

Comprehensive Network Security Monitoring in the Cloud.



The creators of Zeek (formerly known as Bro) designed the Corelight Cloud Sensor to transform Amazon VPC traffic into rich logs, extracted files, and custom insights that accelerate incident response and unlock new threat hunting capabilities.

Quick sensor deployment and configuration in AWS.

The Corelight Cloud Sensor deploys as an AMI from the AWS Management Console and can ingest traffic directly via Amazon VPC traffic mirroring or from 3rd party packet-forwarding agents. Make a few simple data export configurations in Corelight’s management console and you’re ready to go.

Focus on your traffic, not instances.

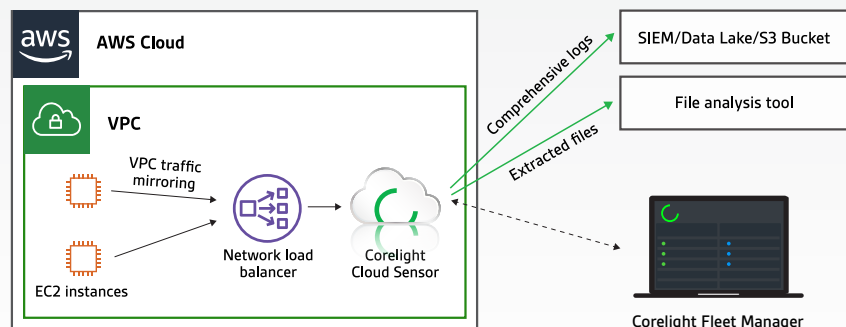
The Corelight Cloud Sensor is designed with flexibility in mind so you can deploy the right sizes for your traffic needs. It’s also conveniently licensed on capacity so you can spin up the Amazon EC2 instances needed for your environment and adjust them as your traffic evolves.

The features you wish open-source Zeek had.

Corelight has merged the power of Zeek with a suite of enterprise features that dramatically improve Zeek usability, like an intuitive management UI, sensor health metrics, and automated data export to Splunk, Elastic, Kafka, Syslog, S3, and more.

Corelight Cloud Sensor for AWS solution

The Corelight Cloud Sensor can ingest traffic via Amazon VPC traffic mirroring (enabled per EC2 instance) or via an Amazon Network Load Balancer, streaming logs and extracted files to SIEMs, Amazon S3, or file analysis tools. Customers can fork and filter the data via Corelight’s management console and easily manage multi-sensor environments with Corelight Fleet Manager’s sensor policy templates and role-based access controls.



Specifications

CloudSensor for AWS



Best-in-class Zeek deployment:

- Corelight's best-in-class Zeek platform in an Amazon Machine Image (AMI)
- Built-in Zeek packages for detection, monitoring, and data enrichment
- Intuitive, fast configuration with a beautiful web UI
- Capacity-based licensing model for deployment flexibility
- Zeek log export to Splunk, Elastic, Kafka, Syslog, Amazon S3, and SFTP
- High performance and efficient file extraction
- 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

The Corelight Cloud Sensor provides visibility into Amazon VPC traffic to monitor:

- Scalable cloud applications
- Dynamic workloads

Scalable across a range of AWS EC2 instance types:

Instance	Nominal capacity	Instance	Nominal capacity
m5.xlarge	500 Mbps	m4.xlarge	500 Mbps
m5.2xlarge	1 Gbps	m4.2xlarge	1 Gbps
m5.4xlarge	2 Gbps	m4.4xlarge	2 Gbps

AWS minimum system requirements:

- An M4 or M5 type AWS EC2 instance
- Amazon VPC traffic mirroring enabled OR mirroring via 3rd party packet-forwarding agents



Corelight delivers the most powerful network security monitoring (NSM) solutions that help large organizations defend themselves by transforming network traffic into rich logs, extracted files, and security insights. Corelight makes a family of virtual, cloud, and physical sensors that take the pain out of deploying open-source Zeek and make it faster and enterprise-ready. Corelight's customers include Fortune 500 companies, government agencies, and research universities.

We make the **world's networks safer.**

For more information:

info@corelight.com

888-547-9497

510-281-0760

corelight.com

@corelight_inc.