SOLUTION BRIEF

Cribl Stream and CrowdStrike Falcon Data Replicator (FDR) Integration

You rely on CrowdStrike Falcon for rich endpoint telemetry. But keeping all that data hot and searchable for years is expensive.

With Cribl Stream, you can export CrowdStrike Falcon Data Replicator (FDR) data, shape it, and send it where it delivers the most value, so you can meet long-term retention requirements and boost threat hunting without blowing up your budget.

The challenge

You need deep endpoint visibility to:

- Detect and prevent increasingly complex threats
- Align to frameworks like MITRE ATT&CK
- Support investigations and compliance

But more visibility means more data. That extra volume strains your SIEM and SOAR platforms, driving up:

- Ingest and storage costs
- Processing overhead
- Time to search and investigate

Keeping full-fidelity endpoint data in those analytics platforms for the long term quickly becomes cost-prohibitive.

The solution

CrowdStrike Falcon gives you detailed endpoint visibility and response capabilities. Falcon Data Replicator (FDR) exposes that data in an AWS S3 bucket within the CrowdStrike Security Cloud.

Cribl Stream:

- Securely retrieves data from FDR
- Parses, enriches, and shapes it to your needs
- Routes it to the right destinations

You can send high-value events to your SIEM or SOAR, full-fidelity data to a security data lake, and long-term archives to low-cost storage.
This lets you handle growing data volumes while optimizing how each dataset is used across your security analytics stack.

The benefits

- Collect data from CrowdStrike Falcon Data Replicator and route it to one or more destinations based on your analytics and retention needs.
- Send only the data you actually need for detection, investigation, and advanced threat hunting to SIEM and SOAR platforms to improve performance and control ingest costs.
- Enrich event data with device metadata from CrowdStrike FDR to give analysts more complete security context for faster, more accurate decisions.
- Use Replay in Cribl Stream to move data from your security data lake back into analytics platforms on demand, so you can run long-term investigations without keeping everything hot and indexed all the time.

The integration of Cribl Stream and CrowdStrike FDR data provides visibility into the below activities at the endpoint and more:

- Behavioral alerts
- Information about processes (create, listen, termination, modification)
- Commands and scripts run
- Registry modifications
- Domain Name Service (DNS) activity
- Netflow
- File activity (create, modify, delete)
- Scheduled task or start-up modifications
- HTTP activity

While these security-relevant event types are among the most important sources to the security and compliance organizations, the verbosity of the events is usually too taxing for most analytics platforms such as a SIEM. Cribl Stream provides the solution for satisfying long-term investigative and compliance requirements while also optimizing the data sent to the analytics platforms as needed.

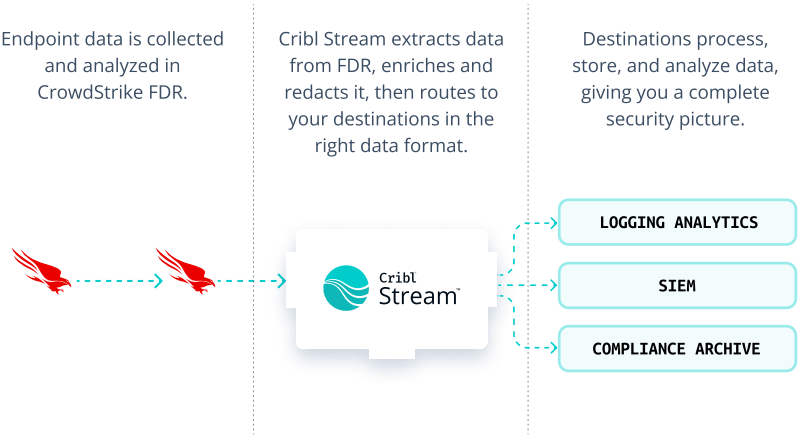
Cribl observability solutions gives CrowdStrike customers new resources to maximize their security efforts, allowing teams greater speed and agility to transform and route critical data.

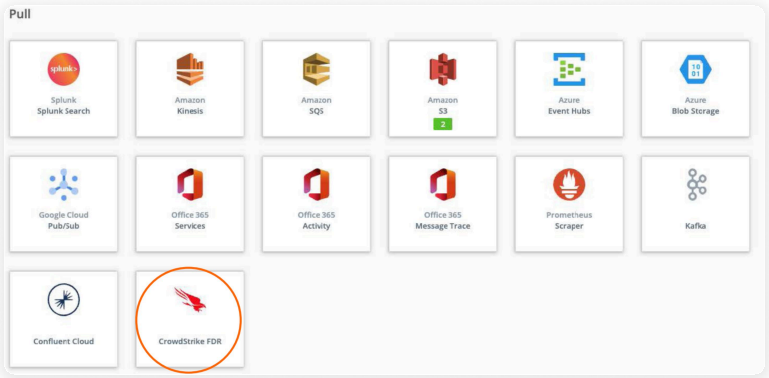
Integrating Cribl Stream with CrowdStrike FDR

It only takes a few minutes to configure Cribl Stream to retrieve data from CrowdStrike FDR. In summary, the steps you'll need to take are:

1. Configure Cribl Stream to pull data from the CrowdStrike FDR S3 bucket
2. Install the Cribl Pack for CrowdStrike FDR
3. Set up any data enrichment you want to perform
4. Configure your destinations

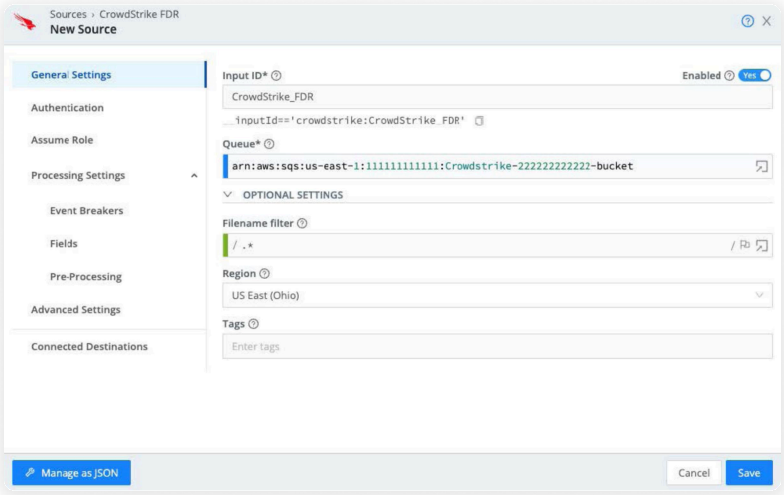
Let's get started.



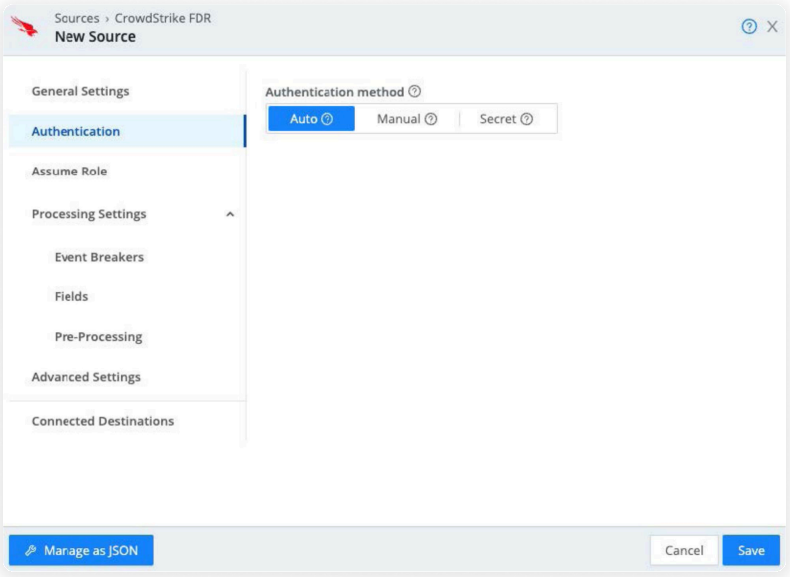


Step 1

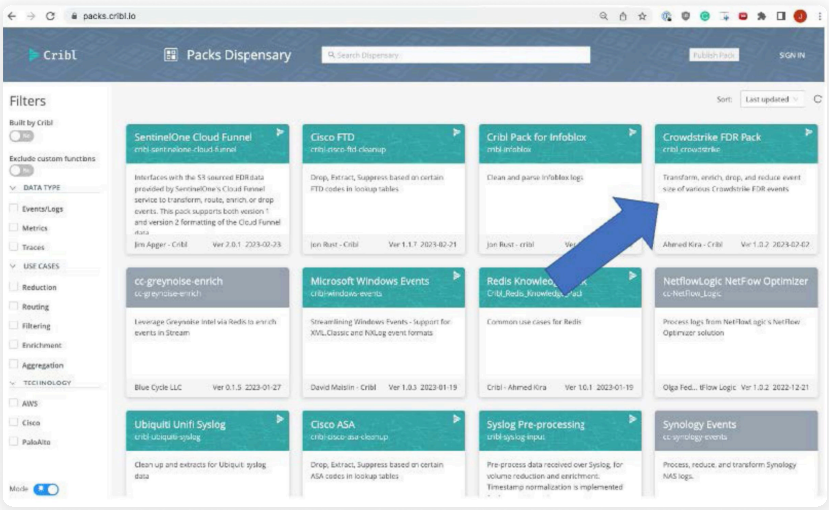
Configure the CrowdStrike FDR Stream source tile to pull data from the Falcon Data Replicator AWS S3 bucket

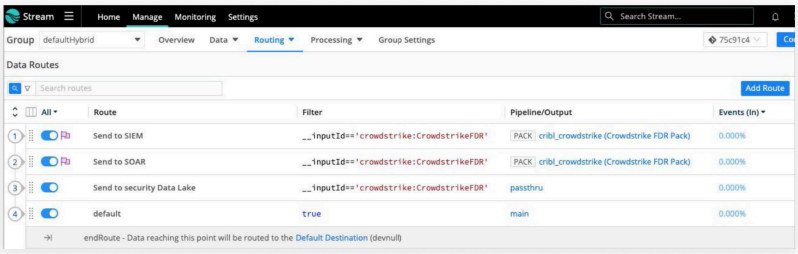


Provide an Input ID, the name, URL, or ARN of the SQS queue to read notifications from, then select the region from the dropdown.



Configure access to the bucket on the Authentication tab using AWS IAM policies or access/secret key pairs.





Step 2

Download and install the Crowdstrike FDR Pack from the Cribl Pack Dispensary to quickly transform, reduce, drop, or enrich data that will be routed to a security analytics platform.

Step 3

Configure destination tiles for your analytics platforms and security data lake then route data to those destinations.

The below example accomplishes the following:

- Filter events that were sourced from Crowdstrike FDR, route them through the Crowdstrike FDR pack, then send the optimized events to the SIEM.
- Filter events that were sourced from Crowdstrike FDR, route them through the Crowdstrike FDR pack, then send the optimized events to the SOAR platform.
- Route all events (filter=true) via the passthrough pipeline into the AWS S3 security Data Lake.

Cribl

The AI Platform for Telemetry

Learn more at cribl.io | Join our Slack community
Try Cribl Sandboxes | Follow us on LinkedIn and X

© COPYRIGHT 2026 CRIBL, INC. ALL RIGHTS RESERVED

SB-0074-EN-1-0626