corelight

Solution brief

Performance and asset visibility powered by the Corelight Open NDR Platform

One sensor, one source of truth—unify SecOps and NetOps with asset intelligence and network performance alerting from sensors you already own

Corelight sensors already capture the high-fidelity network data required for industry-leading security evidence. Now, that same traffic unlocks two new capabilities: asset classification and intelligent network performance alerting. By extending the value of network evidence to serve both Security Operations and Network Operations teams, Corelight eliminates tool sprawl, breaks down organizational silos, and delivers a single source of network truth—with no additional hardware, no active polling, and no dedicated NetOps vendor bloat.

THE CHALLENGE

Security and Network Operations teams share responsibility for network health and performance, yet they operate with separate toolsets and workflows. This fragmentation creates blind spots, delays incident response, and drives up operational costs. Common pain points include:

- **"Is it the network?" takes hours to answer**—When users complain about slow applications, NetOps teams can face challenges proving the network is healthy—requiring multiple tools, active polling, and hours of manual investigation across disconnected dashboards
- **Understanding devices on the network**—CMDBs are incomplete or outdated. EDR agents can't cover printers, IoT, IT, or unmanaged devices. Analysts waste time asking "What is this IP?" instead of investigating real threats
- **Tool sprawl and redundant infrastructure**—Dedicated NetOps tools like SolarWinds, Riverbed, and NetScout require separate hardware, licensing, and operational overhead—adding cost without serving the security mission

THE SOLUTION

Corelight delivers performance and asset visibility from a single sensor deployment, extending the value of Zeek®-based network evidence to serve both the AI SOC and NetOps. The sensor passively extracts two new intelligence layers from traffic already being collected for security purposes:

1. **Asset classification (asset_classification)**—continuously discovers every device, OS, software version, and network role from observed traffic. Devices are classified the moment they communicate, including unmanaged endpoints, IoT, and shadow IT that bypass traditional inventory tools

2. **Network performance alerting (net-perf)**—an anomaly-first architecture that generates intelligent, domain-aware alerts only when configurable performance thresholds are crossed. Alerts are correlated to actual service names rather than ephemeral IP addresses

Asset intelligence: Know what's on your network

- Passively fingerprint and classify every device—servers, workstations, IoT, IT—from observed traffic
- Continuously update OS versions, application banners, and client fingerprints in real time, not on a scheduled poll
- Surface unmanaged endpoints, IoT, and shadow IT that bypass traditional inventory tools
- Unify asset intelligence across physical sensors, cloud software sensors, and VPC traffic mirroring

Performance anomalies: Answer "Is it the network?" in minutes

- Receive domain-aware alerts correlated to actual service names, not abstract IP addresses
- Instantly isolate faults with placement-aware client vs. server RTT decomposition (cli_rtt and svr_rtt)
- Pivot directly from a performance alert to the exact connection log via the first-trigger UID for rapid forensic investigation
- Toggle on-demand enrichment (enrich_logs=T) to append full-resolution delay metrics to standard Zeek logs for definitive evidence

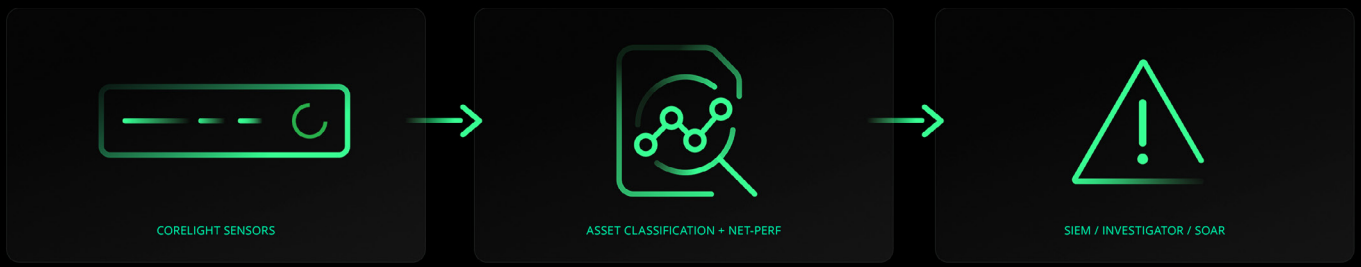
Tool consolidation: One sensor for SecOps and NetOps

- Consolidate security and network performance monitoring into a single platform—no additional hardware or agents
- Eliminate the "swivel chair" effect between disconnected IT, CMDB, and security tools
- Deliver tangible value to NetOps from your existing security investment
- Pre-built dashboards for Investigator or your SIEM, ready out of the box

HOW IT WORKS

1. Corelight sensors (physical, virtual, or cloud) passively observe mirrored network traffic. Zeek parses this traffic into rich protocol logs.
2. Asset classification analyzes network evidence to identify and categorize every device on the network, emitting a dedicated asset_classification.log
3. Net-perf monitors performance thresholds and fires domain-aware alerts only when configurable performance thresholds are exceeded, writing to net_perf.log with a direct forensic pivot (UID) to the triggering connection
4. Logs integrate directly into Investigator, existing SIEMs, and SOAR platforms—enriching every security alert with asset identity and performance context

The solution architecture



1. Passive traffic observation

2. Classify assets & detect performance anomalies

3. Enriched alerts with asset + performance context

To learn more about performance and asset visibility, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497