JOINT SOLUTION

Corelight for CrowdStrike® Falcon Next-Gen SIEM

Disrupt future attacks by harnessing detections, evidence, and insights from the world's leading Open NDR Platform

LEGACY TOOLS CAN'T KEEP PACE WITH ADVERSARIES

Modern IT and security complexity, outdated Intrusion Detection Systems (IDS), and legacy SIEMs have made protecting networks more complex, resulting in insufficient monitoring and slow threat response. Security teams are overwhelmed by the volume of alerts, hampering their operational efficiency. Cybercriminals exploit this by-bypassing legacy endpoint detection and response (EDR) systems, targeting the less monitored network periphery, and rapidly spreading through networks by attacking areas with limited visibility.[1]

INTEGRATION HIGHLIGHTS

- Detect network threats in real time at the point of observation
- Close visibility gaps and validate network inventory
- Reduce MTTR with Falcon-enriched Corelight evidence
- Expose hidden attacks with rich, lightweight telemetry
- Improve operational efficiency and reduce complexity

UNIFY NETWORK AND FALCON TELEMETRY IN A SINGLE CONSOLE

Unify Corelight evidence (shown as a blue 'Remote Services / Remote Desktop Protocol' indicator of lateral movement) with Falcon endpoint, identity, and cloud data in Falcon Next-Gen SIEM for full visibility and protection.

[1] CrowdStrike 2024 Global Threat Report

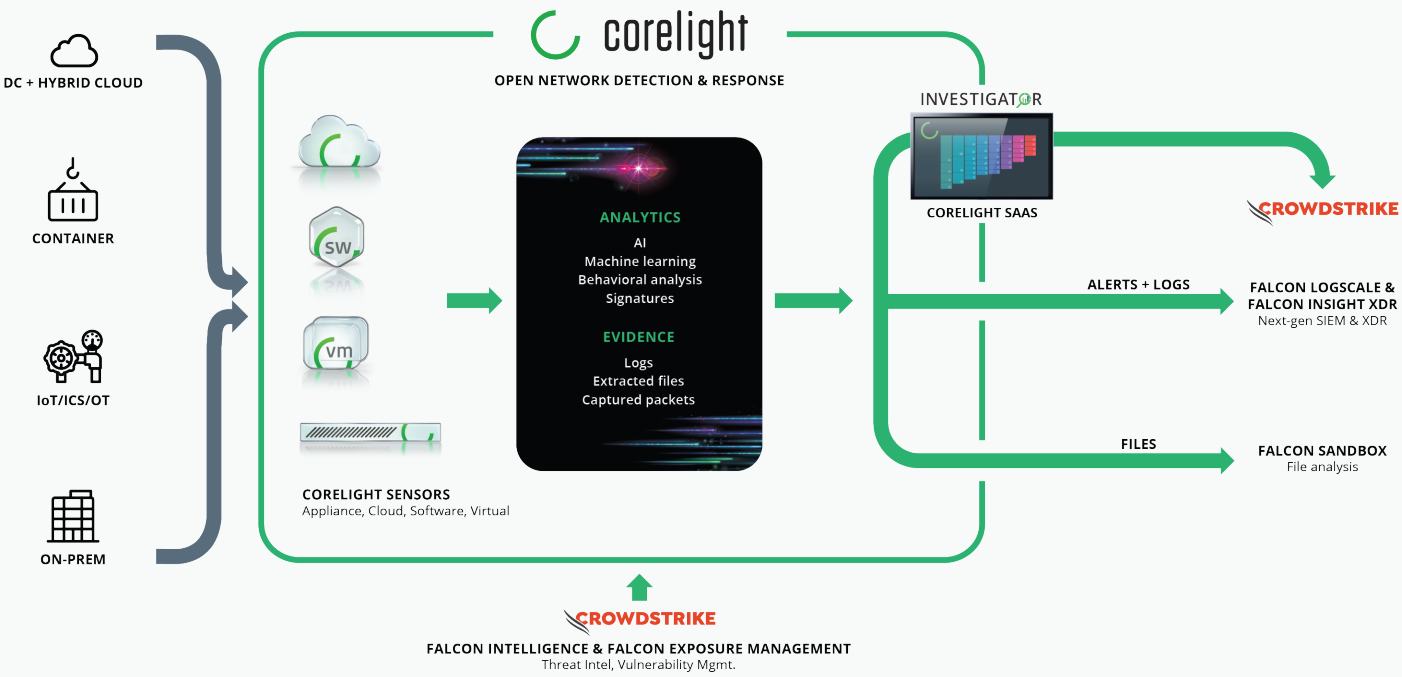
DISRUPT FUTURE ATTACKS WITH NETWORK EVIDENCE

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 incident response in CrowdStrike Falcon Next-Gen SIEM so you can quickly evict adversaries while increasing operational efficiency.

Your team can detect and respond faster with risk-based alert prioritization, quick pivoting to endpoint, workload, identity, and additional security telemetry, and the application of CrowdStrike's world-class intelligence at the point of observation on the network. Your threat hunters can scour rich network telemetry that provides the context to reduce dwell time and find hidden attacks—yet is lightweight enough to be stored for years within the Falcon platform.

The Corelight Open NDR Platform transforms network and cloud activity into evidence. Easily deployed and available in on-prem 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), network security monitoring, and Smart PCAP solutions for complete visibility and protection.

NATIVE INTEGRATION IMPROVES OPERATIONAL EFFICIENCY



Native integration and out-of-the-box workflows for CrowdStrike Falcon improve operational efficiency by consolidating tools, streamlining data onboarding, and reducing complexity compared to legacy tools.

SOLUTION BENEFITS

IMPROVE NETWORK DETECTION COVERAGE

Expand detection and speed incident workflows in Falcon Next-Gen SIEM with third-party network detections and comprehensive indicators for threats, including lateral movement and encrypted attacks. Find and investigate evasive threats with AI-powered detections and full contextual insights from Corelight directly within the Falcon platform. Use Corelight Sensors to expand detection coverage by leveraging CrowdStrike Falcon Intelligence Premium rules that can only be instrumented on the network.

ACCELERATE RESPONSE

Ingest full network telemetry from Corelight into the Falcon platform for a rich, pivotable history of everything that crosses your network, enabling analysts to make connections quickly and confidently from within CrowdStrike's threat-centric command console. Tie Corelight alerts to CVEs identified by CrowdStrike Falcon® Spotlight to enable risk-based alert prioritization of exploits against known vulnerable hosts. Quickly pivot between network, endpoint and beyond using Corelight logs pre-correlated with Falcon Sensor IDs in Falcon Next-Gen SIEM.

INCREASE OPERATIONAL EFFICIENCY

Consolidate toolsets and move faster with connected data in one place. Automate manual data tasks and store more data while saving on costly maintenance. Accelerate deployment with over 20 native dashboards, 25 correlation rules, and 60 queries designed specifically for Corelight third-party data in Falcon Next-Gen SIEM.

GET COMPLETE VISIBILITY

Gain a commanding view of your organization and all devices that log onto your network—including endpoints that may lack the Falcon agent or cannot support sensor deployment. Reduce asset inventory gaps using Corelight's Entity Collection to identify unmanaged endpoints.

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