corelight

White Paper

Why the cloud needs NDR

Introduction

If cloud environments are locked down by default and everything is logged, is cloud network traffic analysis really helpful? Yes. In the cloud, network telemetry data makes investigations faster, ensures hunts are conclusive, and catches threats other tools miss — like Sunburst.

Why network monitoring matters in the cloud

While network monitoring has been around for a while, here's why it matters in the cloud:

Broadest visibility coverage

With NDR you can cover myriad systems, north/south traffic to and from your cloud environment, plus east/west traffic, all with a few devices, as opposed to deploying hundreds or thousands of agents.

Automate to deploy & manage at scale

NDR in the cloud is exceptionally easy to use. You can mirror machine traffic from your global cloud infrastructure in minutes or disable it on the fly when demand dries up.

NDR uses cloud-native services

NDR leverages cloud-native packet mirroring services like AWS VPC Traffic Mirroring and Google Cloud VPC Packet Mirroring that act as virtual taps, copying network traffic and streaming it to your NDR stack. Cloud-native mirroring can be enabled on every instance and between containers, with no additional CPU consumption in passive mode.

No agents to deploy

Because NDR is enabled by cloud-native services, there are no agents to deploy which means monitoring is invisible to attackers and extremely difficult to tamper with.

Out-of-band

NDR is out of band, so there's no inline blocking that could cause a disruption.

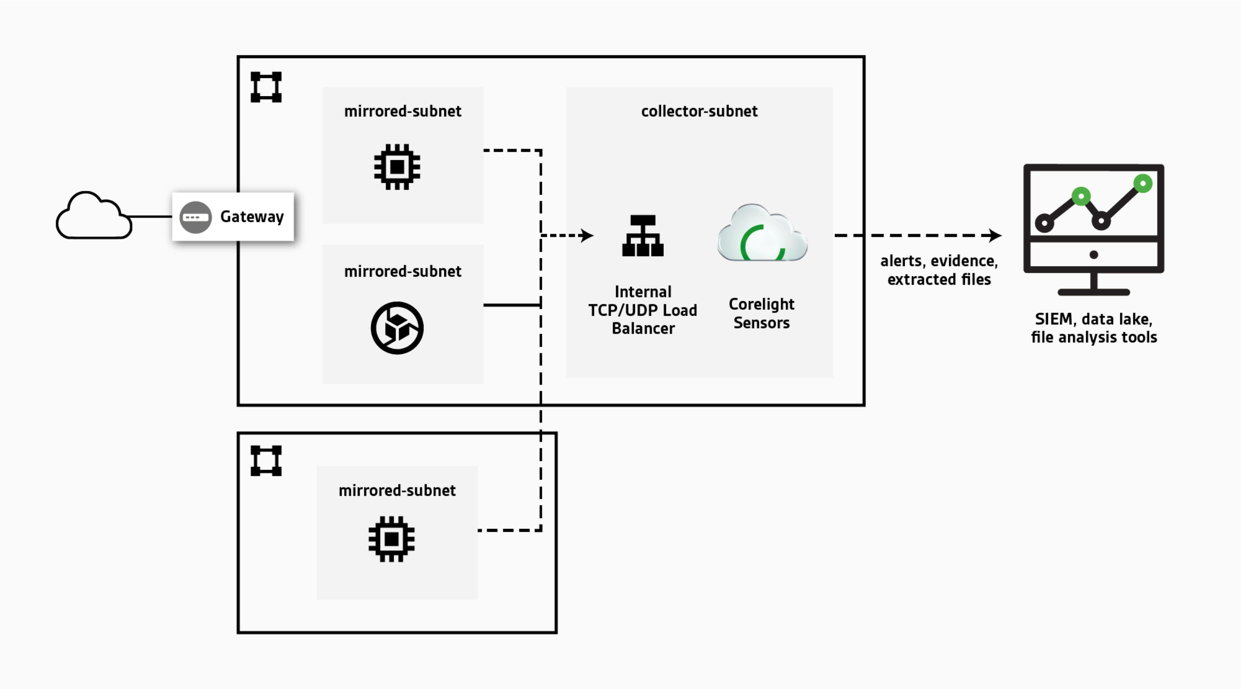
Provides context that endpoint lacks

NDR provides visibility and context not available from other cloud security solutions.

Corelight's unique approach to NDR in the cloud

The Corelight Cloud Sensor provides visibility into cloud environments to monitor scalable cloud applications, dynamic workloads, and more. Corelight's best-in-class NDR platform in a GCP format includes:

- Corelight's Zeek and Suricata platform in a cloud-ready format
- Deep insight into encrypted traffic
- Enterprise support, maintenance, and software updates
- Built-in Zeek packages for detection, monitoring, and data enrichment
- Capacity-based licensing model for deployment flexibility
- Zeek log export to Splunk, Kafka, Syslog, JSON, REDIS, and SFTP
- High performance, efficient file extraction
- Comprehensive REST API for configuration and monitoring
- World-class support from the Zeek experts


mirrored-subnet
collector-subnet
Gateway
mirrored-subnet
Internal TCP/UDP Load Balancer
Corelight Sensors
alerts, evidence, extracted files
SIEM, data lake, file analysis tools
mirrored-subnet

Available for AWS, Microsoft Azure, and Google Cloud, Corelight Cloud Sensors package enterprise Zeek and Suricata at speeds up to 8 Gbps.

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