corelight

## Cloud Sensor for GCP

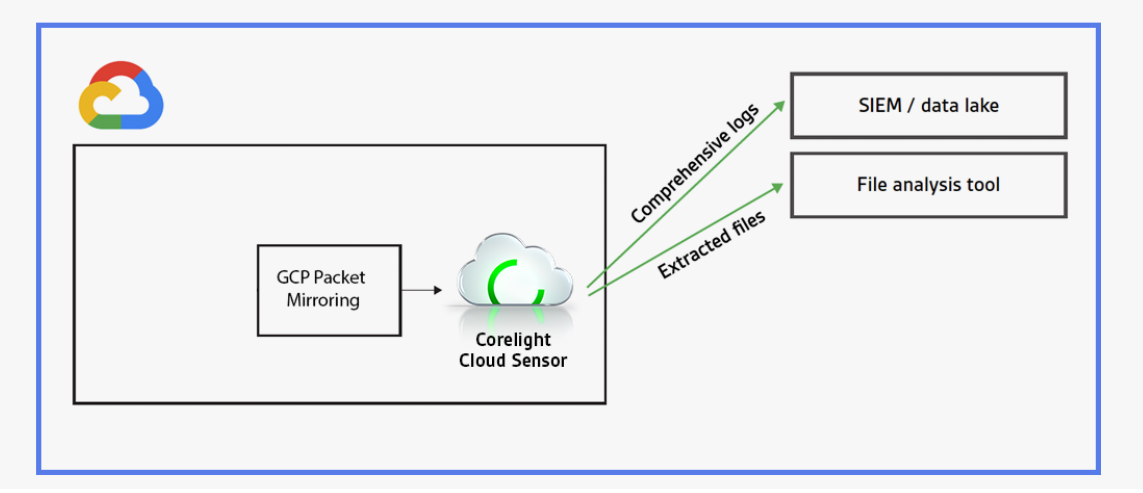
# Comprehensive network insight in Google Cloud

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.

**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.

## *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 had**
Corelight has merged the power of Zeek and Suricata with 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.

# Specifications

**Best-in-class Zeek and Suricata deployment:**
- Corelight's best-in-class Zeek and Suricata platform in a Google Cloud 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 |

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**