

# Flexible traffic visibility in a virtual form factor.

The creators of Zeek (formerly known as Bro) designed the Corelight Virtual Sensor to go wherever you need it, analyzing network traffic at speeds of up to 2 Gbps.

## Deploy in VMware or Hyper-V in 15 minutes.

Successfully deploy Corelight Virtual Sensors in a few simple steps: download the image, activate the license key, and follow the installation wizards to set a handful of configuration parameters.

## Focus on your traffic, not instances.

The Corelight Virtual 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 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 its usability, such as a Core Collection of Zeek packages for detection and monitoring, sensor health metrics, and automated data export to Splunk, Elastic, Kafka, Syslog, S3, and more.



The Corelight Virtual Sensor provides network traffic insights across a range of environments:

- In branch locations
- On manufacturing floors
- In remote offices
- In high-value enclaves

## Scalable across a range of VMware reference configurations:

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	500

# Specifications

## Best-in-class Zeek deployment:

- Corelight's best-in-class Zeek platform in a virtual machine
- Built-in Zeek packages for detection, monitoring, and data enrichment
- Intuitive, 15 minute configuration, with a beautiful web UI
- Capacity-based licensing model for deployment flexibility
- Zeek log export to Splunk, Elastic, Kafka, Syslog, SIEMs, 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

## Virtual Sensor (2Gbps)

### VMware minimum system requirements

- VMware ESX 6.5 or later
- 2 cores, 8 GB RAM, 500 GB disk
- Online access for initial configuration

### Hyper-V minimum system requirements

- Windows Data Center 2016
- Online access for seeding (i.e., inserting certificate)

## Hyper-V reference configurations:

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	64	500



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.