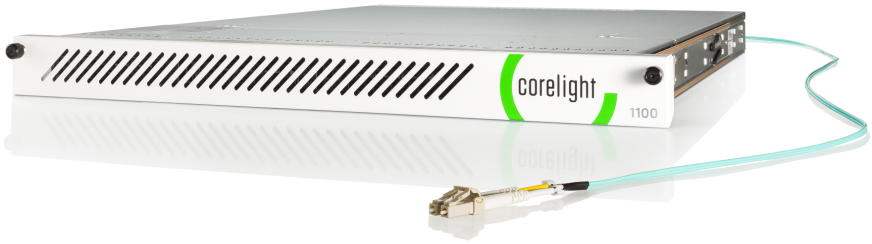

AP 1100 Sensor (20 Gbps)

Visibility made elegantly simple

The Corelight AP 1100 Sensor gives your SOC comprehensive, actionable insights into your network with high-fidelity, structured data.

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 and extracted files, and you're done. Get new features via automatic updates and enterprise support from the creators of Zeek®.

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 Zeek had

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

AP 1100 Sensor (20 Gbps): Specifications

Best-in-class Zeek and Suricata deployment in a compact 1U sensor:

- Engineered for stability and performance, by the creators of Zeek
- Four 1G/10G SFP/SFP+ interfaces 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
- 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
- For more info on Suricata support in the AP 1100 Sensor, read this whitepaper
- World-class support from the definitive Zeek experts included, additional support programs available; see our website for details

Specifications

Size and weight	1U rackmount, (19 x 31.85 x 1.7 inches), 48 lbs
Monitoring interface	Four 1G/10G SFP/SFP+ modules. Support for copper and optical modules at 1G and/or 10G
Management interface	2 x 1G ports 4 x 10G SFP+ ports
External connector	VGA, USB
Power	100-240 VAC 50/60 Hz redundant dual PSUs. Approximately 270W usage when idle and 439W 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