Joint Solution

Corelight for CrowdStrike Services

Comprehensive network security monitoring for incident response and compromise assessment

Blind spots, combined with the silent failure of traditional cybersecurity solutions, prolong the time needed to detect intellectual property (IP) theft, disruptive malware attacks, and data breaches. In addition, many organizations struggle to defend the Internet of things (IoT), such as smart medical or manufacturing devices, which lack the protection of traditional endpoints and are susceptible to attacks over the network.

The solution to these challenges lies on the network. By monitoring your network holistically, you can uncover the ground truth of your environment and use it to detect and disrupt current and future intrusions.

Adversaries can't evade the network: Virtually all attacks must cross a network, and in doing so, attackers create a trail of evidence.

The network doesn't lie: The network offers defenders a source of truth that attackers cannot alter.

Network visibility drives knowledge: Comprehensive visibility gives teams operational awareness and an asymmetric knowledge advantage over adversaries.

Knowledge fuels disruptive defense: By understanding your environment and acting quickly, you can disrupt or contain attacks and improve your security posture.

Complete network visibility

Corelight for CrowdStrike Services provides extensive network security capabilities for more efficient and effective assessment, response, and ongoing monitoring. Corelight adds unparalleled visibility into your network through a unique partnership that enables CrowdStrike Services teams to investigate faster, hunt for unknown attacks, close visibility gaps, and even disrupt future threats.

Corelight's on-prem and cloud sensors go anywhere to capture industry-standard telemetry and insights for seamless ingestion into the CrowdStrike Falcon platform, extending coverage to every device on the network–including unmanaged endpoints and IoT.

The benefits of Corelight for CrowdStrike Services

COMPLETE VISIBILITY
Gain visibility across your entire network and learn if attackers have breached your defenses and are moving unnoticed in your environment.

FASTER INVESTIGATIONS
CrowdStrike consultants' skills and experience, combined with multifaceted detection from Corelight, allow security teams to respond and contain incidents faster and more efficiently.

EXPERT HUNTING
Network evidence equips CrowdStrike's highly skilled and experienced analysts with fertile hunting grounds to proactively detect new and unknown attacks using network metadata.

DISRUPT FUTURE ATTACKS
Corelight network sensors used by CrowdStrike analysts are available to you for future use with the Falcon platform, ensuring that you can both improve your security posture and stop future breaches.

Why Corelight?

- The only Network Detection & Response (NDR) vendor to receive a strategic investment from CrowdStrike's Falcon Fund
- Enterprise-class, Open Network Detection & Response Platform
- Founded by the creators and maintainers of Zeek®–the global standard for network security monitoring
- Proprietary detection technology augmented by continuous engineering from open source communities
- Hundreds of proprietary detections covering lateral movement, command and control, encrypted threats and more
- Proven in 300+ of the largest and most critical enterprises and government agencies in over 16 countries
- World-class enterprise support, with highest percentile ratings for customer satisfaction

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

The Z and Design mark and the ZEEK mark are trademarks and/or registered trademarks of the International Computer Science Institute in the United States and certain other countries. The Licensed Marks are being used pursuant to a license agreement with the Institute.