CloudSensor for Azure

corelight

Comprehensive Network Security Monitoring in the Azure Cloud.

The creators of Zeek (formerly known as Bro) designed the Corelight Cloud Sensor to transform Microsoft Azure 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 Azure.

The Corelight Cloud Sensor deploys as an Azure VM Image and ingests Azure traffic 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.

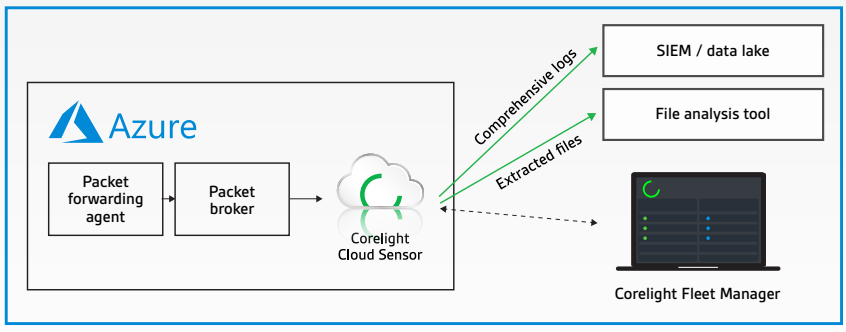
The Corelight Cloud Sensor is designed with flexibility in mind so you can deploy the right sizes for your traffic needs. It's also conveniently licensed on capacity so you can spin up the Azure instances needed for your environment and adjust them as your traffic evolves.

The features you wish open-source Zeek had.

Corelight has merged the power of Zeek with a suite of features that dramatically improve its performance and 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, and more.

Corelight Cloud Sensor for Azure solution

The Corelight Cloud Sensor deploys as an Azure VM Image instance and ingests mirrored-traffic from a packet-forwarding agent. After making a few simple config changes in Corelight's management console the sensor will export data to downstream storage and analytics tools such as SIEMs or file analysis platforms. Corelight offers export controls, such as log fork and filter and fleet management capabilities for multi-sensor environments such as policy templates and role-based access controls.



Specifications

Cloud Sensor for Azure

The Corelight Cloud Sensor provides visibility into Microsoft Azure traffic to monitor:

- Scalable cloud applications
- Dynamic workloads
- And more...

Best-in-class Zeek deployment:

- Corelight's best-in-class Zeek platform in an Azure-ready format
- 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, 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

Scalable across a range of Azure Ds v3 instance types:

Instance	Nominal capacity
D8s v3	1 Gbps
D16s v3	2 Gbps
D32s v3	4 Gbps
D48s v3	6 Gbps
D64s v3	8 Gbps

Azure minimum system requirements:

- Azure Ds v3 series (D8s minimum instance)
- Traffic mirroring via 3rd party packet-forwarding agents

corelight

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.