

# NDR FOR THE ENERGY SECTOR

UTILITIES | RENEWABLES | OIL & GAS | REFINERIES | PIPELINES & STORAGE | TRANSMISSION & DISTRIBUTION

Relentless cyberattacks and advanced persistent threats (APTs) are driving the energy sector to deploy Network Detection and Response (NDR). Why? NDR excels at real-time monitoring of traffic between IT and OT networks, detecting attempts by adversaries to pivot from corporate networks into operational infrastructure. It acts as another defensive layer, identifying threats that bypass traditional endpoint security and actively compromise critical infrastructure.

For utilities, producers, refiners, distributors, and other sector organizations the stakes include downtime and the safety of infrastructure. NDR's comprehensive visibility and detection empowers SOC's to find both known threats and hunt for the unknown — like the subtle signs of adversaries operating below the radar. Security teams find that detecting adversaries who use living-off-the-land (LOTL) techniques becomes easier thanks to NDR's rich network data, which also enhances forensic investigations by providing detailed insights into past behavior. With the ability to detect anomalous network activity, they can spot early signs of breaches and data exfiltration, enabling faster intervention. Additionally, contextual logs allow for efficient malware, phishing, and ransomware mitigation, in some cases saving companies **from paying ransoms at all**.

## BENEFITS OF CORELIGHT NDR



### VISIBILITY

- Uncover threats before impact with real-time traffic monitoring of IT and OT networks, including control centers, substations, and supply chains
- Strengthen ransomware defense to see early signs of reconnaissance and scanning, and capture evidence of data access / movement
- Comprehensively **inventory** devices, services, credentials, and certificates on the network
- Safeguard operations by spotting lateral movement to stop threats before critical systems are affected



### DETECTIONS

- Protect command integrity by detecting anomalies in OT protocols including Bacnet, Modbus, DNP3, and more
- Lower operational disruption risks: see irregularities in vulnerable systems using behavioral analytics
- Automate broad file-based malware detection and identify payloads like BlackEnergy using YARA rules



### RESPONSE

- Triage up to 50% faster and accelerate IR to help ensure uptime and continuous operations
- Interrupt exfiltration and unauthorized transfer attempts to safeguard sensitive data
- Identify attack origin, scope, and spread to rapidly contain incidents, including phishing



### FORENSICS + OPERATIONS

- Support NERC CIP standards efforts and maintain detailed logs for investigations and root cause analysis
- Improve future defensive strategies by retrospectively identifying APT behaviors on the network
- Enhance system insight by optimizing logs for high-priority traffic flows to reduce SOC noise and enhance focus on key activities

# FIGHT BACK AGAINST ENERGY'S BIGGEST CYBERSECURITY THREATS



## Identify ransomware reconnaissance + more

Advanced threat actors typically conduct extensive reconnaissance before launching attacks. NDR identifies early-stage activities that are often ransomware precursors, detecting scanning patterns, enumeration attempts, brute force, and other key warning signs. Even in worst-case scenarios, NDR aids in mitigation of exploits, malware, and phishing — which is a common ransomware delivery vector. It reveals attack origins, the precise data stolen (if any), and helps with file recovery. NDR empowers your team with full visibility and actionable evidence to respond swiftly and decisively, ensuring resilience when seconds count.



## Protect infrastructure against state-sponsored threat groups (e.g., APT31, APT33)

**State-sponsored adversaries** attacking sector infrastructure bypass EDR systems or infiltrate unmanaged devices to gain footholds for persistence. And while it's difficult to see initial access, once an adversary makes their next move — like a port scan or C2 beacon — NDR can see it. Energy companies also leverage NDR's protocol analysis to identify anomalies in industrial control system communications that might indicate tampering or unauthorized commands. Monitoring Modbus logs, NDR can detect commands attempting to modify a system's operational behavior, such as exceeding permissible control thresholds or activating or deactivating devices. It can also spot unauthorized IP addresses, flagging deviations before equipment damage or safety incidents occur.



## Defend against sensitive data theft

Protect proprietary and business data essential to maintaining your competitive advantage and operational continuity. NDR's continuous network monitoring can identify anomalies such as subtle changes in communication patterns indicating lateral movement, gradual increases in outbound traffic to suspicious destinations, or unusual data flows during off-hours, bringing attention to hidden exfiltration. Detailed connection records that track sources, destinations, and data volume provide key insights for investigations.

## STRENGTHENING CYBERSECURITY FOR THE ENERGY SECTOR

SAFEGUARDING SYSTEMS  
RELIED ON BY

**32+M**

U.S. CUSTOMERS

ENHANCING  
CYBER RESILIENCE IN

**GULF**

ENERGY HUBS

TRUSTED  
BY OVER

**20**

ENERGY SECTOR CLIENTS

OPERATING  
ACROSS

**6**

CONTINENTS

POWER GENERATION,  
DISTRIBUTION, RENEWABLE  
ENERGY, OIL REFINING,  
LOGISTICS, WATER AND WASTE  
MANAGEMENT

"It provides great visibility into our network and details and  
**classifies traffic other devices fail to see."**

— Corelight customer, Net Promoter Survey, Fall 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 visibility and aggregate industrial telemetry across hybrid environments
- Monitor OT/IT convergence points for APTs and lateral movement
- Expand visibility to unmonitored assets and third party data
- Inventory assets in use with Corelight's [Entity Collection](#)
- Establish baseline network activity to detect security events

### EXPANDED DETECTION COVERAGE

<b>Lateral Movement</b>	PLC-to-PLC scanning, abnormal function calls
<b>Command Injection</b>	Unauthorized Modbus writes, unexpected register changes
<b>Replay Attacks</b>	Timed ICS command sequences replays Reconnaissance
<b>Reconnaissance</b>	Port sweeps, unauthorized device enumeration
<b>Protocol Anomalies</b>	Invalid function codes, malformed packets
<b>IT/OT Bridge Detection</b>	Traffic from IT-originating hosts in ICS VLANs

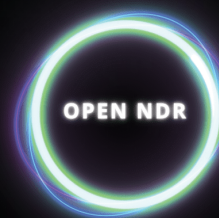
- Parses 10+ industrial protocols including BACnet, DNP3, EtherCAT, CIP/ENIP, Modbus/TCP, PROFINET, and S7Comm. Corelight's [ICS/OT Collection](#)
- Enhance NERC CIP programs with perimeter monitoring and real-time detection and response
- Improve malware detection rates by up to 35% with YARA file analysis
- Uncover unauthorized access points and expired certificates
- Extract insights from encrypted traffic analysis
- Create custom detections to identify unauthorized access to sensitive data

### FASTER INCIDENT RESPONSE

- Lower MTTR with AI-assisted workflows, automation, and guided triage
- Automatically capture evidence from suspicious flows and extend forensic windows with Smart PCAP
- Discover the entire kill chain with fast, chainable searches
- Increase close rates and validate containment

### STREAMLINED OPERATIONS

- Enhance resilience and improve reporting for NIS2, CEER, etc.
- Quickly and precisely generate detailed audit reports
- Ensure reliability with continuously monitored and updated software
- Access technical support provided by industry-leading Corelight experts
- Benefit from an open platform to accelerate innovation and avoid vendor lock-in
- Available ruggedized hardware for on-site ICS environments



#### 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

Deploy as physical or virtual appliances, cloud sensors, or with air-gapped support

Integration-ready with SIEMs, SOAR, and XDR tools



## ENHANCE VISIBILITY AND SECURITY FOR ICS/OT DEVICES AND PROTOCOLS

Corelight's turnkey **ICS/OT Collection** enhances the Open NDR Platform by monitoring the most common ICS and OT protocols, empowering security teams to defend against threats across diverse environments.

- Log protocols like BACnet, DNP3, EtherCAT, and Modbus
- Identify new services in the connection log in real-time
- Based on contributions from DHS CISA

## 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](mailto: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. © Copyright 2025 Corelight, Inc.

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.