SOLUTION BRIEF

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

SOLUTION BRIEF

Perfect 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

CrowdStrike's Falcon Data Replicator replicates log data from your CrowdStrike environment to a stand-alone target. This target can be a location on the file system, or a cloud storage bucket. Scripts are used to download the files from the bucket but these scripts need to be scheduled to run, and the files downloaded need to be processed. These files also need to be managed and optimized to prevent filling the file system.

This solution works for Splunk but there are some issues:

- *Visibility into the download process is limited*
- *Timestamp identification needs to be configured*
- *Different source types are needed for each category of data*

The Solution

Cribl Stream provides an out-of-the-box solution that easily compliments CrowdStrike FDR data, allowing it to be sent to any destination or SIEM platform. Not only does it provide superb visibility into your data flow but Cribl's observability solution also eliminates custom scripts, scheduling, and downloaded file maintenance. A Stream pipeline helps optimize FDR by filtering out unwanted data, and can reserialize events by removing fields through configuration. Source types can easily be assigned to different categories of data, simplifying processing as well as making data much easier to use. Additionally, Stream gives the flexibility to configure timestamp extractions for each category of FDR events.

THE CHALLENGE

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

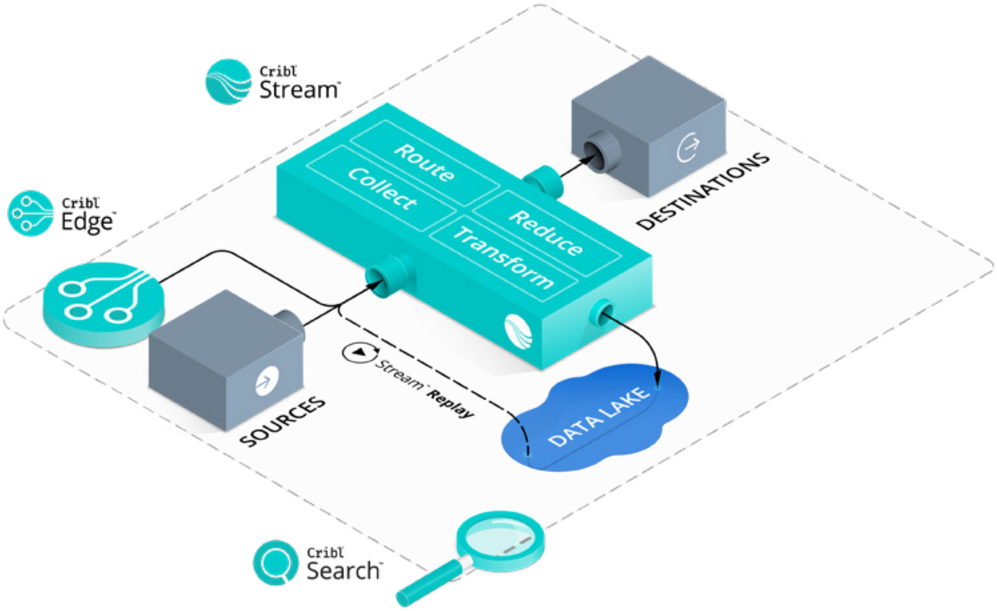
THE SOLUTION

Cribl Stream can consume CrowdStrike FDR data and send it to any destination 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

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.



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 2017, 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.