Software Sensor

Complete network visibility, anywhere

Corelight's Software Sensor is our most flexible solution. Gain visibility in those hard-to-reach places across your network where you cannot put an appliance.

The power of Corelight, deployed on your existing Linux hardware

Leverage your existing infrastructure investments and bring your own hardware. Corelight's Software Sensor can be deployed on your existing Linux-based system. Capture files from network traffic at high speed, and lower data volume into your SIEM by reducing data of minimal value.

Extend the power of Corelight's open NDR platform across your hybrid, multi-cloud, and distributed networks. Corelight's Software Sensor delivers network traffic insights across a range of environments – including low bandwidth, remote, and air-gapped environments.

Accelerate threat hunting and response with next-level analytics

Corelight's open NDR platform delivers behavioral analysis, machine learning, and signatures to provide our customers with 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.

Specifications

Best-in-class Zeek® deployment:

- Corelight's platform in a lightweight (< 60MB) software binary
- Enterprise support, maintenance, and software updates
- Built-in Zeek detection, monitoring, and enrichment packages
- Capacity-based licensing model for deployment flexibility
- Zeek log export to Splunk, Kafka, Syslog, JSON, REDIS, and SFTP
- High performance and efficient file extraction
- Comprehensive REST API for configuration and monitoring
- World-class support from the definitive Zeek experts

Minimum system requirements

- Any 64-bit Linux distribution

Scalable across a range of reference configurations:

Nominal capacity	vCPUs	RAM (GB)	Workers
500 Mbps	2	8	1
1 Gbps	4	16	2
2 Gbps	8	32	4
4 Gbps	16	64	8
8 Gbps	32	128	16

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