Virtual Sensor

Flexible traffic visibility in a virtual form factor

The Corelight Virtual Sensor for Hyper-V is designed to go wherever you need it, analyzing network traffic at speeds of up to 8 Gbps.

Deploy in 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 wizard 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.

Microsoft Hyper-V

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

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

Hyper-V reference configurations:

Nominal capacity	vCPUs	RAM (GB)	Disk (GB)
500 Mbps	4	16	500
1 Gbps	8	32	500
2 Gbps	16	64	500
4 Gbps	32	128	1000
6 Gbps	48	192	2000
8 Gbps	64	256	4000

Hyper-V minimum system requirements
- Windows Server 2016 Hyper-V environment
- Online access for seeding (i.e., inserting certificate)

corelight

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