOU DIDN'T HAVE ACCESS TO BEFORE

The more data you have, the more difficult it gets to see it all. Depending on where that data lives, you may not be able to get to the data you need to query. Cribl Search gives teams the power to collect, process, and ask questions of data anywhere – whether it's in flight, in an observability lake, or at the edge.

EASILY SEARCH DATA ACROSS MULTIPLE VENDORS IN A SINGLE INTERFACE

Incumbent search vendors often have limitations on the number of tools they can query across. Administrators and developers then have to create dashboards to holistically evaluate the results, taking away time they could be spending on strategic initiatives. Cribl Search gives teams the power of federated search, enabling users to query multiple data sources at once and bring the results together into a single user interface.

RIGHTSIZE COSTS AND OPTIMIZE PEOPLE HOURS ASSOCIATED WITH PROPRIETARY SEARCH TOOLS

Data logistics is expensive and time-consuming. Asking questions of your data is pay to play: Pay to collect, pay to store, and pay per query. And executing on all that is often complex, requiring extensive people hours and specific staff experience with proprietary tools. Cribl Search's vendor-agnostic approach to federated search streamlines costs and ensures your team has time to work on what really matters.

REMOVE THE MENTAL AND OPERATIONAL OVERHEAD OF DETERMINING WHAT TO DO WITH YOUR DATA

When you're using legacy tooling or otherwise need to collect, store, and query using multiple platforms, you've got to ask a lot of questions. What source will this data be collected from? What's the best way to collect it? Once I've got it, where should I store it? How much will I be charged by this other tool per query? Cribl Search takes away the mental and operational overhead of figuring out what to do with your data. Use a single tool to query data wherever it lives, reducing stress, costs, and complexity.

CRIBL SEARCH GIVES
TEAMS THE POWER TO
COLLECT, PROCESS, AND
ASK QUESTIONS OF DATA
ANYWHERE – WHETHER
IT'S IN FLIGHT, IN AN
OBSERVABILITY LAKE, OR
AT THE EDGE.

Summary

The majority of data created goes largely underutilized, leading to decreased data visibility. It's also expensive and impractical to search all data: You've got to collect, store, and index it first. Additionally, many leading search technologies are still limited to effectively querying data stored in a single vendor.

Cribl Search is a vendor-agnostic analytics tool that performs 'search-in-place' queries, enabling search of multiple data sources at once while still presenting the results in a single unified interface. When teams use Cribl Search, they:

- *Get access to data they didn't have access to before*
- *Deploy a single, system-agnostic search capability for ease of use*
- *Reduce costs and people hours needed for dedicated staff to manage each proprietary search tool*
- *Remove the mental and operational overhead of determining what to do with your data*

Cribl Search: From petabytes to insights.

To get started today, [click here](#) to access or create a Cribl.cloud account. Learn more about the advantages of Search [in this blog](#). The [Cribl Slack Community](#) is also a great place to connect with leaders from other teams.

ABOUT CRIBL

Cribl makes open observability a reality for today's tech professionals. The Cribl product suite defies data gravity with radical levels of choice and control. Wherever the data comes from, wherever it needs to go, Cribl delivers the freedom and flexibility to make choices, not compromises. It's enterprise software that doesn't suck, enables tech professionals to do what they need to do, and gives them the ability to say "Yes." With Cribl, companies have the power to control their data, get more out of existing investments, and shape the observability future. Founded in 2018, Cribl is a remote-first company with an office in San Francisco, CA. For more information, visit www.cribl.io or our [LinkedIn](#), [Twitter](#), or [Slack](#) community.

©2023 Cribl, Inc. All Rights Reserved. 'Cribl' and the Cribl Flow Mark are trademarks of Cribl, Inc. in the United States and/or other countries. All third-party trademarks are the property of their respective owners. Updated 7/2023.