



## 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.

### 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.

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

## AP 200 Sensor (2 Gbps): Specifications

### 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

---

<b>Size and weight</b>	1U half-depth rackmount (19 x 14.5 x 1.75 inches), 22 lbs
<b>Monitoring interface</b>	4 SFP interfaces. Support for copper and optical modules at 100M & 1G.
<b>Management interface</b>	One 10/100/1000 copper ethernet port
<b>External connector</b>	VGA, USB
<b>Power</b>	120/240 VAC 50/60 Hz single PSU. Approximately 83W usage when idle and 141W usage at load.
<b>Operational mode</b>	Out of band—fed by tap, span, or packet broker



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**