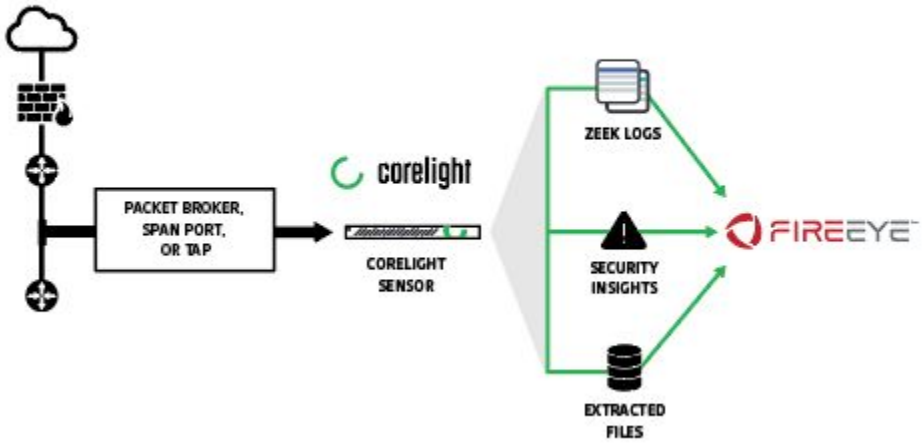
Joint Solution

Maximize network visibility and minimize response times with Corelight and FireEye

Incident responders and threat hunters can't do their job without first making sense of their environment. Corelight's rich network data pairs with FireEye to dramatically improve incident response and threat-hunting capabilities. While nearly all attacks must cross the network, common sources of network data (like Netflow records) lack critical details and often leave security operators in the dark. Using the power of open-source Zeek, Corelight comprehensively details network activity across 35+ protocols, transforming raw traffic into rich logs, extracted files, and custom-scripted insights.

The Corelight/FireEye solution:



The joint solution pairs deep network traffic analysis from Corelight with next generation SIEM, orchestration, and threat-intelligence capabilities from FireEye, allowing security professionals to accelerate their response to threats.

Corelight integrates with FireEye, streaming this rich network data to the powerful FireEye Helix security orchestration platform to deliver real-time, actionable insights into network traffic. FireEye intelligence enriches hundreds of relevant data types across dozens of protocols to help customers identify high-priority threats. The result: vastly superior capabilities for network threat detection, hunting, and response.

Pre-built FireEye Helix dashboards deliver security insights from Corelight logs

FireEye Helix dashboard showcasing Corelight and Zeek data

Corelight has created custom Helix dashboards that enable customers to:

- Effectively detect and respond to attacks
- Identify anomalies quickly
- Hunt for attackers using contextual data (beyond just alerts)

These dashboards can also be utilized for anyone leveraging Zeek, the open-source network security monitoring platform that underlies the Corelight technology. This additional context coupled with leading FireEye intelligence allows mutual customers to focus their energy on the threats that matter.

To learn more about the FireEye and Corelight integration, please visit either the FireEye Market **fireeye.market/vendors/corelight** or the Corelight website **corelight.com**.

Zeek provides the best security data from network traffic

Corelight solutions are built on a foundation of Zeek, the powerful and widely-used open source network analysis framework that generates actionable, real-time data for thousands of security teams worldwide.

Zeek extracts over 400 fields of data in real time directly from network traffic, covering dozens of data types and protocols from Layers 3 to 7, and includes data about TCP connections, SSL certificates, HTTP traffic, emails, DHCP, and more. The Zeek data logs are structured, interconnected, and organized specifically to provide more powerful threat-hunting capabilities to SOC/DFIR teams so they can investigate and resolve incidents faster.

Corelight Sensors—available in physical, cloud, and virtual formats—take the pain out of deploying open-source Zeek by adding integrations and capabilities that large organizations need. The Sensors operate out-of-band and use high-performance hardware along with a specialized version of the open-source Zeek network security monitor to ingest network traffic, transforming it into rich network logs and extracted files. Corelight Sensors' capabilities include:

- 25 Gbps+ of monitored traffic
- Hardware, cloud, or virtual appliance models
- A web-based sensor management GUI
- A comprehensive API
- On-box performance and health monitoring
- Dynamic file extraction
- Flexible export options, including data formats, filtering, and forking
- Shunting to handle elephant flows over 25 Gbps (AP 3000 only)
- Support from the creators and builders of Zeek

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovative security technologies, nationstate-grade threat intelligence, and world-renowned Mandiant® consulting. With this approach, FireEye eliminates the complexity and burden of cybersecurity for organizations struggling to prepare for, prevent, and respond to cyberattacks.

Defenders have always 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.

info@corelight.com | 888-547-9497