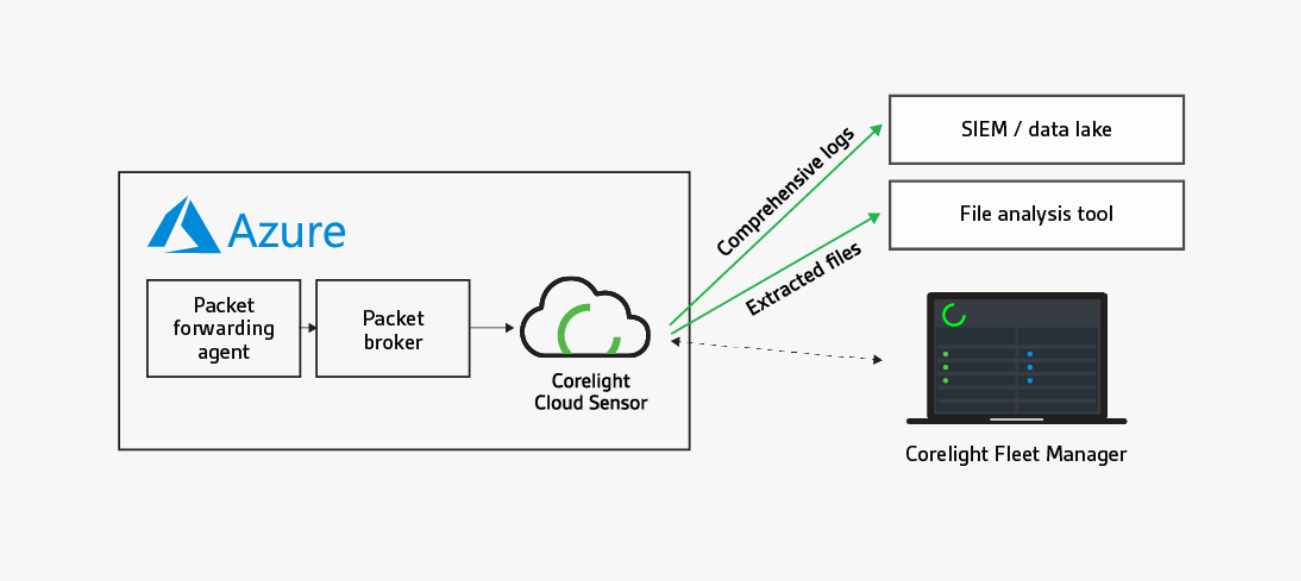
Cloud Sensor for Azure

Comprehensive monitoring in Azure

The creators of Zeek designed the Corelight Cloud Sensor to transform Microsoft Azure traffic into rich logs, extracted files, and custom insights to accelerate incident response and unlock new threat hunting capabilities.

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

Work faster and more effectively in Azure Sentinel
The Corelight for Azure Sentinel data connector enables ingestion of events from Zeek and Suricata via Corelight Sensors into Azure Sentinel. Corelight for Azure Sentinel also includes workbooks and dashboards, hunting queries, and analytic rules to help organizations drive efficient investigations and incident response with the combination of Corelight and Azure Sentinel.

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 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 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 expert

Scalable across a range of Azure Ds v3 instance types:

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

Azure minimum system requirements:

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

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

All rights reserved. © Copyright 2021 Corelight, Inc.