Joint solution

Modernize SecOps with Corelight & Elastic Security

Empower your SOC with deep network visibility, insights, and faster threat response

Security Operations Center (SOC) teams face severe visibility gaps when they lack high-quality network telemetry. Relying solely on endpoint data and traditional logs leaves analysts with incomplete context about operational and adversarial activities moving across the hybrid environment. Without deep visibility into north-south and east-west traffic, detection accuracy drops and alert fatigue sets in. These blind spots force your team into slower manual investigations, ultimately reducing confidence and increasing your mean time to respond to active threats.

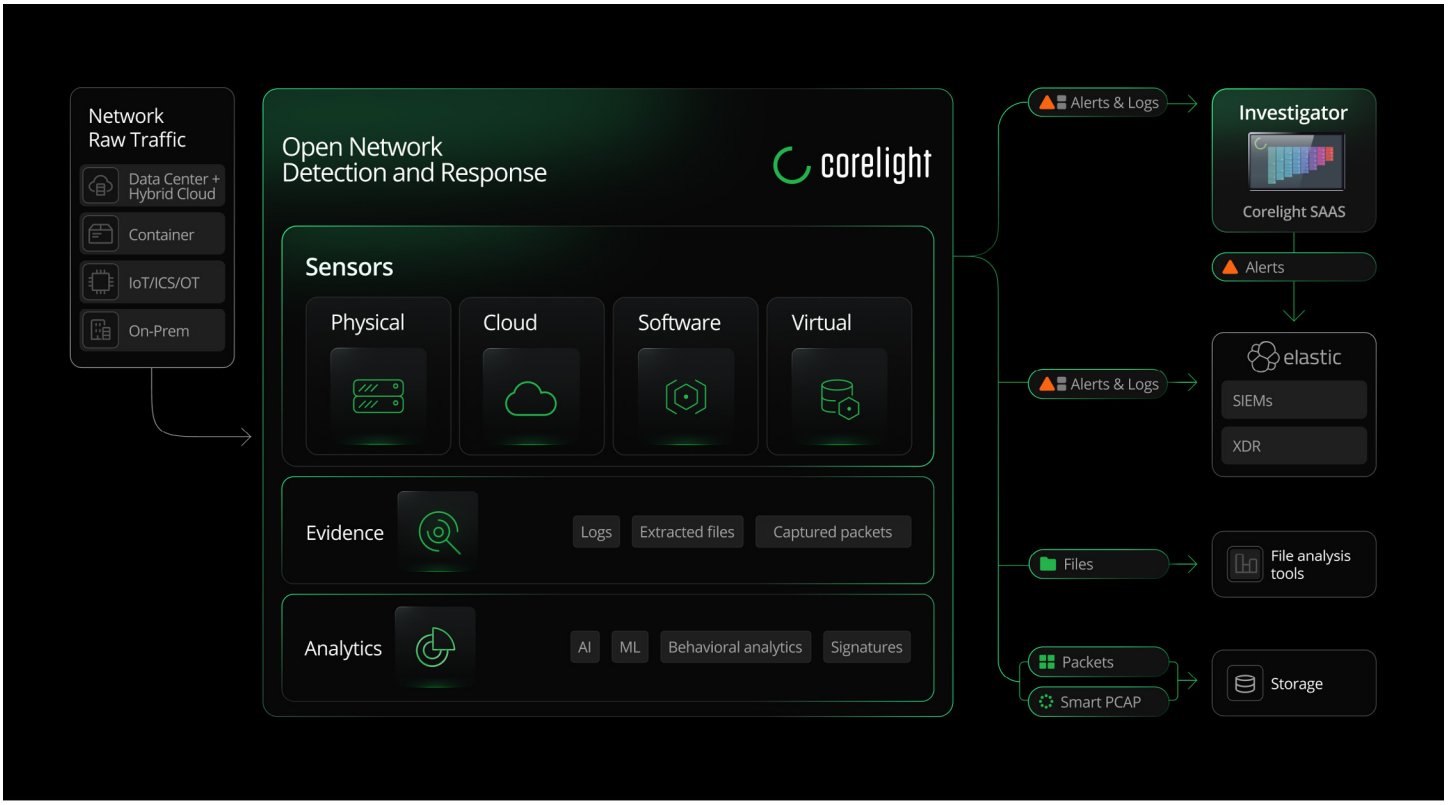
Integrating Corelight's network evidence with Elastic SIEM and XDR turns your data into decisive action. To that end, Corelight provides native support for Elastic Common Schema (ECS) to deliver unparalleled visibility that breaks through the noise and supercharges network detections across north-south, east-west, and everywhere in between. With seamless correlation and advanced analytics, your SOC team can spot complex threats faster, accelerate investigation queues, and respond with clarity and speed. The Corelight-Elastic integration does more than eliminate the traditional blind spots in threat visibility; it empowers your team to act quickly with the confidence you need to stay ahead of today's increasingly sophisticated, AI-enabled adversaries.

INTEGRATION HIGHLIGHTS

- Supercharge detection, investigation, and response
- Eliminate blind spots in threat visibility across all network traffic
- Advanced analytics to identify 75+ MITRE ATT&CK TTPs
- Accelerate time to value with pre-built dashboards, detection rules, and queries

Accelerate investigations and response times while streamlining workflows

With full-protocol, entity-rich evidence across 70+ data types delivered out of the box, Corelight provides SIEM analysts using Elastic Security a clear picture of all the activity across their global networks. Intuitive dashboards provide at-a-glance views of an organization's security posture and visual insights into potential threats. With summary charts, counters, and maps, SOC analysts can quickly discern trouble spots and drill down into details to validate threats. This clarity and guidance, along with pre-defined workbooks, detection rules, and queries, provide focus where it's most needed to accelerate investigations and response times while streamlining workflows.



Accelerate time to value with native integration.

corelight

To learn more about the Elastic integration, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497