Joint Solution

Corelight NDR powers CrowdStrike Services for Healthcare Organizations

Stop breaches and quickly respond to incidents

Healthcare organizations face unique cybersecurity challenges, with patient data at risk and increased susceptibility to ransomware, backdoors, rogue software updates, and other cyberattacks. These attacks often target IoT and medical devices that do not support endpoint agent software yet store or access patient health information (PHI) via applications such as Cerner, Epic, and Citrix, endangering patient privacy and safety.

The solution to these challenges lies on the network. Corelight for CrowdStrike Services provides extensive network security capabilities, delivering unparalleled visibility and protection for your organization's infrastructure. By using Corelight Open NDR, CrowdStrike consultants can uncover the ground truth of your environment and use best-in-class evidence to detect and prevent 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 does not 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.

The benefits of Corelight for CrowdStrike Services

EXPAND VISIBILITY

Gain visibility across your entire network, extending coverage to every device on the network–including medical, clinical, and guest wired or wireless devices. Corelight Sensors deploy passively out-of-band, ensuring zero disruptions or performance impact.

ACCELERATE INCIDENT RESPONSE

CrowdStrike consultants' expertise, combined with Corelight's multifaceted detection capabilities, enable security teams to respond and contain incidents faster and more efficiently, reducing impact to patient care.

IMPROVE DETECTION COVERAGE AND ACCURACY

Identify potential breaches and monitor attacker movements within your environment. Network evidence allows CrowdStrike's skilled analysts to proactively detect new and unknown attacks using network metadata, safeguarding your healthcare organization from emerging threats.

DISRUPT FUTURE ATTACKS

Corelight network sensors used by CrowdStrike analysts are available to you for ongoing use, allowing you to maintain your security posture after an engagement to prevent future breaches and support HIPAA and HITRUST compliance.

Real-world examples of Corelight’s impact

CHILDREN’S HOSPITAL

A large children's hospital used Corelight to confirm a backdoor on an exploited Exchange email server. Corelight's proprietary detections provided the hospital with the necessary insight to identify and respond to the attacker’s encrypted command and control (C2) traffic, ultimately securing their sensitive patient information and maintaining the integrity of their systems.

UNIVERSITY MEDICAL CENTER

A non-profit hospital center experienced a breach and used Corelight to trace its origin. By providing complete network visibility, Corelight enabled the medical center to identify the source of the breach, allowing them to take swift action to remediate the issue and strengthen their security posture.

PRACTICE MANAGEMENT COMPANY
A publicly traded practice management and electronic health record company's incident response team leveraged Corelight's internal network visibility to detect the lateral movement of an attacker who escalated privileges after gaining remote access. With Corelight's detection capabilities, the company was able to quickly identify and contain the threat, minimizing potential damage and disruption to its services.

Why Corelight?

- The only network detection and 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

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

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