Joint solution brief

Corelight for SentinelOne Singularity Platform

Simplify investigations and prioritize alerts according to risk with integrated network, endpoint, and vulnerability data directly in the network sensor.

Security teams struggle to maintain an effective security posture for their organizations because their legacy security tools often can't support today's modern infrastructures or increasingly sophisticated adversaries. Moreover, the overwhelming volume of alerts from the legion of devices across the environment and the lack of visibility into unsecured and unknown devices is wearing down analysts grappling with too much data but not the right insights.

SOLUTION HIGHLIGHTS

- Superior visibility into all network traffic and devices
- Enhance detections with Singularity-enriched evidence in the Corelight sensor
- Simplify investigations and prioritize alerts according to risk
- Immutable network evidence that goes back months for compliance

Unify network and Singular Endpoint telemetry in a single console

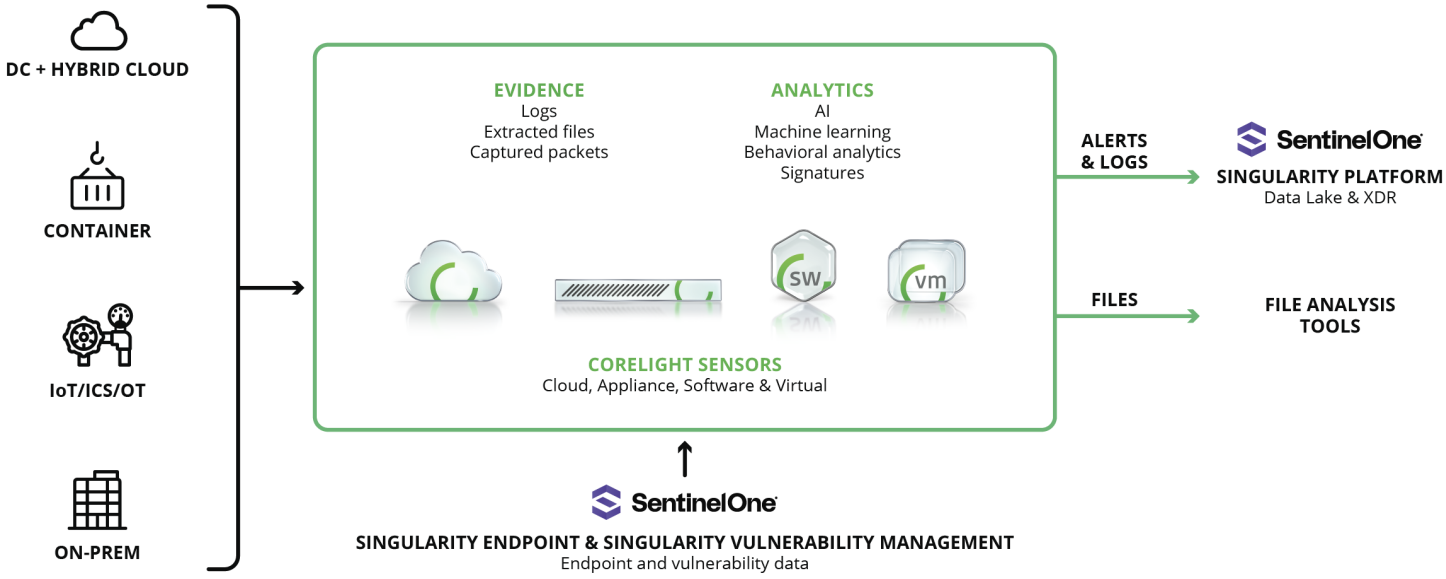
DISRUPT FUTURE ATTACKS WITH ENRICHED NETWORK EVIDENCE

Native Corelight integration across the SentinelOne Singularity Platform can address these common challenges. Based on the design pattern of elite defenders, Corelight's Open Network Detection & Response (NDR) Platform provides detections, evidence, and insights that amplify the speed and efficiency of threat investigations. By enriching Corelight logs with Singularity endpoint and vulnerability data, security teams can more effectively detect and prioritize threats based on current risks to the environment.

Enrichment of relevant data at the point of observation in Corelight sensors helps analysts streamline and accelerate investigations, as well as regain control of the overwhelming volume of alerts pouring into the security operations center (SOC). Additionally, integration of SentinelOne's leading endpoint detection and response (EDR) with Corelight's advanced NDR provides a comprehensive view of all network activity across hybrid and multi-cloud environments, including support for unsecured and unknown endpoints.

Easily deployed and available in on-premise, cloud, and SaaS-based formats, Corelight combines the power of open source and proprietary technologies to deliver a complete Open NDR Platform that includes modern intrusion detection (IDS), advanced network security monitoring, and Smart PCAP solutions for complete visibility and protection.

Native integration streamlines and accelerates investigations



Simplify investigations and prioritize alerts according to actual risk to the enterprise with integrated network, endpoint, and vulnerability data.

SOLUTION BENEFITS

With full contextual and integrated endpoint, vulnerability, and network data now available directly from Corelight network sensors, analysts can simplify and accelerate their investigations for a more secure posture across the enterprise.

COMPLETE VISIBILITY

Spot early-, mid-, and late-stage signs of network compromise with superior visibility into all network traffic across the enterprise, including support for devices that can't support endpoint agents. Singularity-enriched Corelight evidence and detections can go back many months for retrospective look-backs.

IMPROVE NETWORK DETECTION AND COVERAGE

Expand detection and prioritize threats according to their verified risks to the environment with enrichment of Corelight network telemetry with SentinelOne endpoint and vulnerability data at the point of observation directly in the network sensor.

ACCELERATE RESPONSE

By pre-correlating Corelight Entity Collection or Known Hosts logs with Singularity Endpoint Agent UUIDs (at the point of observation in the sensor), SOC teams can pivot seamlessly between NDR and EDR data, as well as identify unmanaged endpoints in real-time.

INCREASE OPERATIONAL EFFICIENCY

Boost analyst efficiency and reduce data costs in downstream analytics with 4:1 consolidation of legacy tools that provides uniform network telemetry across on-premise, hybrid, and multi-cloud environments. Simplify compliance requirements with immutable network evidence that goes back months not days.

corelight

To learn more about Corelight for SentinelOne, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497