AP 200 Sensor (2 Gbps)

Full network visibility in a half-depth sensor

Corelight designed the AP 200 Sensor to deliver Zeek evidence and Suricata alerts in a compact size that thrives in small server closets or on cramped factory floors.

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 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 reliable performance needed in critical deployments.

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, sensor health metrics, and automated data export to Splunk, Elastic, Kafka, Syslog, S3, and more.

AP 200 Sensor (2 Gbps): Specifications

The Corelight AP 200 Sensor is designed for traffic analysis at speeds up to 2 Gbps:

- In branch offices
- In your DNS subnet
- In front of critical
- services or systems
- In front of VPNs

Best-in-class Zeek and Suricata in a 1U half-depth sensor:

- Engineered for stability and performance, by the creators of Zeek
- Four 1G 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
- Up to 2 Gbps of Zeek-only traffic monitoring
- 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 the AP 200 Sensor, read this whitepaper

Specifications

Size and weight	1U half-depth rackmount (19 x 14.5 x 1.75 inches), 22 lbs
Monitoring interface	4 SFP interfaces. Support for copper and optical modules at 100M & 1G.
Management interface	One 10/100/1000 copper ethernet port
External connector	VGA, USB
Power	120/240 VAC 50/60 Hz single PSU. Approximately 83W usage when idle and 141W 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 world's leading platform for network security monitoring.

info@corelight.com | 888-547-9497

The Z and Design mark and the ZEEK mark are trademarks and/or registered trademarks of the International Computer Science Institute in the United States and certain other countries. The Licensed Marks are being used pursuant to a license agreement with the Institute.

All rights reserved. © Copyright 2022 Corelight, Inc.