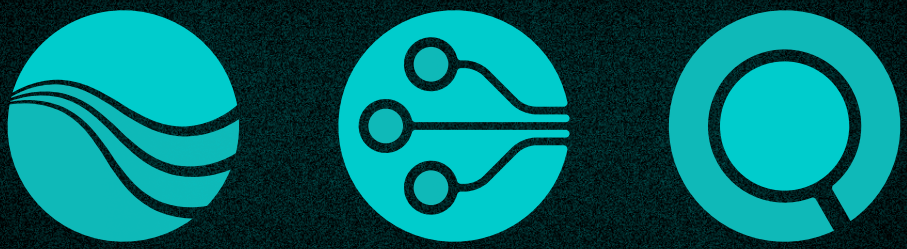
Cribl

SOLUTION GUIDE

Cribl Product Overview



SOLUTION GUIDE

Cribl Product Overview

DOCUMENT PURPOSE

This solution guide provides a holistic view of the Cribl solution, and how it enables open observability for teams. Read on for an overview of the solution's features, key capabilities, benefits, and deployment options.

Executive Summary

Every organization has to deal with a myriad of challenges: scaling to keep pace with data growth, increasing cyberthreats, flat budgets, and a dearth of talent. In the face of these challenges, operations teams have been forced to make compromises in what data they deliver to which analysis tools.

But what if you could make choices without compromising? What if you could unlock the value of all of your data no matter how fast it grew and deliver it in any format to any tool that needs it? What if you knew the exact best time to visit the restroom during a movie at the theater? (Kidding — you're on your own here.) What if this could actually be done without busting your budget?

The Cribl suite of products puts you back in control of your data, giving you the power to choose what is best for your organization, the control to get the data where you want, and the flexibility to put it in any format you need on the fly.

Solution Overview

Introduction

The Cribl solution enables an open observability architecture that combines data collection, routing, processing, and analysis for ultimate visibility and control.

Solution Architecture

The figure below gives a bird's eye view of Cribl's solution architecture. Cribl Stream and Edge make it a breeze to collect, process, and deliver observability, security, or telemetry data in real time to wherever you need it. Use out-of-the-box ad hoc data collection capabilities to get data from your lakes to your analytics tools, and perform federated search-in-place queries with Cribl Search to increase the scope of analysis — enabling compliance and insights.

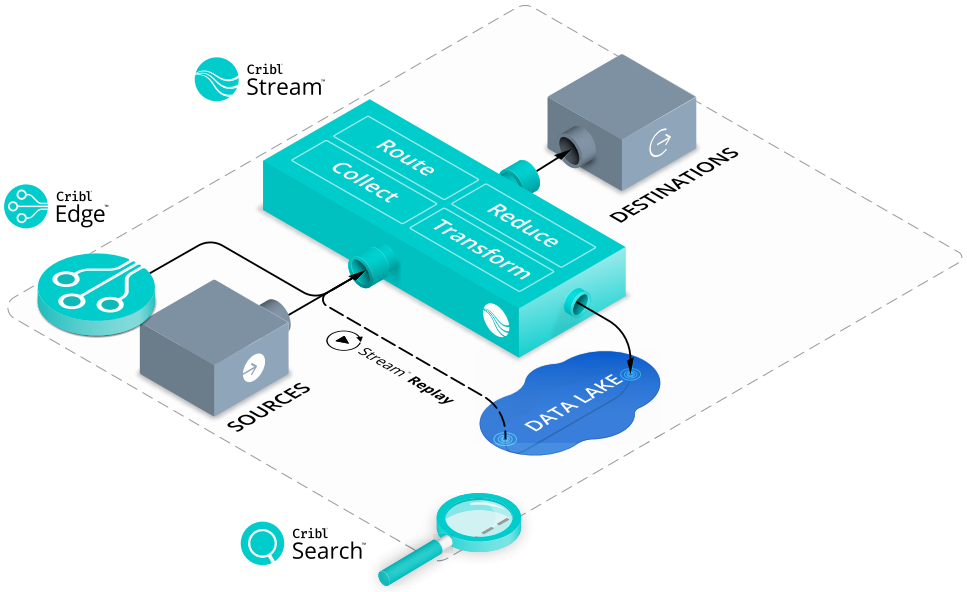


FIGURE 1
High-level solution architecture.

Solution Benefits

FLEXIBILITY TO ELIMINATE TOOL LOCK-IN

Choose the best vendor tool(s) without requiring new agents or collectors.

SIMPLIFY OBSERVABILITY DATA ENGINEERING

Easiest way to get data in, visualize data flows, and replicate functionality.

COMPLETE CONTROL & CHOICE OVER YOUR DATA

Route data where it has the most value. Control access to sensitive data.

OBSERVE MORE

Search data in place, only forward useful data tailored to organizational needs. Route data to multiple destinations and maintain full fidelity data in inexpensive object storage.

STRETCH YOUR INVESTMENT

Optimize costs and enable experts to spend time adding value — not managing infrastructure.

Products

The Cribl solution includes the following suite of products:

CRIBL STREAM

Cribl Stream is an observability pipeline that gives you the flexibility to route, shape, restructure, and enrich data from any source to any destination without adding new agents. Gain control over your data and simplify your observability efforts. Instrument everything, analyze more data, and pay less.

CRIBL EDGE

Cribl Edge is a highly-scalable edge-based data collection system for logs, metrics, and application data that enables administrators to reliably collect and process logs, metrics, and application data in real time from Windows or Linux machines, apps, and microservices and deliver them to any supported destination.

CRIBL SEARCH

Cribl Search is a vendor-agnostic analytics tool that enables teams to perform 'search-in-place' queries for more cost-effective data utilization, whether that data is at the edge, in flight, in an observability lake, or within existing systems.

Diagrams

The below diagrams give closer looks at the processing and transformation options that Cribl Stream and Cribl Edge provide internally. Sources collect data, and get it to Destinations via QuickConnect or Routes, which manage data flowing through Pipelines. Additionally, users can transform and analyze log events in any destination with Cribl Search.

Note: *Cribl Stream may serve as an intermediary destination for Cribl Edge.*

FIG.02
Cribl Stream basic solution architecture.

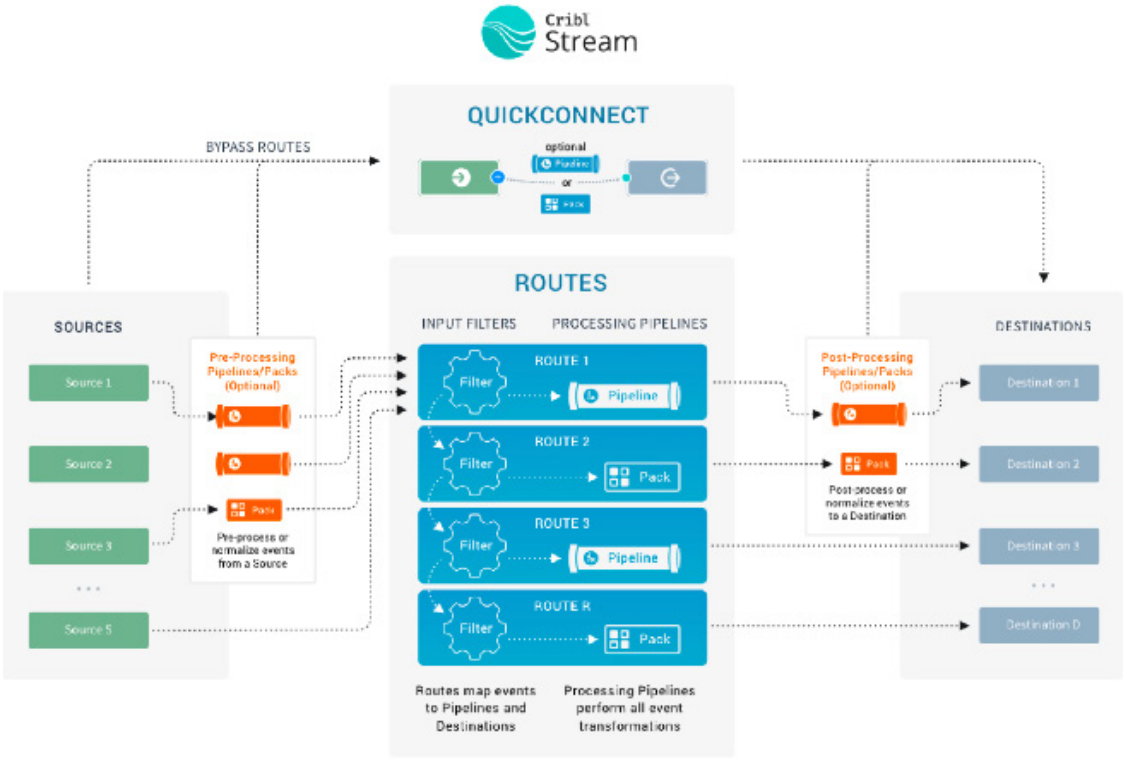


FIG.03
Closer look at a single Stream Worker (instance).

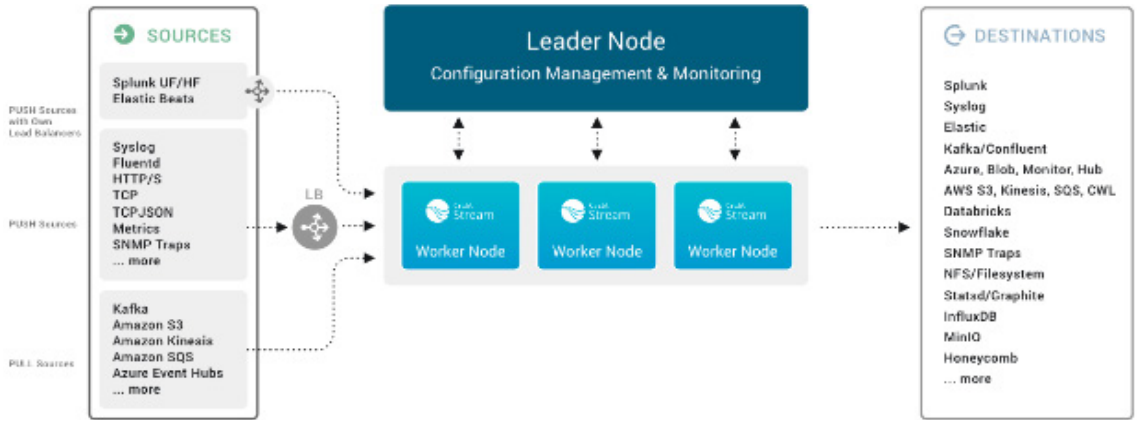


FIG.04
Cribl Stream scales up to meet enterprise needs in a distributed deployment.

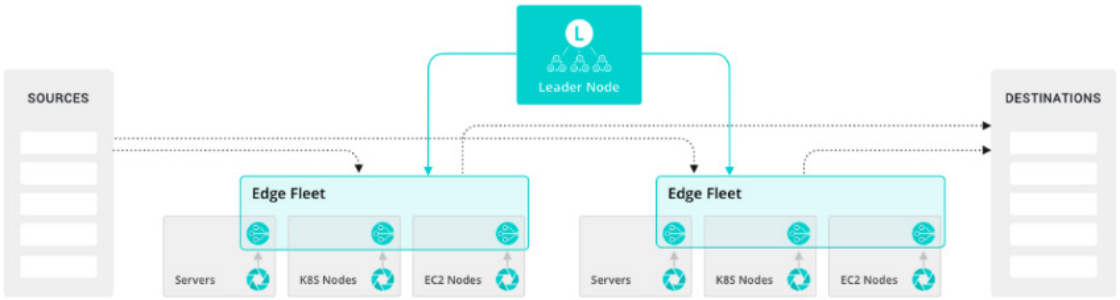


FIG.05
Cribl Edge basic solution architecture. Edge processing, management, and receivers.

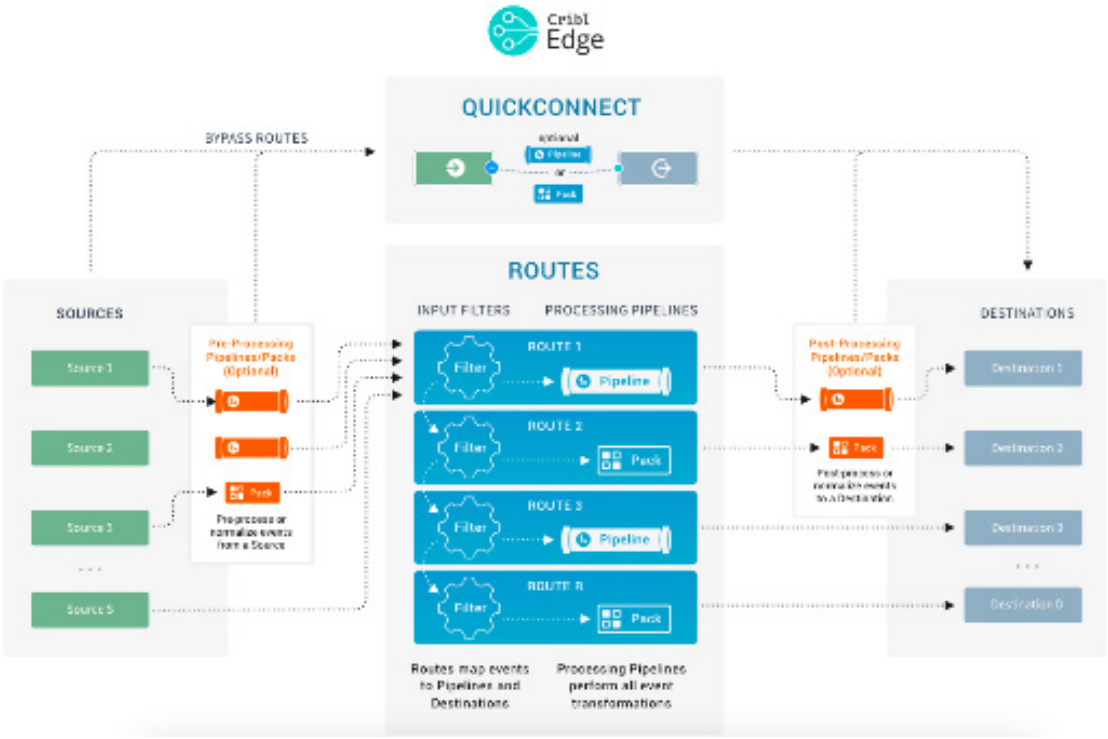


FIG.06
Double-click into a single Edge node.

Key Capabilities

EXPLORE DATA FIRST, THEN COLLECT

The Cribl solution leverages the power of Edge and Stream to explore logs, metrics, and application data at their egress points, giving you the option to dive into the data before deciding to collect and process it. Collect logs, metrics, and application data from any source at unprecedented scale — and even schedule batch collection from multiple APIs. Use ad-hoc data collection to recall data from your observability lake, and replay it to your analytics tools.

COST-EFFECTIVE ROUTING AND PROCESSING WHEREVER YOU NEED IT

The Cribl solution enables data reduction, transformation, and routing at the edge, providing more flexibility and lowering costs for forwarding and storing data. Forward data to Cribl Stream for additional processing or land it in the destination of your choice.

A "SEARCH THEN FORWARD" APPROACH

Cribl Search rounds out the solution with its search-in-place query capabilities that can federate searches across multiple data types and multiple data stores, prior to collecting and storing the data. Eliminate risk and uncertainty by querying data wherever it lives — at the edge, moving through an observability pipeline, stored in a data lake, or kept in TSDBs or log stores.

Overall, Cribl provides more data choice and flexibility. When organizations use Cribl to route data where it has the most value, complex projects like scaling with multiple tools or infrastructure consolidation become a lot easier. Cribl's end-to-end observability solution enables teams to easily control access to or sanitize sensitive data in flight, reduce security risk, and support compliance efforts, giving users better data visibility and reliable analytics while making the most of budgets for licensing, hardware, storage, and people.

Solution Deployment

BEFORE YOU DEPLOY: KEY CONSIDERATIONS

Before you get up and running with the Cribl suite of products, you need to determine the type of deployment that would best fit in your environment. Here are a few things to consider that will help you in your deployment planning:

- ***Amount of Data Ingest:*** *This is defined as the amount of data planned to be ingested per unit of time. How many MB, GB, or TB/day?*
- ***Amount of Data to Be Collected at the Endpoint:*** *What amount of that data is planned to be ingested at the endpoint per unit time?*
- ***Amount of Data Processing:*** *This is defined as the amount of processing that will happen on incoming data. Are there a lot of transformations, regex extractions, parsing functions, field obfuscations, etc.?*
- ***Routing and/or Cloning:*** *Is most data going to a single destination, or is it being cloned and routed to multiple places?*
- ***Deploying Onto Servers with No Internet Access:*** *Do you need to accommodate air-gapped on-prem servers (i.e., servers with no internet access)?*

Once you understand these key points and answer the questions above, it'll be easier to figure out which deployment is the best fit for your use case.

TYPES OF DEPLOYMENT

- *Use* **Single-Instance Deployment** *when incoming data volume is low, and/or amount of processing is light. For guidance, check out our* **Getting Started Guide***.*
- *Use* **Distributed Deployment** *to accommodate increased load. (See* **Sizing and Scaling** *for detailed guidance. See* **Bootstrap Workers from Leader** *to streamline Workers' deployment via scripting.) For help, take a look at our* **Distributed Quick Start***.*
- *Use Cribl.Cloud to quickly launch a Cribl-hosted deployment of the combined Cribl solution (Stream, Edge, and Search). With this option, Cribl assumes responsibility for provisioning and managing all infrastructure, on your behalf.*

RECOMMENDED SOLUTION DEPLOYMENT OPTION: CRIBL.CLOUD

The Cribl.Cloud platform quickly spins up all Cribl products — Stream, Edge, and Search — in just a few minutes. This deployment option puts the Leader and the Worker Node in Cribl.Cloud, where Cribl assumes responsibility for managing the infrastructure, simplifying deployment and adding flexibility. (If needed in the future, you can expand this to a hybrid deployment of your choice with any desired complexity.) To get started, check out our **Launch Guide** and sign up on the **Cribl.Cloud** portal.

ADDITIONAL RESOURCES

- Cribl Documentation
- Getting Started Guide
- Distributed Quick Start
- Launch Guide
- Cribl Community
- Cribl Support
- Cribl University
- Cribl Curious
- Self-Guided Trials
- Cribl Github Repos
- Docker Hub

Summary

Let's face it: Running an effective observability practice is starting to seem impossible. Data volumes are growing astronomically, leading to higher licensing expenses, rising infrastructure costs, and data retention.

Business needs are changing too, and they're getting more complex. Not only does security continue to be a concern, but companies also need to make sure they can move with the market while maintaining the data visibility they need for effective analysis. Proprietary tool sprawl can make it hard to get data from one place to another or use data sets across teams and platforms.

When you simplify data flow with an observability pipeline and introduce top-tier search capabilities into your approach, you regain choice and control over all your data.

Cribl's end-to-end observability solution combines data collection, routing, processing and analysis for ultimate data visibility and control – while reducing costs and complexity. Deployable in the cloud, on-prem, or using a hybrid approach, the Cribl solution:

- *Leverages the power of Edge and Stream to explore logs, metrics, and application data at their egress points, giving you the option to dive into the data before deciding to collect and process it.*
- *Enables data reduction, transformation, and routing at the edge, providing more flexibility and lowering costs for forwarding and storing data. Forward data to Cribl Stream for additional processing or land it in the destination of your choice.*
- *Eliminates risk and uncertainty with search-in-place query capabilities that can federate searches across multiple data types and multiple data stores, prior to collecting and storing the data.*

The fastest way to get started with Cribl is in the cloud! The Cribl.Cloud platform quickly spins up the Cribl solution — including Stream, Edge, and Search — in just a few minutes. To get started, check out our **Launch Guide** and sign up on the **Cribl.Cloud** portal.

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.