Cribl
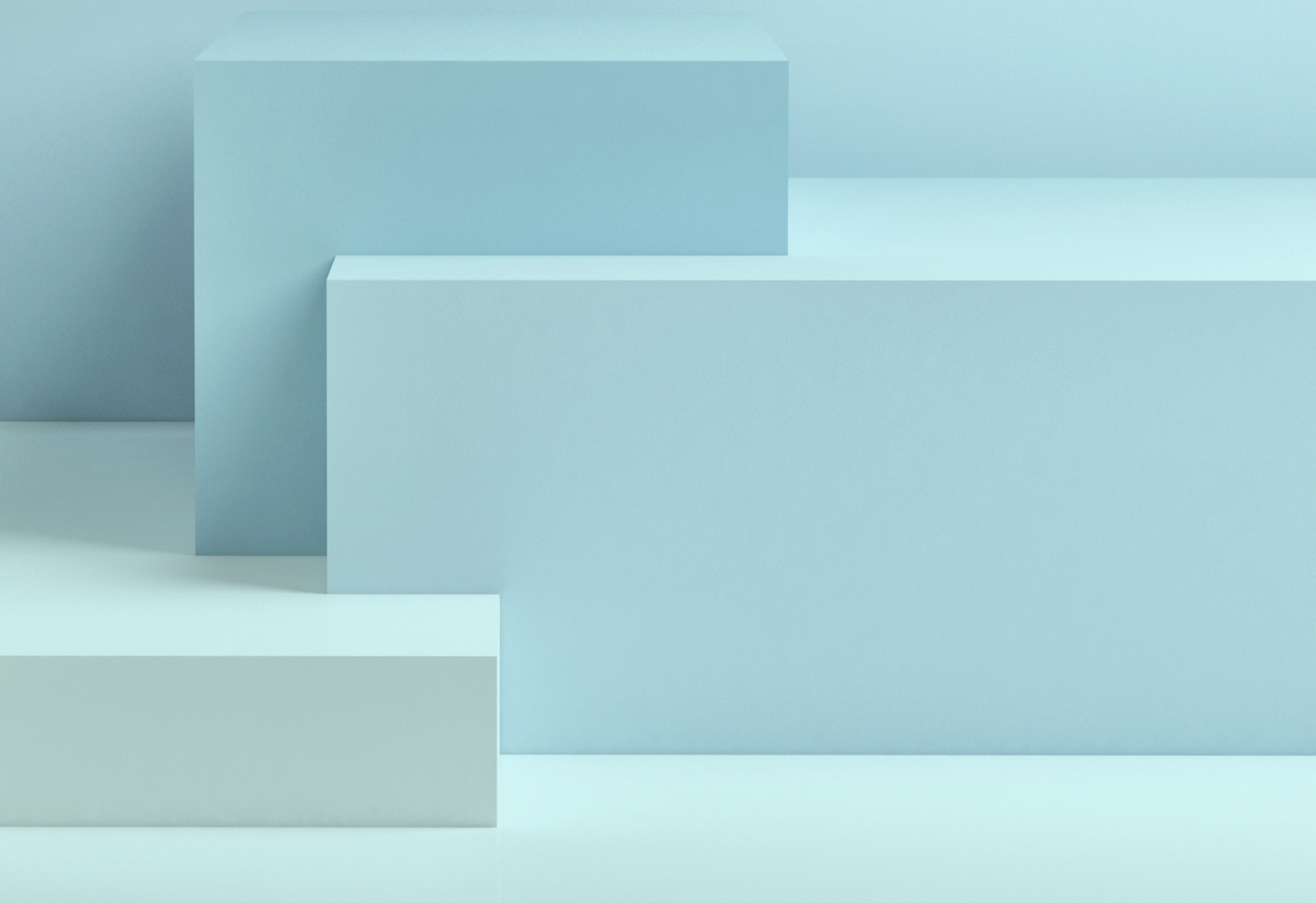
Bolster Data Security and Performance with Cribl Stream™ and CrowdStrike Falcon Data Replicator

THE CHALLENGE

Customers want a way to further optimize their CrowdStrike Falcon Data Replicator data prior to sending it to their logging or SIEM platforms.

THE SOLUTION

Cribl Stream can consume CrowdStrike FDR data and send it to any destination, log or SIEM platform. Route data to the best tool for the job by translating and formatting data into any tooling scheme you need.

THE BENEFITS

- Simplify collection data by formatting into any tooling schema

- Route to multiple destinations, including low-cost storage locations

- Optimize FDR data, reducing infrastructure budget and improving performance of analytical tools

- Enrich or mask FDR data in-flight

SOLUTION BRIEF
—

Bolster Data Security and Performance with Cribl Stream™ and CrowdStrike Falcon Data Replicator

Together, Cribl Stream and CrowdStrike Falcon Data Replicator gives customers visibility, flexibility, and control over data volumes.

The Challenge

Traditional security tools struggle to adapt to the new world of cyber threats. To keep up with the growing daily threats, understaffed security teams need new cloud-delivered solutions and tactics focused on consistently and repeatedly generating attack resolutions. Environments are growing in complexity as many teams deal with increasing data volumes, add new platforms, and incorporate new workflows to meet regulatory requirements. As threats evolve, teams need the flexibility to get data into multiple tools from multiple sources, safely integrate all their security tools, and deploy new use cases.

The Solution

Cribl Stream provides an out-of-the-box solution that easily complements CrowdStrike Falcon Data Replicator (FDR), allowing it to be sent to any destination, log or SIEM platform. FDR provides your SOC with actionable insights to improve performance by seamlessly collecting events in near real-time from your endpoints, cloud workloads, and identities, leveraging the Falcon platform's single, lightweight agent. The Cribl integration with FDR not only provides superb visibility into your data flow but Cribl's observability solution also eliminates custom scripts, scheduling, and downloaded file maintenance, simplifying your data management and minimizing manual tasks. This solution removes the manual effort of sifting through large volumes of data, minimizes data hosting and management costs, and frees up your team to focus on critical security incidents.
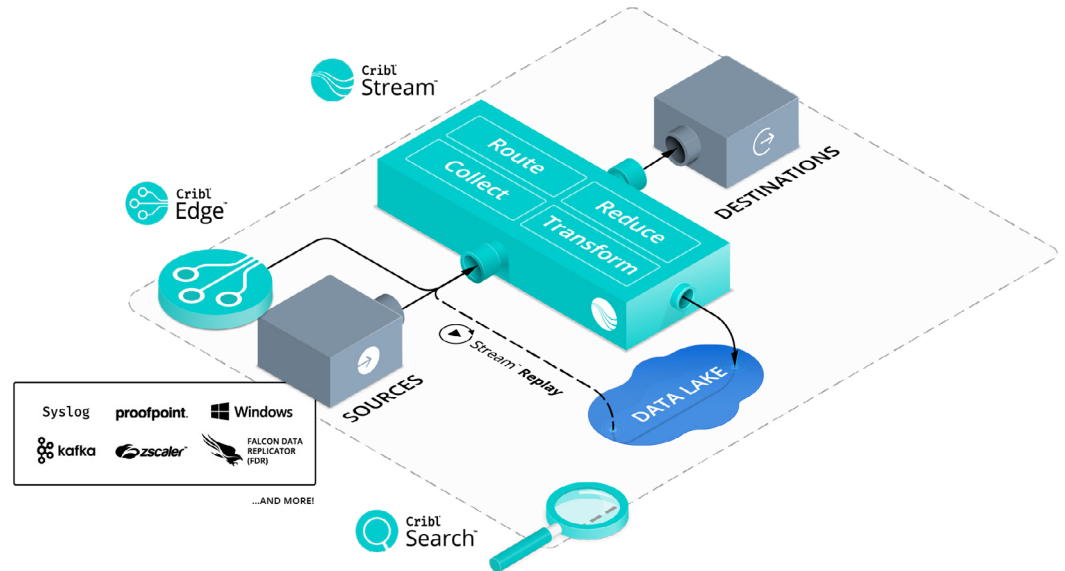
The Benefits of using CrowdStrike with Cribl's Observability Solution

SIMPLIFY COLLECTION DATA FOR FDR

Stream can translate and format data into any tooling schema, meaning you can collect all of your data once and repurpose it for any destination. This process reduces the duplication of data ingestion and allows you and different teams to pick the best analytics solutions. Customers who have an existing log collection or aggregation tier system can route the data into FDR while not impacting their existing solution. Stream is also vendor agnostic. This gives customers the flexibility to collect and process observability data in real time and deliver them to Stream or FDR.

ROUTE DATA TO MULTIPLE DESTINATIONS

Routing data to the right tools and destinations gives you the flexibility to optimize your observability and security efforts. Cribl Stream powers these efforts by helping you get all of your data into the destinations where it generates the most value including low-cost storage locations like S3. Different departments can choose different analytics environments without having to deploy new agents or forwarders.

OPTIMIZE FDR DATA

Crowdstrike FDR logs are rich with data and Stream helps optimize the volume by trimming unused or unwanted data. CrowdStrike customers can also utilize Cribl's Packs framework which allows organizations and communities of data engineers to build and share configuration models. The CrowdStrike FDR Pack helps customers reduce up to 80% of logs. Reducing the volume of data can help control license compliance, reduce infrastructure budget, and improve performance of analytical tools.

ENRICH OR MASK FDR DATA

Cribl Stream brings top-tier enrichment to CrowdStrike customers, allowing you to enrich or mask logs in-flight. CrowdSrike customers can leverage Cribl Stream's out-of-the-box Mask function to mask or obfuscate data in motion. Put simply, organizations can encrypt sensitive data in real time before it is forwarded to and stored at a destination, ensuring anonymity for every customer. During the migration process, Stream helps CrowdStrike users keep personally identifiable information safe, enabling deeper customer relationships.

Summary

Customers benefit from better protection, better performance and immediate time-to-value with CrowdStrike. Combined with Cribl Stream's observability solution and top-tier enrichment capabilities, customers can shape all of the data they need to make the best decisions about their environment. With a robust and easy-to-use GUI, Cribl and CrowdStrike enable customers to easily visualize and control data volumes.

With Cribl Stream, CrowdStrike customers can:

- *Simplify collection data by formatting into any tooling schema*
- *Route to multiple destinations, including low-cost storage locations*
- *Optimize FDR data, reducing infrastructure budget and improving performance of analytical tools*
- *Enrich or mask FDR data in-flight*

Together, Cribl observability solutions give CrowdStrike customers new resources to maximize their security efforts, allowing teams greater speed and agility to transform and route critical data.

To get started with Crowdstrike and Cribl Stream today, **click here** to download Stream. The **Cribl Slack Community** is also a great place to connect with leaders from other teams leveraging both CrowdStrike and Cribl.

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.