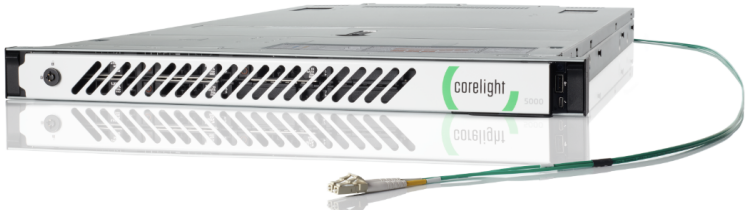

AP 5000 Sensor (100 Gbps)

High-throughput network insight

The AP 5000 reliably scales Zeek and Suricata to deliver high-fidelity network data to your analytics pipeline at industry-leading scale.

Plug-and-play, configure in 15 minutes

Corelight Sensors are zero maintenance and take only minutes to deploy: connect the traffic feed, specify where to send logs, alerts, and extracted files, and you're done. Get new features via automatic updates and enterprise support from Zeek's creators.

Tuned for enterprise performance and scale

Engineered from the ground up with keen attention to detail, Corelight Sensors are security-hardened and run a custom OS based on the Linux kernel. A specialized NIC provides the performance that large-scale deployments require, with built-in support for merging high-volume traffic feeds.

Next-level analytics

Behavioral analysis, machine learning, and signatures give Corelight customers comprehensive threat detection coverage across network vulnerabilities and attacks. The Corelight Labs team continuously validates our detections on live customer networks to ensure that the best analytic and machine learning models are used for a given security challenge. Continuous detection engineering from open source communities also gives Corelight customers crowd-sourced confidence to detect known threats and delivers immediate access to zero day detections.

The features you wish open-source had

Corelight has merged the power of Zeek and Suricata with a suite of enterprise features that dramatically improve usability, like an intuitive management UI, flow shunting, sensor health metrics, fleet management, and automated data export to Splunk, Elastic, Kafka, Syslog, S3, and more.

AP 5000 Sensor (100 Gbps): **Specifications**

The Corelight AP 5000 Sensor is designed for traffic analysis at speeds 100 Gbps and beyond:

- In high-volume data centers
- In Science DMZs
- In telecommunication networks

Zeek and Suricata deployment in a compact 1U sensor:

- Engineered for stability and performance, by the creators of Zeek
- 2 QSFP28 bays that support 2x100G, 2x40G, or 8x10G interface options in a powerful, specialized NIC
- Intuitive, 15-minute configuration, with a beautiful web app UI
- Data export to Kafka, Splunk, Elastic Search, SIEMs, syslog, Amazon Kinesis, Apache Avro, and SFTP
- Up to 100 Gbps of Zeek-only traffic monitoring
- Available shunting to improve performance in high volume or encrypted environments
- High performance and efficient file extraction
- Comprehensive REST API for configuration and monitoring
- Minimalist, custom OS optimized for secure operation
- Automatic updates and feature enhancements
- World-class support from the definitive Zeek experts included, additional support programs available
- For more info on Suricata support in Corelight Sensors, read this whitepaper.

Specifications

Size and weight	1U rackmount (17.1 x 29 x 1.75 inches), 47.4 lbs
Monitoring interface	2 QSFP28 modules. Support for optical modules at 8 x 10G, 2 x 40G or 2 x 100G
Management interface	2 x 1 Gbe LOM port 4 x 10 Gbe SFP28 ports
External connector	VGA, USB
Power	100-240 VAC 50/60 Hz redundant dual PSUs. Approximately 443W usage when idle and 852W usage at load
Operational mode	Out of band—fed by tap, span, or packet broker

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. On-prem and in the cloud, our open Network Detection and Response platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology.

info@corelight.com | 888-547-9497