corelight

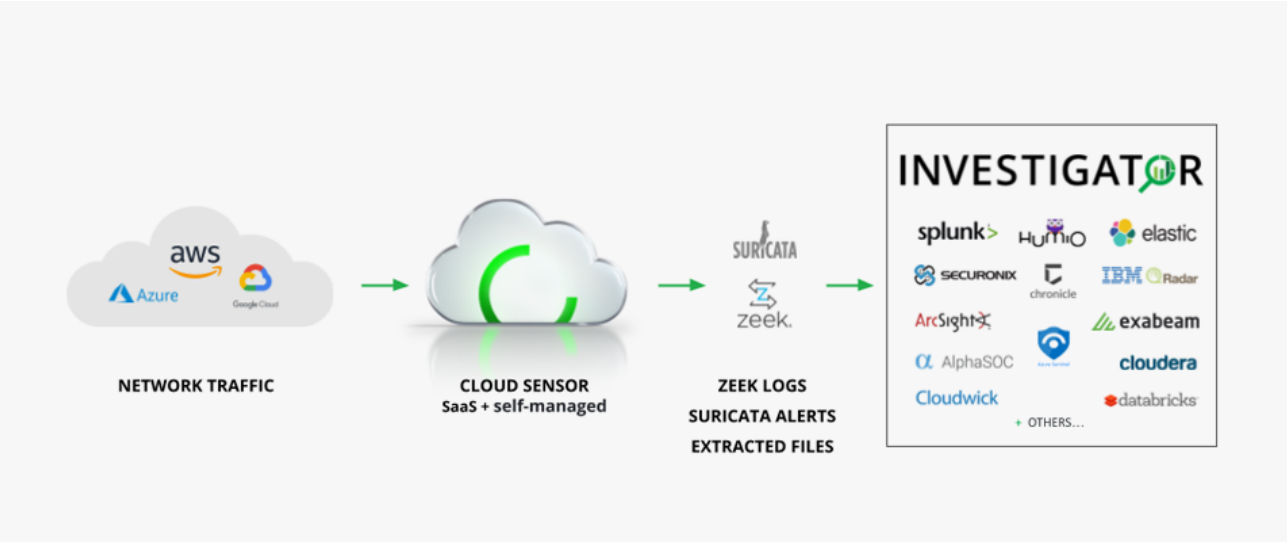
Cloud Sensor for AWS

Complete visibility for continuous security

Transform VPC traffic into comprehensive, correlated evidence to accelerate response and unlock new threat hunting capabilities.

Solution overview

Corelight Cloud Sensor for AWS ingests cloud traffic and transforms it into rich logs, extracted files, and custom insights to give defenders detections and context-rich evidence. We leverage the power of Corelight Labs, open source Zeek and Suricata, and machine learning to deliver next-level analytics and provide analysts with a clear understanding of their cloud, multi-cloud, and hybrid environments in real time.



Corelight Cloud Sensor for AWS is available as a SaaS and a self-managed solution and can be deployed behind AWS Network Load Balancer (NLB) or AWS Gateway Load Balancer (GWLB) to scale elastically, based on the volume of traffic. Our solution turns mirrored traffic into comprehensive logs, extracted files, and custom insights that can be streamed in real time into Corelight Investigator as well as SIEM and XDR solutions to provide SOC teams with the evidence needed to accelerate incident response and unlock new threat hunting capabilities.

Whether you're on-prem or in the cloud, network traffic is still the ultimate source of truth. Corelight enables SOC teams to quickly detect and respond to threats by turning cloud and container traffic into security-centric, comprehensive evidence.

Complete network visibility across hybrid and multi-cloud environments

Organizations are pressured to adopt a growing amount of cloud services yet struggle to expand their on-prem visibility into the cloud. Traditional, cloud-native tools are hard to tune and lack the context and correlation needed for alert triage. Our comprehensive coverage provides signature, behavioral, and machine learning detections for insights into encrypted traffic and detection of C2 behavior, data exfiltration, and more.

Faster investigations and expert-level threat hunting

Corelight reduces friction by integrating and complementing SOC workflows and providing uniformity in data across environments to reduce learning curves and accelerate response. We provide interlinked logs, enriched with cloud and container control plane attribution, which can be stored for years for future hunting and analytics needs.

Deploy and scale at cloud speed

Deploying an NDR stack should be easy. Corelight Cloud Sensor for AWS can be set up in minutes, requires zero maintenance, and is the only elastically scalable solution on the market —meaning no pre-provisioning of traffic. This lifts the heavy burden off of SecOps, freeing resources to focus on incident response and threat hunting.

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. On-prem and in the cloud, our open Network Detection and Response platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the world's leading platform for network security monitoring.

info@corelight.com | 888-547-9497