

Full network visibility in a half-depth sensor.

The creators of Zeek (formerly known as Bro) designed the Corelight AP 200 Sensor to deliver the comprehensive, actionable network visibility of Zeek 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.

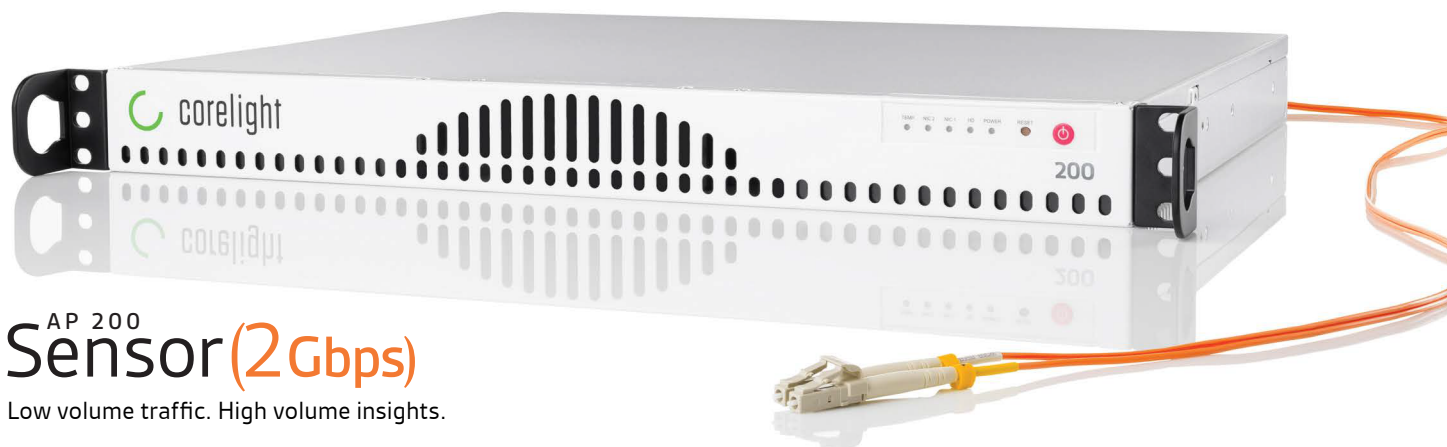
Engineered from the ground up with keen attention to detail, Corelight Sensors are security-hardened and run a custom OS based on the Linux kernel. A specialized NIC provides the reliable performance needed in critical deployments.

The features you wish open-source 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, 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 (2Gbps)

Low volume traffic. High volume insights.

Specifications

Best-in-class Zeek 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
- Zeek log export to Splunk, Elastic, Kafka, Syslog, SIEMs, 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
- World-class support from the definitive Zeek experts



AP 200 Sensor (2Gbps)

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 delivers the most powerful network security monitoring (NSM) solutions that help large organizations defend themselves by transforming network traffic into rich logs, extracted files, and security insights. Corelight makes a family of virtual, cloud, and physical sensors that take the pain out of deploying open-source Zeek and make it faster and enterprise-ready. Corelight's customers include Fortune 500 companies, government agencies, and research universities.

We make the **world's networks safer.**

For more information:

info@corelight.com

888-547-9497

510-281-0760

corelight.com

@corelight_inc.