corelight

Data sheet

Corelight network evidence

Data + context = **evidence**

What is network evidence?

Corelight's network evidence is the authoritative, AI-ready source of truth for your network activity. It directly addresses the uncertainty caused by fragmented tools and low-fidelity data. It transforms all network traffic into context-enriched, high-fidelity evidence, empowering security teams to operate with absolute confidence across on-premises, hybrid, and cloud environments.

Built on the power of Zeek®—the world's most widely used network security monitoring platform—Corelight's evidence provides the definitive foundation for your security operations.

The gold standard: Network Evidence for NDR

While traditional Network Detection and Response (NDR) often relies on proprietary "black box" scores, Corelight's Open NDR platform focuses on providing the evidence itself.

- **Explainable Detections:** Every alert is backed by structured logs, not just an attack score.
- **Comprehensive Visibility:** Covers the hard to reach parts of the network—including East-West, encrypted, and unmanaged assets—that firewalls and EDR often miss.
- **The Zeek Advantage:** Leverages 20+ years of open-source innovation to provide deep protocol analysis across 70+ data types, ensuring your detections are portable and verifiable.

Superior threat detection

See what other solutions miss. Corelight delivers deep, interconnected, high-fidelity evidence across more than 70 protocols—covering East-West traffic, encrypted channels, and unmanaged endpoints. The result: adversaries lose the advantage of hiding in shadows, and your NDR strategy is strengthened with contextual detections layered for resilient, adaptive defense.

Accelerated investigations

From alert to insight—faster. Siloed or incomplete data grinds investigations to a halt. Corelight unifies every related event and session through unique identifiers, enabling analysts to pivot swiftly from discovery to answer. With log-linked context, teams reconstruct timelines, trace attack paths, and validate incidents in a fraction of the time—reducing triage and investigation effort by more than half.

NETWORK EVIDENCE BENEFITS

Reduce risk and confidently detect threats
Fast investigations—accelerate people and platforms
Confident incident response with zero guesswork
Total control & ecosystem flexibility

Confident, defensible response

Move from confirmation to conviction. After an incident, a clear, reliable historical record is non-negotiable. Only network evidence can provide an immutable record—compact enough for long-term retention, yet rich enough for forensic precision. Corelight empowers teams to reconstruct the entire attack narrative, satisfy audit requirements, and meet legal or regulatory standards—leaving no doubt or guesswork behind.

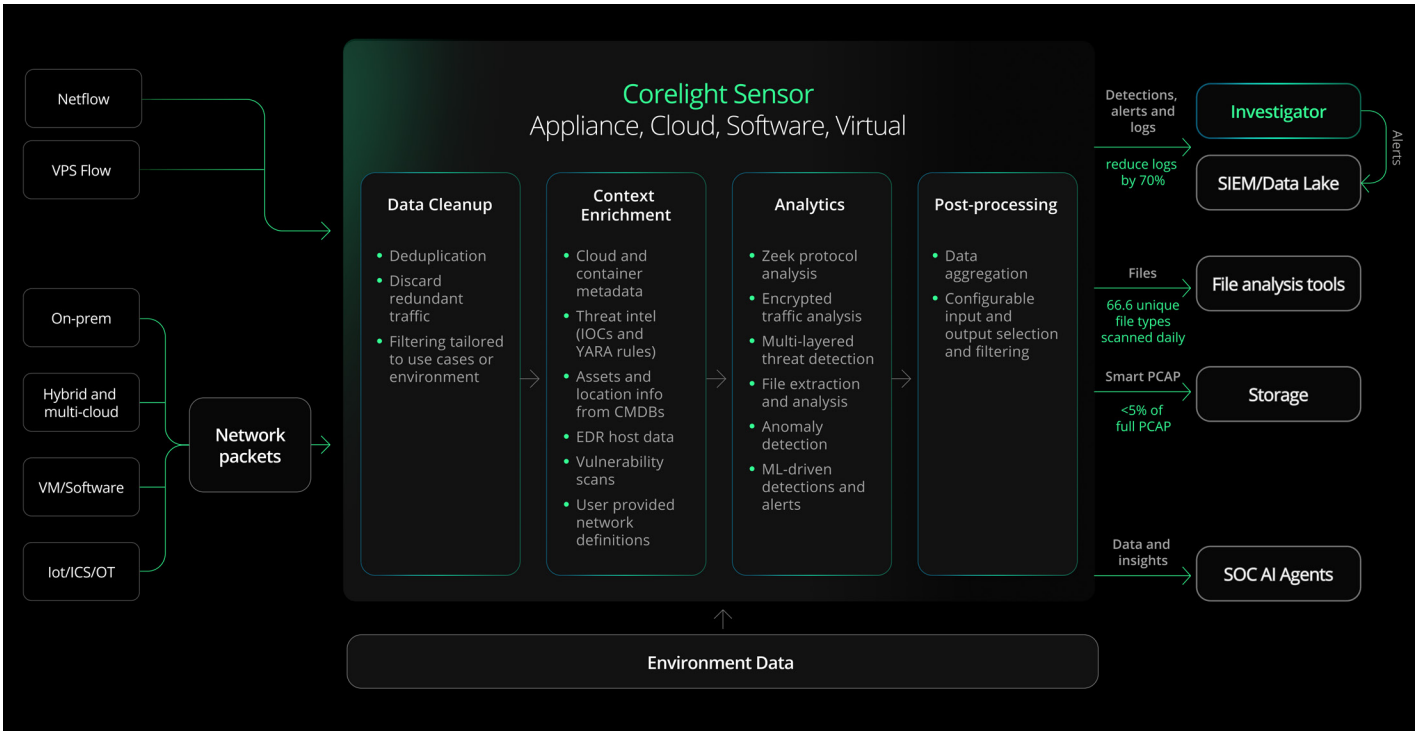
Future-proof flexibility and AI-readiness

Own your evidence. Shape your future. With data delivered in open, machine-readable formats (JSON, TSV, ASCII), Corelight sidesteps vendor lock-in and future-proofs your security architecture. Its Zeek-based, extensible platform makes integration with any security or AI system straightforward, so you can innovate on your terms—ready for tomorrow's workflows, automation, and analytics.

Transforming network traffic to evidence

The Corelight Sensor acts as a high-performance engine that transforms raw packets into actionable intelligence through a structured four-stage process:

How Corelight transforms network traffic to network evidence



1. **Capture & cleanup:** Passively captures traffic (TAP/SPAN, Cloud VPC, or NetFlow) and deduplicates data to ensure a clean, efficient dataset.
2. **Context enrichment:** Before logs are generated, the sensor injects live external context, including Threat Intel (IOCs/YARA) and Asset Identification to associate IPs with known devices and users.
3. **Deep protocol intelligence:** Zeek's analysis engine parses the traffic, extracting semantic details (like URLs, file hashes, and SSL handshakes) and linking every related event with a Unique ID (UID).
4. **Optimized output:** Data is condensed by up to 80% through smart aggregation and routed to your SIEM, data lake, or AI agents in open, machine-readable formats (JSON/TSV).

The Corelight Open NDR Platform

Only Corelight can transform raw network data, at scale, into comprehensive, actionable, and AI-ready network evidence—backed by the open-source Zeek community—empowering security teams to eliminate blind spots, cut investigation time in half, and build a flexible, best-of-breed security ecosystem while retaining true data ownership.

corelight

To learn more about Corelight's network evidence, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497