AP 3000 Sensor (25 Gbps+)

High-throughput network insight

The AP 3000 reliably scales Zeek, Suricata and Smart PCAP to deliver high-fidelity network data to your analytics pipeline.

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 Smart PCAP and 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.

The Corelight AP 3000 Sensor is designed for traffic analysis at speeds up to 25 Gbps and beyond:

- In Science DMZ environments
- In telecommunication networks
- In high-volume data centers

Zeek, Suricata, and Smart PCAP deployment in a compact 1U sensor:

- For more information on sensor support for Suricata, read this datasheet
- For more information on sensor support for Smart PCAP, read this datasheet
- Engineered for stability and performance, by the creators of Zeek
- Up to 8 SFP/SFP+ interfaces OR 2 QSFP+ 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 25 Gbps of Zeek-only traffic monitoring, with speeds over 25 Gbps possible with shunting
- 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 experts included, additional support programs available

Specifications

Size and weight	1U rackmount (19 x 25.6 x 1.75 inches), 51 lbs
Monitoring interface	Up to 8 SFP/SFP+ or 2 QSFP+ modules. Support for copper and optical modules at 1G and 10G or 40G
Management interface	One 10/100/1000 copper ethernet port Two 1/10G SFP+ ports
External connector	VGA, USB
Power	120/240 VAC 50/60 Hz redundant dual PSUs. Approximately 161W usage when idle and 445W usage at load
Operational mode	Out of band—fed by tap, span, or packet broker

corelight

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

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.