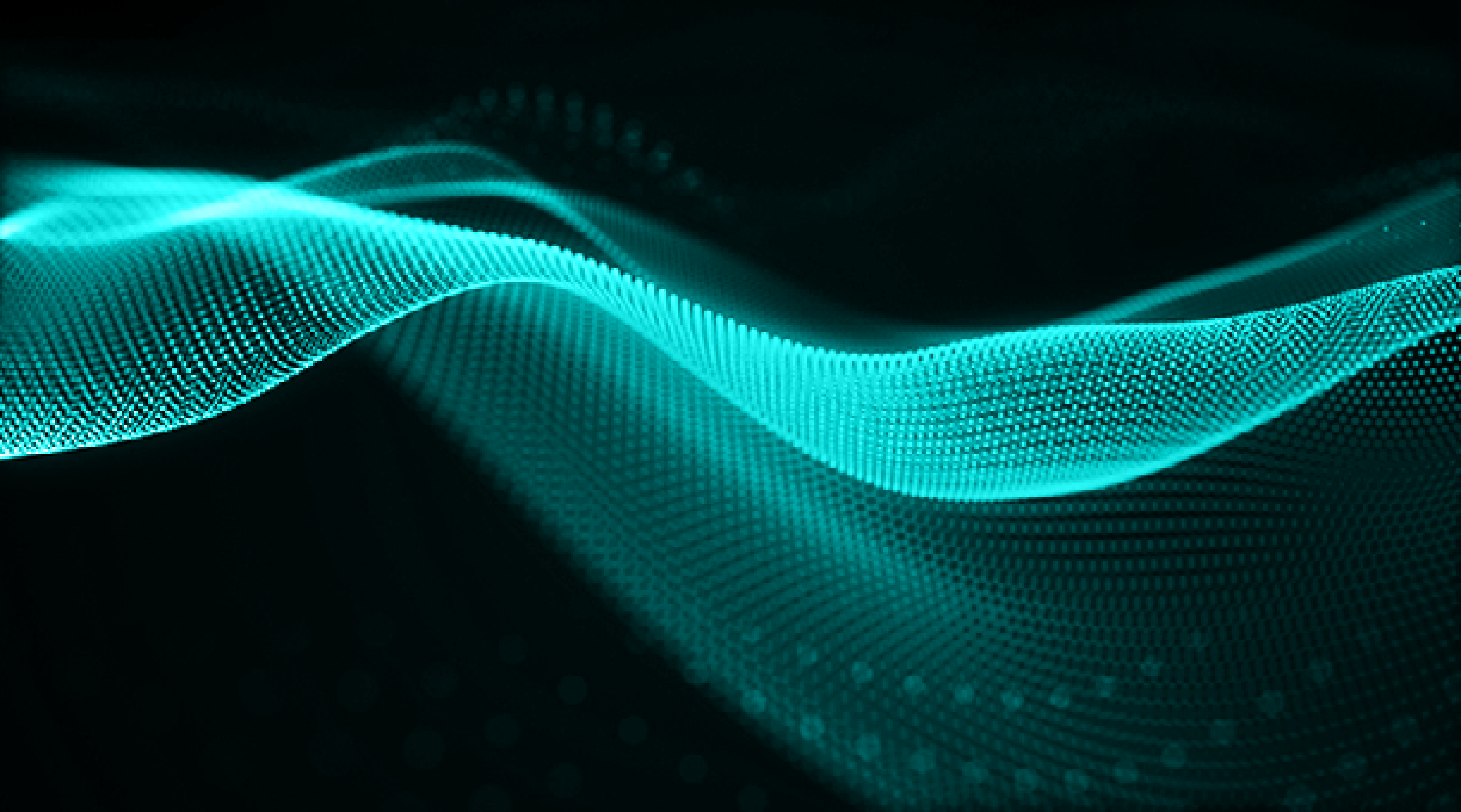
SOLUTION BRIEF

Streamline Network Detection and Enable Faster Response with Corelight and Cribl



SOLUTION BRIEF

Streamline Network Detection and Enable Faster Response with Corelight and Cribl

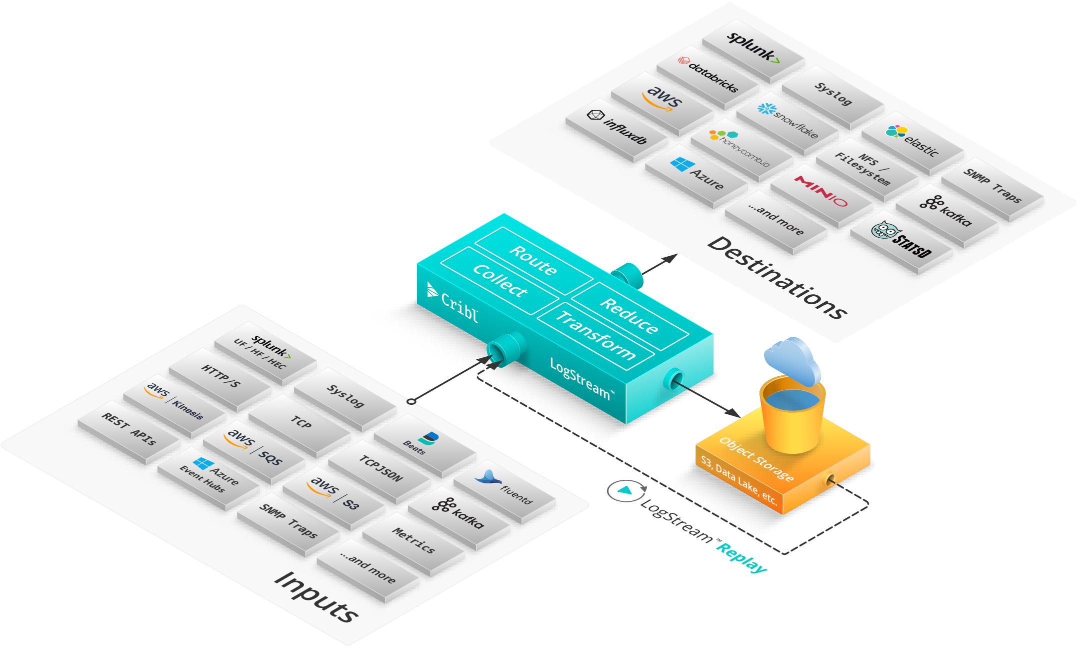
Together, Cribl's observability pipeline LogStream and Corelight's network detection and response solutions enable data analysts at companies of all sizes to transform network traffic into the formats they need and offer the insights necessary for a quick response.

The Power of Corelight and Cribl

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 LogStream for similar reasons. They need an observability pipeline with the flexibility to transform data into the formats needed to route to multiple tools from multiple sources without adding new infrastructure and agents. 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 an observability 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.



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 LogStream 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

The Benefits of using Corelight with Cribl LogStream

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 LogStream is the best way to replay multiple data formats to your analytics tools. Use LogStream 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

LogStream 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. LogStream 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 LogStream'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 LogStream can leverage that list to filter out suspicious events on the fly.

CORELIGHT HAS A GREAT FOUNDATION OF DATA ENRICHMENT CAPABILITIES OUT OF THE BOX. LOGSTREAM 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.

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 LogStream, 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.

REDACT PERSONALLY IDENTIFIABLE INFORMATION (PII) FROM SENSOR AND NETWORK DATA IN REAL TIME

Corelight users can now leverage Cribl LogStream'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. LogStream 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 LogStream 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.

WITH CRIBL LOGSTREAM, YOU CAN SEAMLESSLY MIGRATE TO CORELIGHT FROM ANY PROVIDER – WITHOUT WORRYING ABOUT DROPPING OR LOSING DATA.

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 LogStream 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.

With Cribl LogStream, 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*

Together, Cribl's observability pipeline LogStream 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.

To get started with Corelight and Cribl LogStream today, click here to download LogStream. 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 is a company built to solve data challenges and enable customer choice. Our solutions deliver innovative and customizable controls to route observability data where it has the most value. We call this an observability pipeline, and it helps slash costs, improve performance, and get the right data, to the right destinations, in the right formats, at the right time. Join the dozens of early adopters, including market leaders such as TransUnion and Autodesk, to take control and shape your data. Founded in 2017, Cribl is headquartered in San Francisco, CA. For more information, visit www.cribl.io or our LinkedIn, Twitter, or Slack community.