corelight

Data sheet

Expand threat coverage with flow monitoring

Corelight delivers end-to-end visibility with enriched, high-fidelity data for actionable SOC insights

Corelight transforms raw flow logs into rich, security-ready data, delivering the deep visibility that security teams need to protect their cloud and network environments from sophisticated threat actors. Traditional flow logs are high-volume and low-context, making it challenging to utilize them for security purposes. Corelight closes this gap by enriching flow logs into Zeek®-derived insights such as transaction details, UID, and traffic behaviors, creating a high-fidelity foundation for threat detection, investigation, and compliance. The result is a scalable, security-focused view of your cloud traffic that empowers analysts to detect threats, investigate incidents, and hunt proactively, without the blind spots, data overload, or complexity that often hinder cloud security operations.

COMPREHENSIVE NETWORK COVERAGE

Traditional cloud and network visibility relies on traffic mirroring, which can often be challenging to deploy everywhere due to cost or complexity concerns. This leaves critical flows between workloads, containers, serverless functions, and other network devices unmonitored. Corelight's Flow sensor eliminates these blind spots by enriching flow logs from every network device, delivering complete visibility for stronger detection, faster investigations, and more effective threat hunting across cloud environments.

SIGNIFICANT STORAGE COST REDUCTION

Organizations face rising storage costs from massive, inconsistently formatted flow logs that are hard to analyze and offer limited detection value. Corelight reduces log volume by up to 90% through normalization and smart filtering, preserving security context. This enables longer retention at a lower cost, providing analysts with the historical depth needed for effective investigations without budget strain.

KEY BENEFITS:

Complete coverage: Extend visibility across VPCs, containers, functions, and traditional networks

Noise reduction: Eliminate redundant data and focus on high-value insights

Standard logs: Normalize non-standard flow logs into correlated, structured Zeek logs

Accelerated detection & response: Multi-layered threat detection with context and explainability

Open & interoperable: Export enriched and standardized logs into any SIEM, data lake, or analytics tool

Detection & forensics: Analyze historical flow data stored in S3 buckets

SIEM cost reduction: Reduce flow log data volumes by up to 90%

2X FASTER INVESTIGATIONS

Investigating cloud security incidents can be slow and complex when analysts sift through raw, unstructured flow logs. Corelight accelerates investigations by providing enriched, standardized logs that map directly to attacker techniques and security use-cases. With this contextualized data, analysts can trace the root cause, lateral movement, and impacted assets more quickly, running investigations up to 2x faster, reducing risk exposure, and improving clarity and precision in incident response.

EASY DEPLOYMENT AND MANAGEMENT, CONFIGURE IN MINUTES

Corelight sensors are zero maintenance and take only minutes to deploy: connect the traffic feed, specify where to send logs and extracted files, and you're done. Rest APIs allow for easy configuration and management.

Get new features via automatic updates and enterprise support from the creators of Zeek. Available as hardware, cloud, software, or virtual sensors.

FLOW LOG SENSORS

Corelight Flow Log Sensor transforms raw cloud and network flow logs into high-fidelity, security-ready data for detection, investigation, and compliance. The Corelight Flow Log Sensor ingests flow data such as AWS VPC Flow Logs, combines entries to construct a bi-directional flow, then enriches and normalizes it into standard Zeek logs, reducing data volumes by up to 90%. The result is actionable evidence and detections, delivering clarity from noisy flow logs and extending visibility to places where packet mirroring and taps aren't available.

MINIMUM SYSTEM REQUIREMENTS

- The Corelight Flow sensor should be deployed as a single EC2 instance and not part of an autoscaling group
- The EC2 instance should at a minimum have the following configuration: 4 vCPUs / 16GB RAM / 500GB EBS

corelight

View all specifications:

https://corelight.com/products/product-specifications/

info@corelight.com | 888-547-9497