Corelight

A Zeek force multiplier for your team and tools

Corelight Sensors go wherever your traffic goes.

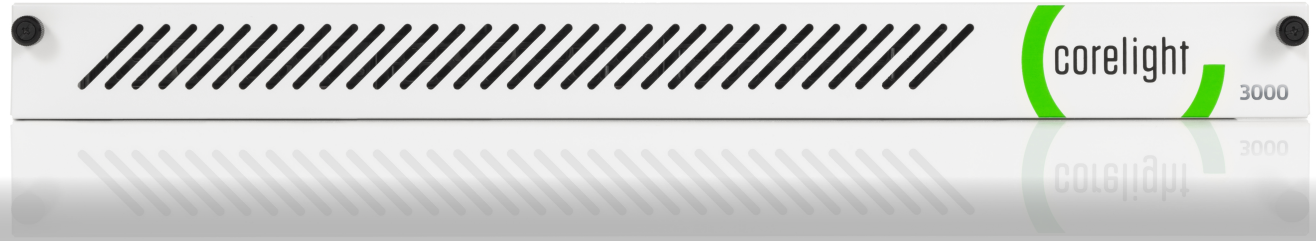
VIRTUAL SENSOR	AP 200	AP 1001	AP 3000	FLEET MANAGER
Up to 2 Gbps	2+ Gbps	10+ Gbps	25+ Gbps	Manage up to 250 sensors
VMware ESXi 6.5 or later Hyper-V on Windows Server 2016	1 rack ½ depth unit	1 rack unit	1 rack unit	Virtual appliance

Virtual Sensor Specs

Nominal Capacity	vCPUs	RAM (GB)	Disk (GB)
250 Mbps	2	8	500
500 Mbps	4	16	500
1 Gbps	8	32	500
2 Gbps	16	65* / 64	500

* VMware only

We make Zeek easy-to-use and significantly more powerful.

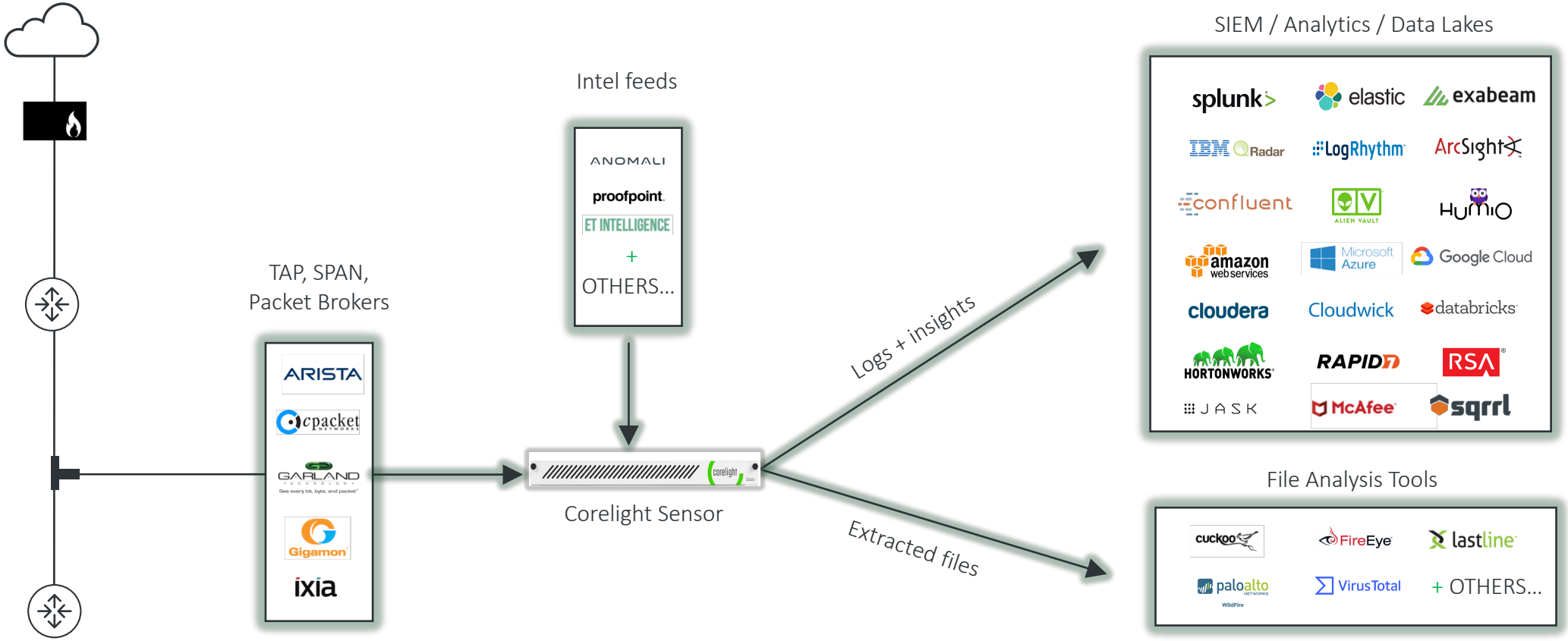


	Open-Source Zeek	corelight
Sensors	Custom hardware purchase	Pre-built sensors in physical and virtual form factors
Deployment Time	Weeks to months	< 15 minutes
Performance	3-4 Gbps max per cluster	25+ Gbps per sensor
Management	Command line only, DIY	Web management GUI, full API, fleet management
Health Monitoring	No	Sensor health + performance monitoring
Integrations	No	SIEM, Analytics, Cloud Storage integrations out-of-the-box
Log Streaming	No	Yes
Log Forking & Filtering	No	Yes
Log Data Reduction	No	Yes - reduces log data volume by up to 30%!
Zeek Scripts	Manual installation	Curated scripts preloaded and sandboxed for security
Support	No	Yes - 24/7 global support from Zeek's creators

Corelight lets you unlock and expand the power of Zeek.

Zeek logs	Zeek file extraction	Zeek packages
Generate logs at 25+ Gbps	Extract files at 25+ Gbps	Deploy preloaded packages like JA3 in 1-click.
Stream logs in real time to SIEMs	Automatically deduplicate files	Run open-source scripts in a secure sandbox
Fork & filter logs to multiple destinations.	Send files to disk or S3	
Reduce data export volumes by up to 30%		

Corelight seamlessly integrates with your security stack.



Corelight gives you one-click package deployment options.

The Core Collection: key packages preloaded, validated, and sandboxed for security.

Detection Packages	Data Enrichment Packages	Operational Packages
Cryptomining detection	URL Extraction in SMTP	Data Reduction
SSL fingerprinting (JA3)	Post data capture in HTTP	SSL certificate monitoring
SSH fingerprinting (HASSH)	DNS hostname annotation	Traffic shunting
HTTP stalling detection		Windows version identification
Long connections detection		
Port scanning detection		

We provide global enterprise support.

FEATURES & BENEFITS	STANDARD SUPPORT	ENTERPRISE SUPPORT
Telephone and email support	Yes	Yes
Next business day response guarantee	Yes	Yes
24 x 7 availability	---	Yes
1 hour response SLA for P1 issues	---	Yes
Executive visibility of all P1 issues	Yes	Yes
Software updates	Yes	Yes
Security bulletins and updates	Yes	Yes
Online support portal and knowledge base	Yes	Yes
Hardware replacement	Yes	Yes
Advanced hardware replacement	---	Yes
No disk RMA requirements	Yes	Yes
Automatic, manual, or onsite update options with granular control	Yes	Yes
Online issue analysis with Corelight Dynamic Health Check	Yes	Yes

Corelight Sensors are battle tested & security hardened.

Corelight Sensors

- Default access disabled to limit attack surface.
- After initial configuration, sensor access is limited to SSH, HTTPS, or Corelight API (TLS).
- Password/key protection, encrypted disks.
- Automatic security updates.
- Processes run in secure enclaves.
- Verified to comply with FIPS 140-2

Open-Source Zeek

- No built in security hardening

Reinvest your time, we can take care of Zeek for you.

Global educational services org.

"Corelight was the easiest product to use. Setting up their appliance took me only 15 minutes."

- Senior Security Engineer

- Unlocked SOC bandwidth for threat hunting
- Reduced avg. incident response time by 95%
- Identified and tuned out IDS false positives

Multinational energy company

"My SIEM support contact was genuinely surprised when Corelight's logs 'magically' flowed to their instance 'pre-cooked'. It was flawless."

- Security Engineer

- Identified and tuned out IDS false positives
- Resolved critical file access incident in minutes
- Significantly reduced unencrypted email sends

Top international law firm

"Corelight takes care of it for us and has given us more bandwidth to threat hunt."

- Information Security Engineer

- Unlocked SOC bandwidth for threat hunting
- Gained east-west visibility to lateral movement
- Automated beaconing detection via RITA

Zeek expertise doesn’t get better than Corelight.

VERN PAXSON	SETH HALL	ROBIN SOMMER	JOHANNA AMANN
Chief Scientist, Corelight *Invented Bro*	Chief Evangelist, Corelight *Key Bro Committer*	CTO, Corelight *Key Bro Committer*	Engineer, Corelight *Key Bro Committer*

See the Corelight difference with a **30 day, risk-free trial.**

Information Security Engineer
Top International Law Firm

”It wasn’t difficult at all. I plugged it in, gave it an internal IP address, whitelisted the Corelight IP address on the firewall, and had it up and running in minutes.”

Corelight vs. Open-Source Zeek

Sensors	Open-Source Zeek	corelight
Physical Sensors	Custom hardware purchase	Pre-built AP 200, AP 1001, AP 3000 supporting 2/10/25 Gbps
Virtual Sensors	No	Corelight Virtual Sensor (VMware, Hyper-V)

Performance		
Peak throughput	3-4 Gbps cluster max	25+ Gbps per sensor
Optimized file extraction	No	Yes – supports file extraction at 25+ Gbps
Performance monitoring	No	Yes – real-time performance metrics (included a definitive packet loss rate)
Packet loss	Variable, risk of >50%	<1%

Management		
Deployment time	Weeks to months	<15 minutes
Management interface	Command line only	Web management GUI
Software updates	Manual	Automatic
Fleet management	None	Yes – Fleet Manager supports up to 250 sensors
Sensor monitoring	None	Yes – detailed health & performance monitoring
API support	None	Yes – full-featured RESTful API for devops
Package installation	Manual	One-click installation for Core Collection packages

Corelight vs. Open-Source Zeek

Data Export/Control	Open-Source Zeek	corelight
Log data reduction	No	Yes – Corelight data reduction package reduces data export by up to 30%
Log streaming (& Kafka)	No	Yes
Log stream filtering	No	Yes – granular log filtering capabilities
Log stream forking	No	Yes – send streams to multiple locations
Traffic shunting	No	Yes – (AP 3000)
File extraction deduplication	No	Yes
Integrations		
SIEMs	Manual	Pre-integrated with Splunk, Elastic, Exabeam, Qradar + others…
Kafka	No	Yes
Security Analytics	Manual	Pre-integrated with Jask, Rapid7, Sqrrl + others
Security & Support		
Jailed processes	No	Yes
FIPS 140-2	No	Yes
Automatic security updates	No	Yes
Disk encryption	Manual	Yes
Support	No	Yes – global 24/7 support from leading Zeek experts

Corelight vs. Open-Source Zeek

Zeek Functions	Open-Source Zeek	corelight
Logging	Yes	Yes
File extraction	Yes	Yes
Zeek Package Manager	Yes	Yes
Zeek Intelligence Framework	Yes	Yes
Zeek NetControl Framework	Yes	No
Zeek Notice Framework	Yes	No
Zeek PCAP Ingestion	Yes	No