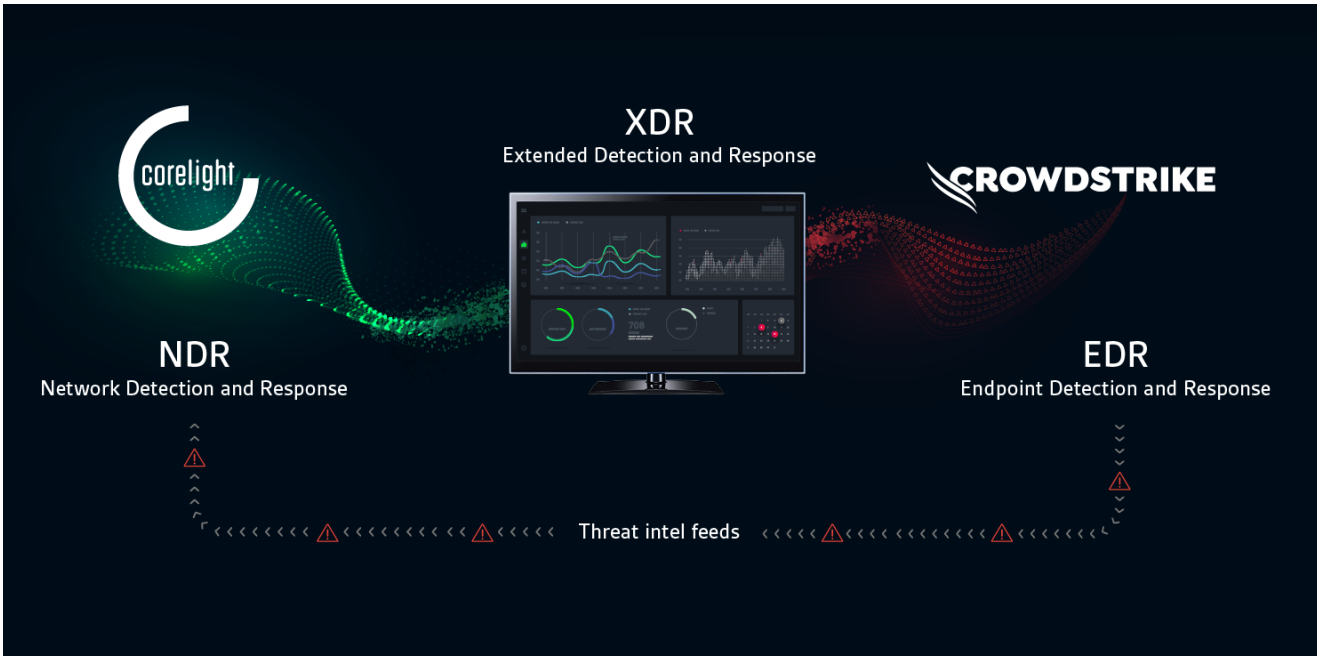
Joint Solution

CrowdStrike + Corelight

Combining Falcon X™ threat intelligence with Corelight's network evidence unlocks extraordinary power, without more work.



Corelight's Network Detection and Response combines rich network telemetry with world-class endpoint threat intelligence from the CrowdStrike Falcon® platform to eliminate blind spots and detect intrusions across on-premises, multi-cloud, and hybrid environments.

Joint Solution: **Corelight + CrowdStrike**

Key benefits

Security for every device
Radically improve detection coverage, especially for high value assets, unmanaged devices, cloud and IoT.

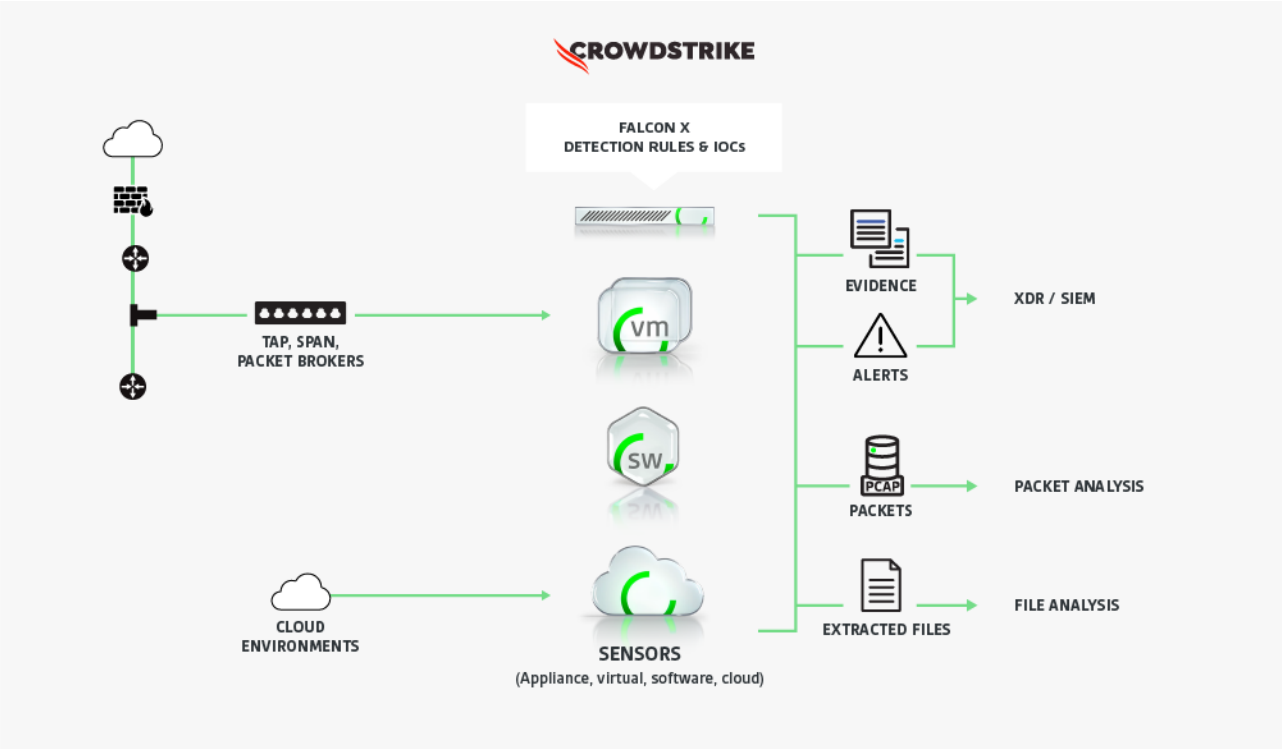
Unified threat intelligence
Leverage detections and IOCs across endpoints and networks for unified threat detection.

Industry leading intel, rules, and evidence to move quickly and decisively to respond to detected threats.
Get the best endpoint intelligence integrated with the best network evidence and alerts.

Close MITRE ATT&CK® gaps
Cover more of the attack chain by correlating endpoint intelligence with proprietary insights into network traffic to assess and find evidence of many TTPs.

Accelerate threat detection
Utilize both Corelight proprietary detections and Falcon X threat intelligence by applying matches on live network traffic, not just SIEM history.

Integration details



Joint Solution: Corelight + CrowdStrike

How it works

Corelight Sensors perform deep analysis on traffic from on-premises, multi-cloud, and hybrid environments to generate alerts that are embedded directly into rich, comprehensive evidence that reduces alert fatigue and speeds up investigations. The sensors pull detection rules and indicators of compromise (like email addresses and DNS names) from Falcon X, and correlate that threat intelligence with observed network behavior. The resulting evidence, alerts, packets and extracted files can be pushed to SIEMs and XDR systems like Humio, packet analysis tools like Wireshark, and file analysis tools like Falcon Sandbox.

"As cyber threats increase in number and complexity, the importance of solutions like Corelight has never been greater, providing increased visibility and comprehensive data that allows organizations to identify vulnerabilities and resolve security issues faster."
– Michael Sentonas, CTO at CrowdStrike

The Corelight + CrowdStrike advantage

- NDR built on open, universal standards, making integration easier with the data and technology you already use
- Suricata alerts embedded directly into Zeek evidence, putting every detection into context to save time, cut alert backlogs, and improve analytics
- CrowdStrike's global team of nation-state and eCrime experts expose sophisticated threats with groundbreaking research

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

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform's single lightweight-agent architecture leverages cloudscale artificial intelligence (AI) and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates over 5 trillion endpoint-related events per week in real time from across the globe, fueling one of the world's most advanced data platforms for security

Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders.

info@corelight.com | 888-547-9497