JOINT SOLUTION

Corelight and CrowdStrike Falcon® Insight XDR optimize visibility, detection, and threat hunting

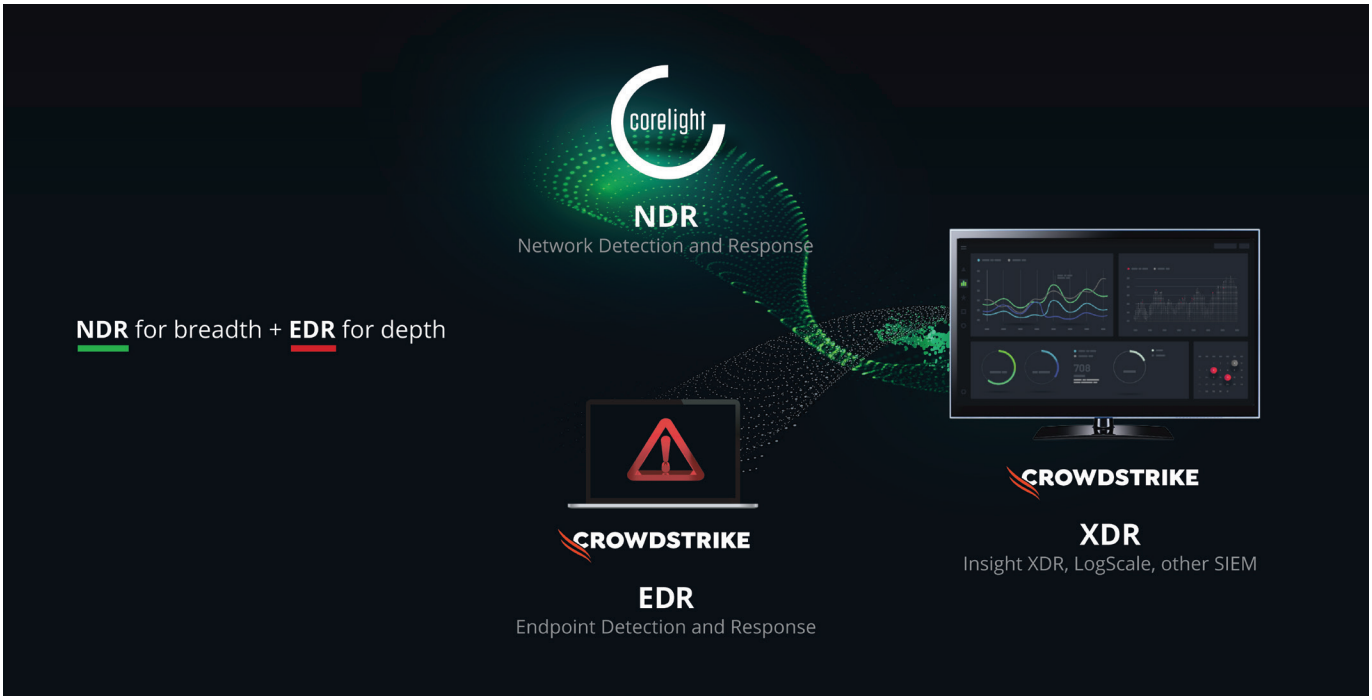
Security operations teams continue to struggle to keep their environments safe with most acknowledging that the growing patchwork of tools cobbled together over the years is hindering their ability to respond effectively. And with the wide adoption of cloud, the proliferation of smart devices, and the appeal of microservices development architectures, threats are getting more complicated and difficult for security teams to keep up with.

Corelight and CrowdStrike offer a solution that simplifies how security operations center (SOC) teams respond to these increasingly sophisticated cyberthreats. By transforming all network data into comprehensive, correlated evidence and analytics, Corelight enables CrowdStrike customers to combine the most advanced network detection and response (NDR) with their endpoint detection

INTEGRATION HIGHLIGHTS

- Open NDR optimized for CrowdStrike Falcon Insight XDR
- Correlated alerts and full contextual evidence
- Designed for years-long threat investigations and detections
- Integrated data and dashboards in a single pane of glass
- Advanced network telemetry to support XDR and Zero Trust initiatives

CORELIGHT FOR FALCON INSIGHT XDR



Corelight's rich network evidence integrates seamlessly with CrowdStrike Falcon Insight XDR to provide the breadth of NDR and the depth of EDR to enable SOC teams to detect and respond to threats faster and easier than ever.

and response (EDR) into an integrated solution that overcomes the complexity that until now seemed out of reach. The result is a modern SOC Visibility Triad that helps SOC teams find and respond to threats faster and easier than ever.

Corelight transforms network traffic into comprehensive, correlated network evidence that integrates seamlessly with CrowdStrike Falcon XDR. Combined, this solution delivers the breadth of NDR and depth of EDR enabling SOC teams to find and respond to threats at new levels of speed and accuracy, and tame the exponential growth of security alerts and incidents to ensure their organizations are secure.

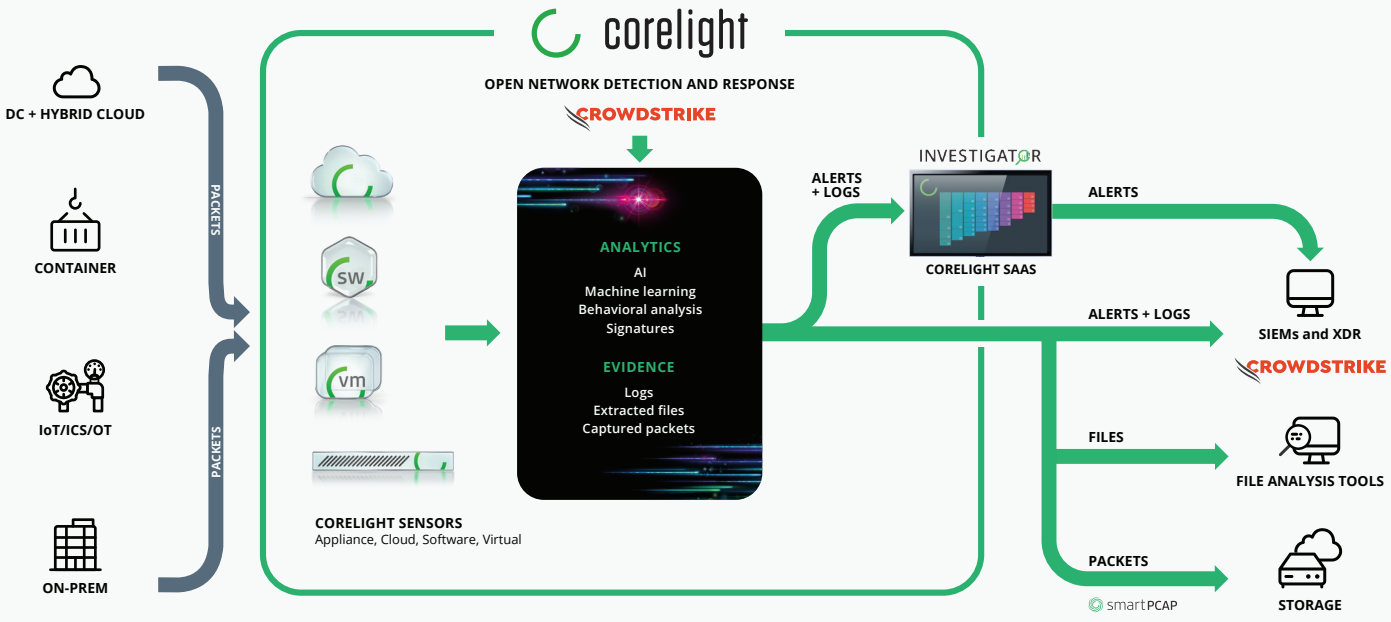
MATURING TOWARD A FULL SOC VISIBILITY TRIAD SOLUTION

Because of its high fidelity network evidence, analytics, and breadth of coverage, Corelight's Open NDR Platform is an ideal first line of defense for detecting threats that legacy tools often miss. By correlating and linking log data from over 50 protocols through passive network monitoring, Corelight provides security analysts using CrowdStrike Falcon Insight XDR a clear picture of all the activity across their global networks.

Native integration helps resource-constrained SOC teams simplify deployment and alert triage by ingesting pre-formatted, correlated network evidence and analytics directly into CrowdStrike data lakes. This helps provide a holistic view of the environment, including context for device inventory, and respond quickly to alerts to mitigate advanced threats from a single pane of glass.

Along with native data integration, the Corelight App for LogScale also includes pre-defined workbooks, custom dashboards, sample queries, and analytic rules to help SOC teams accelerate investigations, incident response, and threat hunting. And with an open and flexible design based on the open-source Zeek and Suricata platforms, Corelight is a preferred NDR partner for Falcon Insight XDR.

CORELIGHT OPEN NDR AND THE CROWDSTRIKE FALCON PLATFORM



SOLUTION BENEFITS

COMPLETE VISIBILITY

As an inaugural member of CrowdStrike's XDR Alliance program, Corelight enables CrowdStrike customers to accelerate threat detection and response with detailed network evidence of all their network traffic, including telemetry on unmanaged devices and those unable to support endpoint agents.

NEXT-LEVEL ANALYTICS

Corelight's high-fidelity telemetry supercharges threat detection and response for Falcon Insight XDR. Corelight Collections further amplify detections with insight into encrypted traffic, command and control activities, and more.

FASTER INVESTIGATION

By correlating alerts, evidence, and packet data, Corelight's contextual evidence integrates directly into CrowdStrike dashboards and workflows to simplify and accelerate investigations.

EXPERT HUNTING

Combining Corelight's rich network telemetry with CrowdStrike EDR enables your team to investigate alerts faster and easier than ever so even junior analysts can be expert threat hunters too.

To learn more about the CrowdStrike integration, request a demo at **https://corelight.com/contact**

CrowdStrike, a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity, and data. Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities. Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. On-prem and in the cloud, our open Network Detection and Response Platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology.

info@corelight.com | 888-547-9497