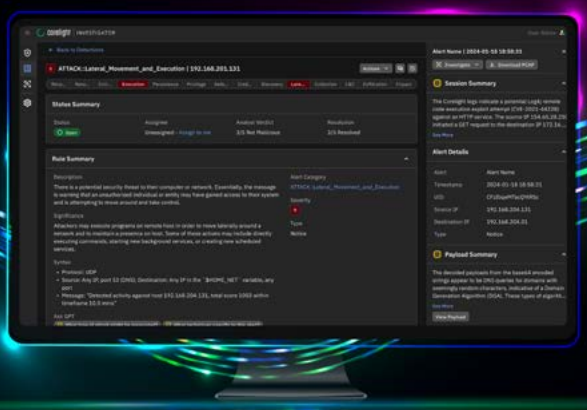
corelight

Data sheet

Investigator

Reduce triage time by up to 50%
with Corelight's Open NDR Platform



Corelight's SaaS-based Network Detection and Response Platform (Investigator) delivers prioritized alerts, automates workflows, and leverages AI to explain the expert-level data needed for triage in plain language—all while reducing SIEM ingest.

ACCELERATE INCIDENT RESPONSE

It has become increasingly difficult for SOC analysts to keep up with the volume of alerts while facing screen fatigue, excessive false positives, and an expanding attack surface. With Investigator, analysts can:

- Receive high-fidelity, prioritized alerts
- Leverage interactive visual timelines to create an accurate view and gain additional context
- Quickly access triage history, including true and false positive history, past remediation to expedite triage
- Gain an instant understanding of alerts, payloads, and next steps with AI-powered summaries and explainers
- Pivot to pre-correlated, raw data without leaving the interface

PLATFORM BENEFITS

Accelerate triage and incident response

Reduce SIEM ingest (and cost)

Increase detection coverage

Consolidate tools and datasets

Integrate with existing SOC tools

Easy to deploy, scale, and customize

Based on open, global standards

INCREASE SOC EFFICIENCY

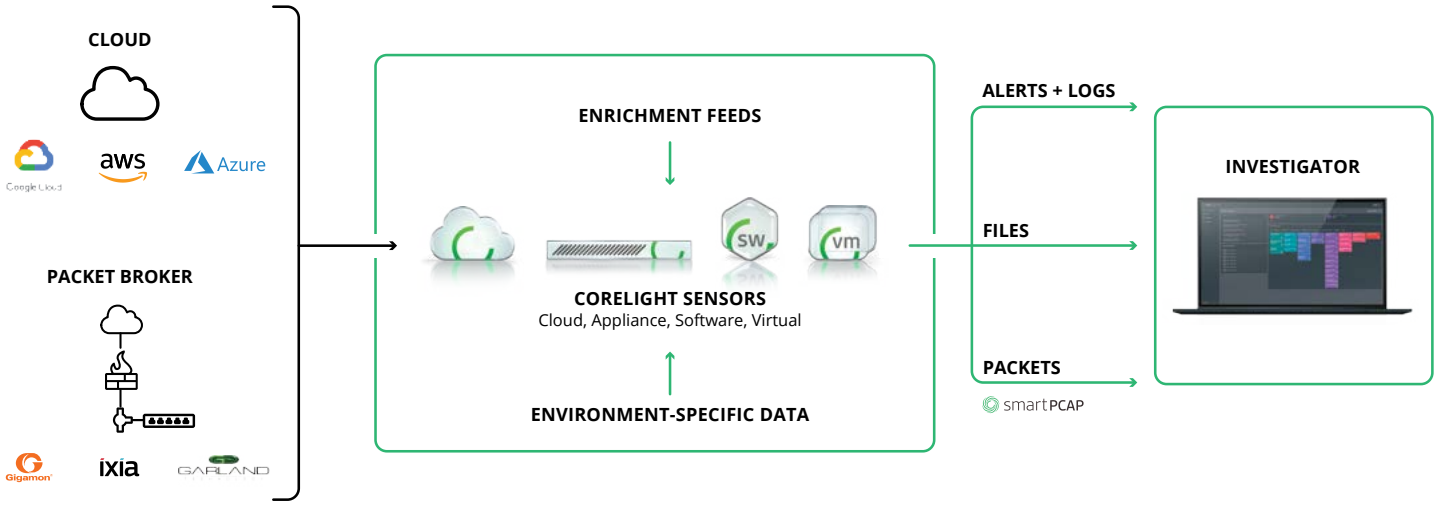
Today's SOC teams struggle with many—and often poorly integrated—tools for infrastructure monitoring and threat detection, in addition to analyst shortages and skill gaps. Investigator increases SOC efficiency by:

- Delivering AI summaries of alerts, payloads, and contextual data while directing the analyst to next steps for investigation
- Consolidating NSM, IDS, and PCAP functionality
- Providing a unified dataset across hybrid and multi-cloud environments
- Capturing alert payload bytes versus entire packets
- Streamlining workflows: one-click takes analysts from prioritized alert to a single-screen triage with pre-correlated context

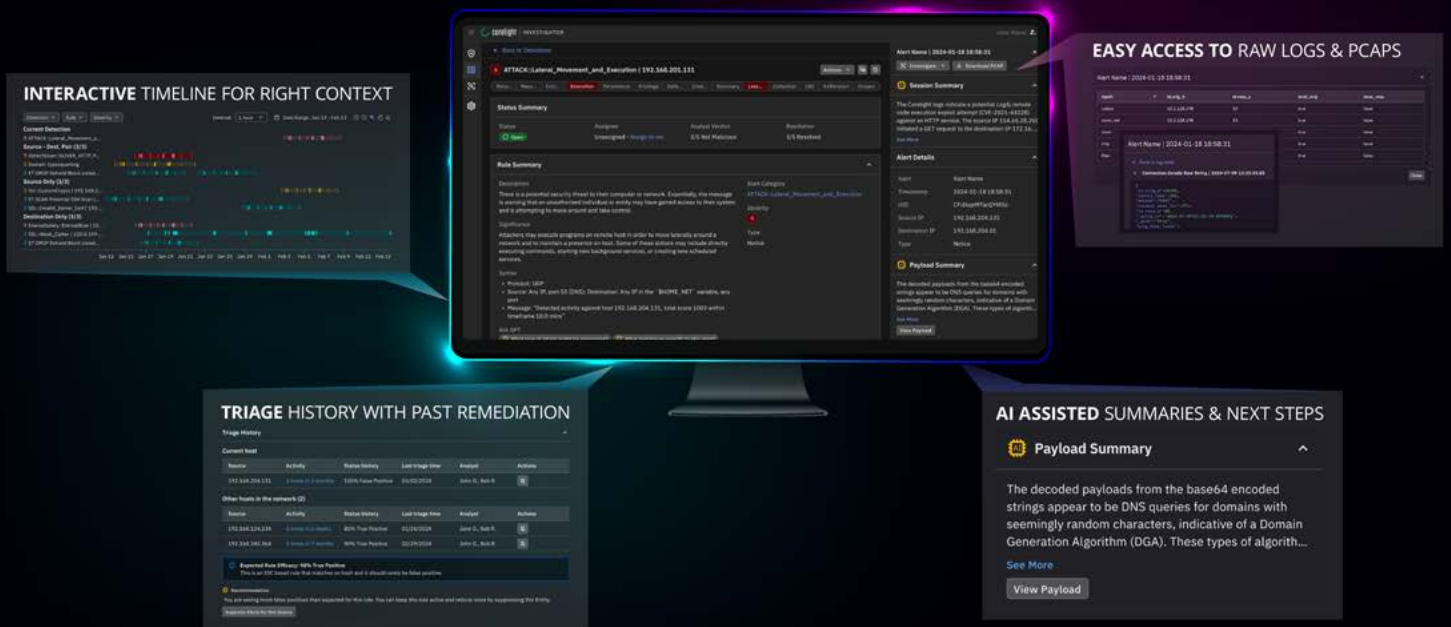
INCREASE DETECTION COVERAGE

Security teams are under constant pressure to reduce the time to detect, but staying ahead of the ever-changing threat landscape continues to be challenging. Detection engineering and custom tuning resources are not readily available in most SOCs, yet the requirement for high-fidelity alerts and complete detection coverage persists. Investigator delivers a comprehensive suite of detection options, covering:

- Transparent AI/ML models
- Behavioral, signature, threat intel, and queries
- Encrypted traffic threat inferences
- Comprehensive MITRE ATT&CK® mapping to uncover 80+ techniques, with exceptional visibility into adversary methods used for Defense Evasion, Credential Access, Discovery, and Command and Control



Corelight alerts and evidence stream from deployed sensors to Investigator for triage and incident response. Investigator also exports to a number of SIEM and XDR solutions.



CLOSE MORE CASES, FASTER. FEATURES INCLUDE:

- Prioritized alerts: alerts are provided with customizable severity scores
- AI explainers: plain-language summaries are provided for alerts, payloads, and contextual data
- Host and network context: auto-classify devices and gain insights into network connections
- Interactive timeline: quickly identify whether other events took place—and when—on the same hosts
- Easy investigation pivots: quickly access raw log data and PCAP for deeper investigation
- Triage history: easily see true and false positive history, analyst activity, notes, and more

SINGLE SCREEN TRIAGE

Interactive visual timelines assist in mapping alerts on related hosts with direct access to the pre-correlated context. Triage history gives analysts on-the-job knowledge by showing historical context that includes activity and actions taken on commonly served alerts. For deeper investigations, raw log data and PCAP downloads are one click away.

> **“A fantastic force multiplier, surfacing correlated information quickly and concisely to help analysts make faster decisions with more complete details.”**

–Information Security Operations Architect
Sally Beauty Supply

LEVERAGE THE POWER OF AI

The power of AI combined with direct access to rich evidence from Corelight provides unparalleled visibility across your network. From simplified explainers of expert-level data, to finding C2 channels and identifying malware, AI continues to be a powerful tool in Corelight's analytics toolbox.

Corelight's supervised and deep learning ML models allow for targeted and effective detections that minimize the false positives commonly associated with some other types of ML models. Corelight's models can identify behaviors like domain generation algorithms (DGAs), which may indicate a host infection, watch for malicious software being downloaded, and identify attempts to exfiltrate data from an organization through covert channels like DNS. Corelight also uses deep learning techniques to identify URLs and domains that attempt to trick users into submitting credentials or installing malware, helping to stop attacks early in the life cycle.

KEY CAPABILITIES

Complete visibility	Eliminate blindspots in your network with a focus on durable detections including machine learning, behavioral analysis, query based alerts, and signatures
Toolset and dataset consolidation	Deliver NSM, IDS, and PCAP functionality in a single architecture with uniformity of datasets across hybrid and multi-cloud environments
Prioritized alert delivery	Reduce false positives and focus on what matters with intelligent alert scoring and direct access to pre-correlated data
AI-driven insights	Harness the power of AI to provide clarity and context, turning expert-level data into plain language and actionable intelligence while being one click away from raw data
Single screen triage	Close cases faster by conducting investigations within a single screen with AI summaries explainers, interactive visual timelines, and triage history
Open platform	Security teams have complete control over their data. Create custom detections and filters, integrate with your security stack, and extend your data without vendor lock-in

corelight

info@corelight.com | 888-547-9497