>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.

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.

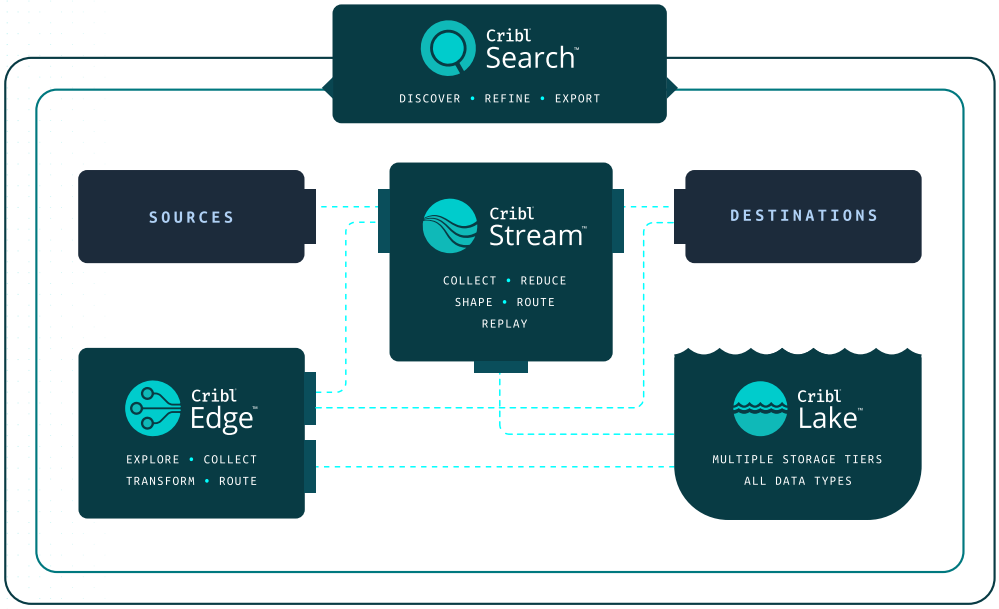
The challenge .

Data volumes — and the number of data sources — are growing year over year, but enterprises are utilizing less and less of it, in some cases 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. Security and IT teams need a vendor-agnostic way to cost-effectively query their data in place,increasing increase efficiency and improving SOC outcomes.

The Cribl Solution.

Cribl Search is an innovative new approach to finding and accessing data regardless of where it is landed and in any format or wherever it is located — at the edge, in a data 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's vendor-agnostic approach to federated search streamlines costs and ensures your team has time to work on what really matters.

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 Cribl's entire suite of products as well as Amazon S3, Amazon Security Lake, Azure Blob, Google Cloud Storage, AWS OpenSearch, and other compliant data stores. Additionally, utilize Search on API endpoints, with many default configurations as well as a user defined generic REST collector. as well as a user defined generic REST collector. Integration with Cribl Lake provides a turnkey data lake solution that enables organizations to easily store, manage, enforce policy and search data. Cribl Lake leverages open formats — no pre-defined schema required, unifies security with rich access controls, and centralizes access to all IT and security data. Cribl handles the heavy lifting so data can easily be stored, searched and routed to the teams and tools that need it. Integration with Cribl Stream and Edge provides additional routing, shaping, and searching of data between the 4 systems and searching of data between the four products. Cribl Edge also enables direct teleporting from Search results, directly into endpoints for additional investigation.

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 access the data you need to query. Cribl Search gives IT and Security teams the power to collect, process, and ask questions of data anywhere — whether it's in flight, in an data 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.

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.

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 or where to store 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.

Search Packs allow you to accelerate on-boarding and time-to-value.

Packs are predefined 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. Packs also provide reference examples that customers can inspect, reverse-engineer, and leverage to meet specific organizational requirements. Packs can be downloaded from our repository and implemented within your Search instances. Users can also create new Packs to easily share functionality with other users and teams. Packs are the fastest way to maximize the value of your Search investment.

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: getting started.

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