>SOLUTION BRIEF_

Enable faster response and streamline network detection with Cribl and Corelight.

THE CHALLENGE

Forward-thinking enterprises that have turned to Corelight's open NDR platform for its ability to transform network traffic into faster, more useful data need an observability solution to match the scale and collect from multiple sensors, without blowing the budget.

THE SOLUTION

Cribl's Stream is an essential part of observability, providing a pipeline that works with all tooling, keeps costs down, and scales with any business — making it the perfect complement to Corelight.

THE BENEFITS

- Route from Corelight sensors to any destination, including object storage for long-term retention.
- Replay sensor data and Zeek logs AD HOC or on a schedule to your SIEM of choice.
- Reduce data volume while preserving insights and remaining compliant.
- Further enrich logs in flight with GeoIP data or DNS information.
- Filter and transform Corelight data into any mapping, including ECS and CIM.
- Seamlessly migrate to Corelight's open NDR platform from any provider.

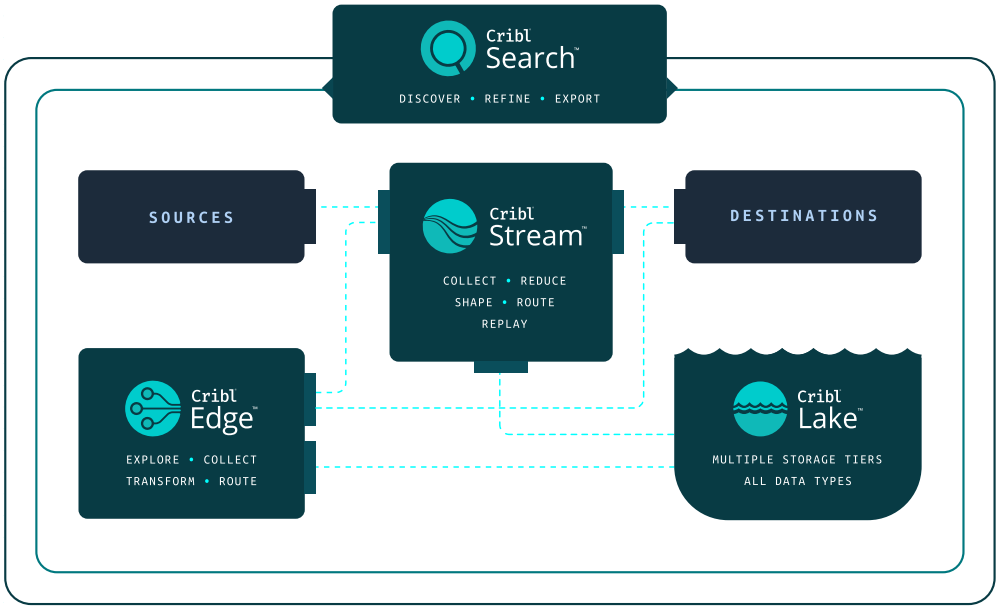
Together, Cribl's Stream and Corelight's response solutions and network detection enable data analysts at companies of all sizes to transform network traffic into the formats they need and offer the insights necessary for a quick response.

The power of Cribl and Corelight.

Monitoring network traffic is essential to security operations at many companies, regardless of size, but what do you do when you've got an ocean of Netflow logs flooding your SIEM? Enterprises that want to streamline network detection and enable faster response are turning to Corelight's open NDR platform to replace that low quality, "side-effect" network data with rich, protocol-comprehensive Zeek logs.

Corelight also provides appliance, cloud, software, and virtual sensors that are easily operated from a centralized location — Corelight's Fleet Manager — giving them one place to drill into specific sensor metrics and get insights enhanced by Corelight Collections.

Enterprises use Cribl Stream for similar reasons. Cribl Stream is a robust streams processing engine focused on centralized parsing and processing of event data. Take any event source and use Stream to route, reduce, reformat, enrich, or otherwise structure data intended for any destination These companies also need a cost-effective strategy for retaining logs long-term and a pain-free way to enrich data with additional information. At the same time, they need a solution that is reliable and scalable, regardless of the amount of data they have, the products they use today, or the tools they may turn to in the future.



Corelight has a great foundation of data enrichment capabilities out of the box. Stream enables even further enrichment of Zeek logs and other Corelight data, so you can shape all of the data you need to drive decisions about your environment.

The benefits of using Corelight with Cribl Stream:

Route from Corelight sensors to any destination, including object storage for long-term retention.

Send data from Corelight's appliance, cloud, software, or virtual sensors to the most effective destinations — including low-cost object storage for long-term retention. Route data to the best tool for the job — or all the tools for the job — by translating and formatting data into any tooling schema they require. Let different departments choose different analytics environments without having to deploy new agents or forwarders.

Replay sensor data and Zeek logs AD HOC or on a schedule to your SIEM of choice.

Cribl Stream is the best way to replay multiple data formats to your analytics tools. Use Stream as a universal receiver to collect from any Corelight source and schedule batch collection from multiple APIs, or recall Corelight sensor data from object storage (like Amazon S3), and "replay" those Zeek logs to analytics tools for later investigations with AD HOC data collection.

Reduce data volume while preserving insights and remaining compliant.

Stream can typically reduce 30% or more of ingested log volume to control costs and improve system performance. Corelight customers can easily eliminate duplicate fields, null values, and any elements that provide little analytical value using dynamic sampling. From the same interface, they can filter and screen events or aggregate log data into metrics for volume reduction at scale — all while keeping a full-fidelity copy in low-cost storage to replay if needed.

Further enrich logs in flight with GeoIP data or DNS information.

Corelight has a great foundation of data enrichment capabilities out of the box. Stream enables even further enrichment of Zeek logs and other Corelight data, so you can shape all of the data you need to drive decisions about your environment. Use Stream's built-in Lookup functions to add GeoIP or Ingest-time data to logs from any source in real-time as they arrive. Got a list of known good domains? Cribl Stream can leverage that list to filter out suspicious events on the fly.

Filter and transform Corelight data into any mapping, including ECS and CIM.

Corelight supports many different mappings, ensuring Corelight data can be applied to visualizations, dashboards, machine learning, and more. What about when you need to switch between them? With Stream, Corelight customers can transform data on the fly to different mappings, including ECS and CIM. In one fell swoop, they can filter out any data irrelevant to the new mapping or add additional information where needed.

With Cribl Stream, you can seamlessly migrate to Corelight from any provider — without worrying about dropping or losing data.

Redact Personally Identifiable Information (PII) from sensor and network data in real-time.

Corelight users can now 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. Stream helps Corelight users keep personally identifiable information safe, enabling deeper customer relationships.

Seamlessly migrate to Corelight's open NDR platform from any provider.

Because Cribl Stream is a universal receiver and router, new Corelight customers can smoothly and securely migrate workloads to a new environment — without worrying about dropping or losing data. The same approach works wonders for Corelight users looking to upgrade existing infrastructure or move over to Corelight's NDR platform from a competitor solution.

Summary.

On a quest for network detection and response (NDR) solutions that can scale with their business on all fronts, many companies have turned to Corelight. These same enterprises now need an observability tool to match: flexible, cost-effective, and reliable. Cribl Stream is an observability pipeline that provides the simplicity, flexibility, and control to work with any tooling, reduce cost of implementation, and perform well with even the largest amounts of data — making it the perfect complement to Corelight.

Together, Cribl's Stream processing engine and Corelight's network detection and response solutions enable data analysts at companies of all sizes to transform network traffic into the formats they need and offer the insights necessary for a quick response.

With Cribl Stream, Corelight customers can:

- Route from Corelight sensors to any destination, including collectors or object storage for long-term retention.
- Replay Corelight data ad hoc or on a schedule to your logging solution or SIEM of choice
- Reduce data volume while preserving insights and remaining compliant.
- Enrich Corelight logs in flight with GeoIP data or DNS information from known threat lists.
- Filter and transform Corelight data into any mapping, including ECS and CIM.
- Seamlessly migrate to Corelight from any provider.

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

ABOUT CORELIGHT

From the Acropolis to the edge of space, defenders have sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders. Corelight gives apex defenders the information and tools they need to successfully detect and respond to threats. Corelight is built on Zeek, an open-source, global standard technology. Zeek provides rich, structured, security-relevant data to your entire SOC, making everyone from Tier 1 analysts to seasoned threat hunters far more effective. Find out more at corelight.com.

ABOUT CRIBL

Cribl, the Data Engine for IT and Security, empowers organizations to transform their data strategy. Customers use Cribl's vendor-agnostic solutions to analyze, collect, process, and route all IT and security data from any source or in any destination, delivering the choice, control, and flexibility required to adapt to their ever-changing needs. Cribl's product suite, which is used by Fortune 1000 companies globally, is purpose-built for IT and Security, including Cribl Stream, the industry's leading observability pipeline, Cribl Edge, an intelligent vendor-neutral agent, Cribl Search, the industry's first search-in-place solution, and Cribl Lake, a turnkey data lake. Founded in 2018, Cribl is a remote-first workforce with an office in San Francisco, CA.

Learn more: www.cribl.io | Try now: Cribl sandboxes | Join us: Slack community | Follow us: LinkedIn and Twitter

SB-0043-EN-1-0524