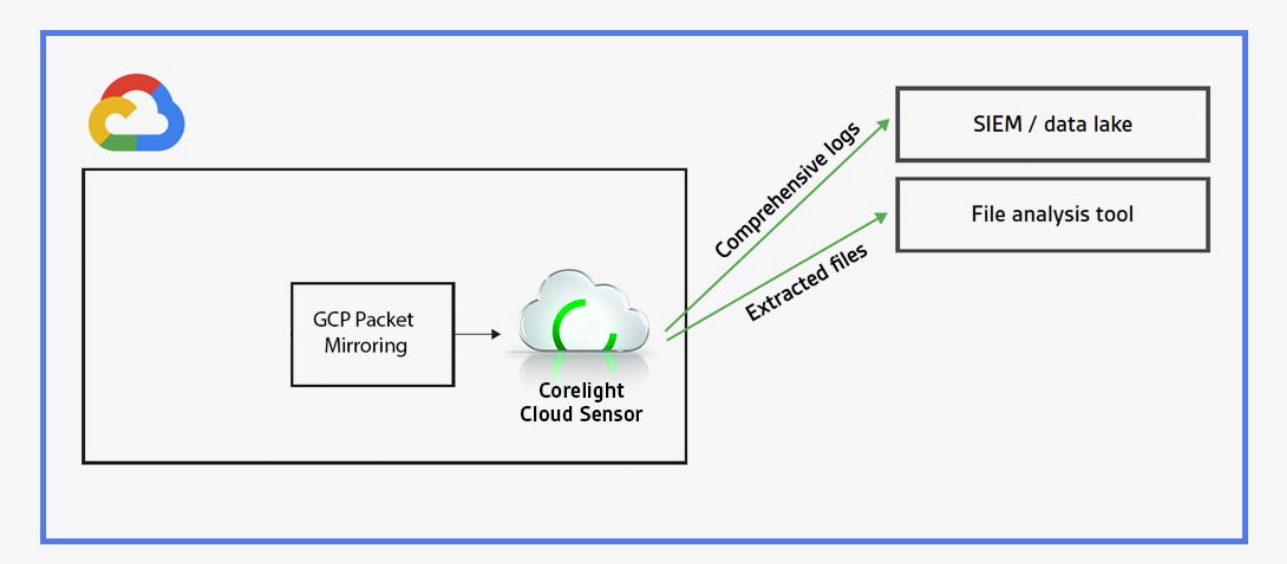
corelight

Cloud Sensor for GCP

Comprehensive network insight in Google Cloud

The creators of Zeek designed the Corelight Cloud Sensor to transform GCP traffic into rich logs, extracted files, and custom insights that accelerate incident response and unlock new threat hunting capabilities.

Corelight Cloud Sensor for GCP solution



The Corelight Cloud Sensor deploys as a GCP VM image instance and ingests traffic directly via GCP Packet Mirroring or from 3rd party packet-forwarding agents. With a few simple config changes, the sensor will export data to downstream storage and analytics tools such as SIEMs or file analysis platforms.

The features you wish open-source Zeek had
Corelight has added a suite of enterprise features to Zeek that dramatically improve its usability, from high-performance file extraction, content including Encrypted Traffic Collection, and automated data export to Splunk, Elastic, Kafka, and more.

Specifications

Best-in-class Zeek deployment:

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

Cloud Sensor for GCP
The Corelight Cloud Sensor provides visibility into GCP to monitor:

- Scalable cloud applications
- Dynamic workloads
- And more…

Scalable across a range of GCP instance types:

Nominal capacity	CPUs	RAM (Gb)	Disk (Gb)	System Requirements
250 Mbps–8 Gbps	2–64	8–256	100–4000	Any 64 bit Linux distribution
				GCP Packet Mirroring enabled OR mirroring via 3rd party packet-forwarding agents

Scalable across a range of reference configurations:

Gbps	Machine name	vCPUs	Memory (GB)	Workers
0.5	e2/n2-standard-2	2	8	1
1	e2/n2-standard-4	4	16	2
2	e2/n2-standard-8	8	32	4
4	e2/n2-standard-16	16	64	8
8	e2/n2-standard-32	32	128	16

Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders.

info@corelight.com | 888-547-9497