corelight

NETWORK DETECTION & RESPONSE

NDR FOR HEALTHCARE

HOSPITALS | CLINICS | PHARMACEUTICALS | BIOTECHNOLOGY | DEVICE MANUFACTURING | MEDICAL RESEARCH

Speed is becoming the defining factor in healthcare cybersecurity. AI-powered attack reconnaissance, fast-moving APT groups, and expanding attack surfaces across cloud, third-party supply chains, medical IoT (MIoT) devices, and telehealth systems escalate the risks of care disruption, system lockouts, and PHI leaks. In response, the industry is rapidly deploying Network Detection and Response (NDR). Healthcare organizations use NDR to gain comprehensive visibility, using its detections to intercept threats before they advance, and AI to fight algorithms with algorithms.

For healthcare SOCs operating in clinics, hospitals, pharmaceuticals, and medical device manufacturing, NDR accelerates defense and threat-hunting operations. Expanding surveillance into hybrid cloud, ICS/OT systems, and MIoT devices allows security teams to intercept cybercriminals entering the network through these pathways. This broad visibility improves the SOC's chances of detecting unauthorized data retrieval attempts prior to breaches, helping them reduce the risk of regulatory violations.

By enabling fast, precise decisions, NDR systems change an organization's defensive trajectory. Advanced systems offer multi-layered detections. These combine signature- and static file-based detection, behavioral analysis, and other AI/ML capabilities to identify both known and unknown threats, such as APTs leveraging living-off-the-land techniques to blend in with normal network traffic. Integrated AI further speeds up IR teams by automating workflows, prioritizing threats, and streamlining response, in some cases cutting triage time by up to 50%. And if malware, phishing, or ransomware strikes, contextual logs deliver clarity, empowering teams to rapidly contain damage and even **avoid paying costly ransoms.** With reaction time increasingly determining outcomes, NDR gives healthcare organizations a strong defense against cyberthreats.

BENEFITS OF **CORELIGHT NDR**

VISIBILITY

- Support operational continuity and data security with continuous monitoring of your network ecosystem
- Reduce escalation risk by identifying threats early with a real-time, multi-layered network detection suite
- Comprehensively **inventory** devices, services, credentials, and certificates on the network

DETECTIONS

- Spot AI-driven reconnaissance with detections for scanning, enumeration, and sweeping behaviors
- Detect exfiltration with features like AWS S3 exfiltration alerts to help you intercept data hacking
- Protect manufacturing integrity by detecting anomalies in OT protocols, including BACnet, Modbus, DNP3, and more

RESPONSE

- Improve MTTR with AI-assisted summaries, workflows, and easy access to raw data, including PCAP
- Disrupt APT behavior by pinpointing lateral movement techniques in SMB and DCE-RPC activity
- Rapidly contain cybersecurity incidents, including phishing by identifying attack origin, scope, and spread
- Transform team performance with integrated visuals and context that provide clear response guidance to any tier

FORENSICS + OPERATIONS

- Support organizational alignment with HITRUST and NIST CSFs, the HIPAA Security Rule, and other guidelines
- Improve future defensive strategies: reconstruct events, trace attack timelines, and determine root causes
- Simplify operations with 4:1 platform consolidation and analytics-ready standardized data

FIGHT BACK AGAINST HEALTHCARE'S **BIGGEST CYBERSECURITY THREATS**

Detect ransomware reconnaissance

Threat actors increasingly leverage AI for automated reconnaissance, using it to rapidly scan healthcare infrastructure to identify vulnerabilities such as unpatched software. This activity is frequently a ransomware precursor. NDR with AI and machine learning, can help you identify and interrupt these early kill chain signs. It detects scanning patterns, enumeration attempts, brute-force attacks, and other indicators. Even in worst-case scenarios, NDR aids in mitigation of exploits, malware, and phishing (a common ransomware delivery vector). It reveals attack origins, precise details about compromised data, and aids in file recovery.

Defend against data theft

Securing sensitive proprietary, research, and patient data is a top concern of the healthcare industry. However, defending against advanced threat actors — such as **state-sponsored APT groups** like APT29 who target such data — requires behavioral detections. While APTs are adept at evading EDR systems and signature- or rule-based defenses, even their most subtle techniques can be uncovered by a SOC equipped with NDR and an accurately-baselined network. By understanding normal network behavior, deviations and threats become visible, enabling the detection of even the stealthiest adversaries. Continuous network monitoring can bring attention to hidden exfiltration by identifying subtle changes in communication patterns indicating lateral movement, gradual increases in outbound traffic to suspicious destinations, or unusual data flows during off-hours. By detecting these behaviors in real-time, organizations thwart adversaries and protect data from compromise.

Mitigate supply-chain risks

Observability is the front line defense against supply-chain attacks that target VPNs and remote management tools. These connections between trusted vendors and healthcare networks have become preferred intruder entryways. NDR alerts SOCs to unauthorized access attempts or unusual commands initiating from a VPN , which may signal an attack or malware delivery. Beyond this, the increasing proliferation of vulnerable devices, such as smart medical equipment underscores the need for **network asset discovery** to comprehensively see, map, and defend other entry points.

STRENGTHENING CYBERSECURITY FOR THE HEALTHCARE INDUSTRY

SAFEGUARDING SYSTEMS THAT SUPPORT
16+M
ANNUAL PATIENT VISITS

PROTECTING THE INTEGRITY OF
150 years
OF R&D

TRUSTED BY OVER
20
HEALTHCARE INDUSTRY CLIENTS

HELPING SECURE MFGS OPERATING IN
30
COUNTRIES

HOSPITALS, PHARMACEUTICAL AND DEVICE MANUFACTURERS, MEDICAL SOFTWARE, RESEARCH LABS AND CLINICS

> "The visibility in the logs that Corelight gives is **unmatched** in my opinion."
>
> — Corelight customer, Net Promoter Survey, Winter 2024

CORELIGHT'S **OPEN NDR PLATFORM**

Close cases faster, with more accuracy and greater efficiency

Strengthen infrastructure security with a system designed to help you detect and quickly neutralize adversaries. Our 4:1 Open NDR Platform combines a full detection suite with IDS, PCAP, NetFlow and NSM and creates a standardized dataset across alerts, logs, files, and packets. Powered by open-source technologies including Zeek®, Suricata®, and YARA, it seamlessly connects alerts to evidence for rapid response, forensics, and reporting. The platform streams logs in real time to your SIEM, offering native integration with existing tools across your security stack. Deployable in a range of environments and scalable from 1 Mbps to 1 Tbps per sensor, it offers central control and management of hundreds of sensors from one dashboard. Streamline operations with this fully integrated solution. **Learn more.**

COMPREHENSIVE VISIBILITY

- Unify network visibility across environments
- Expand visibility to unmonitored assets like MIoT devices and third-party suppliers
- Monitor for advanced attackers moving laterally to expand their foothold
- Pinpoint unknown network vulnerabilities
- Track everything connected to your network: summarize ICS/OT protocols with **Corelight's Entity Collection** to identify devices in use.
- Establish baseline network activity to understand what's normal

EXPANDED DETECTION COVERAGE

- Strengthen ePHI security with real-time monitoring to detect unauthorized access
- Automatically detect anomalous activity in support of NIST and other framework guidance
- Improve malware detection rates by up to 35% with YARA file analysis
- Extract insights from encrypted traffic analysis
- Create custom detections using multiple techniques
- Monitor BACnet, DNP3, Ethercat, Ethernet/IP, Modbus, PROFINET, S7Comm, TDS, and other protocols for threats to industrial equipment with **Corelight's ICS/OT Collection**

FASTER INCIDENT RESPONSE

- Lower MTTR with AI-assisted workflows, automation, and guided triage
- Access unified log data from your network ecosystem, plus raw data including PCAPs with a 10x lookback window for forensics
- Discover the entire kill chain with fast, chainable searches
- Increase close rates and validate containment

STREAMLINED OPERATIONS

- Quickly and precisely generate detailed audit reports for security incidents
- Ensure reliability with continuously monitored and updated software
- Access technical support provided by industry-leading Corelight experts
- Benefit from an open platform that accelerates innovation and avoids vendor lock-in

INCLUDES:

Detections

- SIgnature-based
- Behavioral
- Anomaly
- AI/ML

Static file analysis • Threat intelligence

Integrated visuals and context

Deep integrations with cloud control plane data

Coverage for 80+ MITRE ATT&CK® network TTPs

TRACK EVERYTHING CONNECTED TO YOUR NETWORK

Corelight's turnkey **Entity Collection** enhances the Open NDR Platform, empowering security teams to build a foundation for asset discovery, profiling, and inventory.

- Identify known apps and new local subnets
- Discover activity related to hosts, devices, services, names, certs, domains, and users

WORLD-CLASS SUPPORT

Our support team continually delights customers with their unparalleled knowledge and fast response times.

A Leader in 2025 Gartner® Magic Quadrant™ for Network Detection and Response

Gartner, Magic Quadrant for Network Detection and Response, 29 May 2025, Thomas Lintemuth, et. al

DEFENDING THE WORLD'S **MOST SENSITIVE NETWORKS**

Learn more about Corelight
Speak to an expert: 1-888-547-9497
info@corelight.com

Corelight does not provide legal or compliance advice. You are responsible for making your own assessment of whether your use of the Corelight offerings meets applicable legal and regulatory requirements.

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. The information provided is intended for general informational purposes only. While we strive to ensure the accuracy and reliability of the content presented, we make no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability, or availability with respect to the information, products, services, or related graphics contained herein. All rights reserved.

GARTNER is a registered trademark and service mark, and MAGIC QUADRANT is a registered trademark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved. Gartner does not endorse any vendor, product, or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.