Data sheet

Network insights at scale

Corelight Sensors give your SOC comprehensive, actionable insights into your network with high-fidelity, structured data.

Advanced network traffic analysis tool that leverages open-source Zeek®, Suricata, and YARA technologies to provide high-fidelity insights into network activity.

The ground truth from the network is essential to the entire incident response process, from scoping through containment and verification. Enhance cybersecurity defenses with real-time detection and comprehensive data from Corelight sensors—designed for both on-premises and cloud environments.

CONSOLIDATE TOOLS FOR INTEGRATED NETWORK VISIBILITY

Corelight sensors integrate network telemetry, intrusion detection, packet capture and static file analysis capabilities providing uncompromising network insight and comprehensive detections for threats like lateral movement, command and control, and encrypted attacks. Corelight's Smart PCAP gives security teams complete control over packet capture. Compared to full PCAP, it extends investigation lookback windows up to 10x by capturing only the packets needed.

ADVANCED DETECTION CAPABILITIES

Behavioral analysis, machine learning, and signatures give Corelight customers comprehensive malware identification and threat detection coverage across on-prem to cloud. 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.

BEST-IN-CLASS NDR CAPABILITIES IN A COMPACT 1U SENSOR

Engineered for stability and performance, with integrated network telemetry, intrusion detection, packet capture and static analysis capabilities.

Intuitive, 15-minute configuration, with a beautiful web app UI

Data export to Investigator, Kafka, Splunk, Elastic Search, SIEMs, EDRs/XDRs, syslog, Amazon Kinesis, Apache Avro, and SFTP

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, read this whitepaper

OPTIMIZED 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.

EASY DEPLOYMENT AND MANAGEMENT, 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. Rest APIs allow for easy configuration and management.

Get new features via automatic updates and enterprise support from the creators of Zeek. Available as hardware, cloud, software, or virtual sensors.

APPLIANCE SENSORS

Corelight appliance sensors support Investigator, IDS, Smart PCAP, Zeek, and YARA providing uncompromising network insight and comprehensive detections for threats including lateral movement, command and control, and encrypted attacks.

Specifications	AP 200	AP 1200	AP 3200	AP 5000	AP 5002
Traffic analysis speeds	Up to 2 Gbps	25 Gbps	50 Gbps+	100 Gbps+	100 Gbps+
Traffic analysis speeds - with Zeek, Suricata IDS and Smart PCAP[1]	Up to 1 Gbps	12.5 Gbps	25 Gbps	50 Gbps+	50 Gbps+
Best suited for	• Branch offices • DNS subnet • Critical services or systems • VPNs	• Branch offices • DNS subnet • Critical services or systems • VPNs	• Science DMZ environments • Telecommunication networks • High-volume data centers	• Science DMZ environments • Telecommunication networks • High-volume data centers	• Science DMZ environments • Telecommunication networks • High-volume data centers
Size and weight	1U rackmount, (19 x 14.5 x 1.75 in), 22 lbs	1U rackmount, (19 x 31.85 x 1.7 in), 48 lbs	1U rackmount, (19 x 31.85 x 1.7 in), 48 lbs	1U rackmount, (17.1 x 29 x 1.75 in), 47.4 lbs	1U rackmount, (17.1 x 29 x 1.75 in), 47.4 lbs
Monitoring interface	4 x SFP network ports. Support for 100M and 1G	4 x SFP28 network ports. Support for 4x1/10G	Option of 4 x SFP28 or 2 x QSFP28 network ports. Support for 4x1/10G or 4x10/25G, 2x40G or 8x10G (breakout cable required), depending on option selected	2 x QSFP28 network ports. Support for 8x10G (breakout cable required), 2x40G or 2x100G	2 x QSFP28 network ports. Support for 8x10G (breakout cable required), 2x40G or 2x100G
Management interface	One 10/100/1000 copper ethernet port	2x 1Gbe LOM ports 4x 10/25G, SFP28, OCP NIC 3.0	2x 1Gbe LOM ports 4x 10/25G, SFP28, OCP NIC 3.0	2x 1Gbe LOM ports 4x 10/25G, SFP28, OCP NIC 3.0	2x 1Gbe LOM ports 4x 10/25G, SFP28, OCP NIC 3.0
External connector	VGA, USB	VGA, USB	VGA, USB	VGA, USB	VGA, USB
Power	120/240 VAC 50/60 Hz single PSU. Approximately 83 W usage when idle and 141 W usage at load	100-240 VAC 50/60 Hz redundant dual PSUs. Approximately 400W usage when idle and 600W usage at load	100-240 VAC 50/60 Hz redundant dual PSUs. Approximately 450W usage when idle and 700W usage at load	100-240 VAC 50/60 Hz redundant dual PSUs. Approximately 443W usage when idle and 852W usage at load	100-240 VAC 50/60 Hz redundant dual PSUs. Approximately 443W usage when idle and 852W usage at load

[1] *Traffic analysis based on benchmark profile; actual results will vary based on traffic mix*

Specifications	AP 200	AP 1200	AP 3200	AP 5000	AP 5002
Operational mode	Out of band—fed by tap, span, or packet broker	Out of band—fed by tap, span, or packet broker	Out of band—fed by tap, span, or packet broker	Out of band—fed by tap, span, or packet broker	Out of band—fed by tap, span, or packet broker
Additional		Supports shunting or deduplication to improve performance in high volume environments	Supports shunting or deduplication to improve performance in high volume environments	Supports shunting or deduplication to improve performance in high volume environments	Supports shunting or deduplication to improve performance in high volume environments

CLOUD SENSORS

Corelight Cloud Sensors enable security teams to extend visibility across hybrid and multi-cloud environments with consistent, comprehensive uniform telemetry enriched with control plane data. Accelerate incident response and unlock threat hunting capabilities by providing analysts managing diverse environments with the actionable insights needed in real-time.

Nominal capacity	vCPUs	RAM (GB)	Disk (GB)
500 Mbps	4	16	500
1 Gbps	8	32	500
2 Gbps	16	64	500
4 Gbps	32	128	1000
6 Gbps	48	192	2000
8 Gbps	64	256	4000

VIRTUAL SENSORS

Corelight Virtual Sensors transform network traffic into high-fidelity data for incident response, intrusion detection, and more. The Corelight Virtual Sensor parses dozens of network protocols and generates rich, actionable evidence and detections—designed for security professionals, by security professionals.

	The Corelight Virtual Sensor for Microsoft Hyper-V	The Corelight Virtual Sensor for VMware
Traffic analysis speeds	8 Gbps	8 Gbps
Best suited for	• branch locations • manufacturing floors • remote offices • high-value enclaves	• branch locations • manufacturing floors • remote offices • high-value enclaves
System requirements	Hyper-V minimum system requirements • Windows Server 2016 Hyper-V environment • Online access for seeding (i.e., inserting certificate)	VMware minimum system requirements • VMware ESX 6.0 or later • 4 cores, 16 GB RAM, 500 GB disk • online access for initial configuration

SCALABLE ACROSS A RANGE OF REFERENCE CONFIGURATIONS:

Nominal capacity	vCPUs	RAM (GB)	Disk (GB)
500 Mbps	4	16	500
1 Gbps	8	32	500
2 Gbps	16	64	500
4 Gbps	32	128	1000
6 Gbps	48	192	2000
8 Gbps	64	256	4000

FLOW LOG SENSORS

Corelight Flow Log Sensor transforms raw cloud and network flow logs into high-fidelity, security-ready data for detection, investigation, and compliance. The Corelight Flow Log Sensor ingests flow data such as AWS VPC Flow Logs, then enriches and normalizes it into normalized Zeek logs, reducing data volumes by up to 90%. The result is actionable evidence and detections, delivering clarity from noisy flow logs and extending visibility to places where packet mirroring and taps aren't available.

Minimum system requirements

- The Corelight Flow sensor should be deployed as a single EC2 instance and not part of an autoscaling group
- The EC2 instance should at a minimum have the following configuration: 4 vCPUs / 16GB RAM / 500GB EBS

corelight

View all specifications:

https://corelight.com/products/product-specifications/

info@corelight.com | 888-547-9497