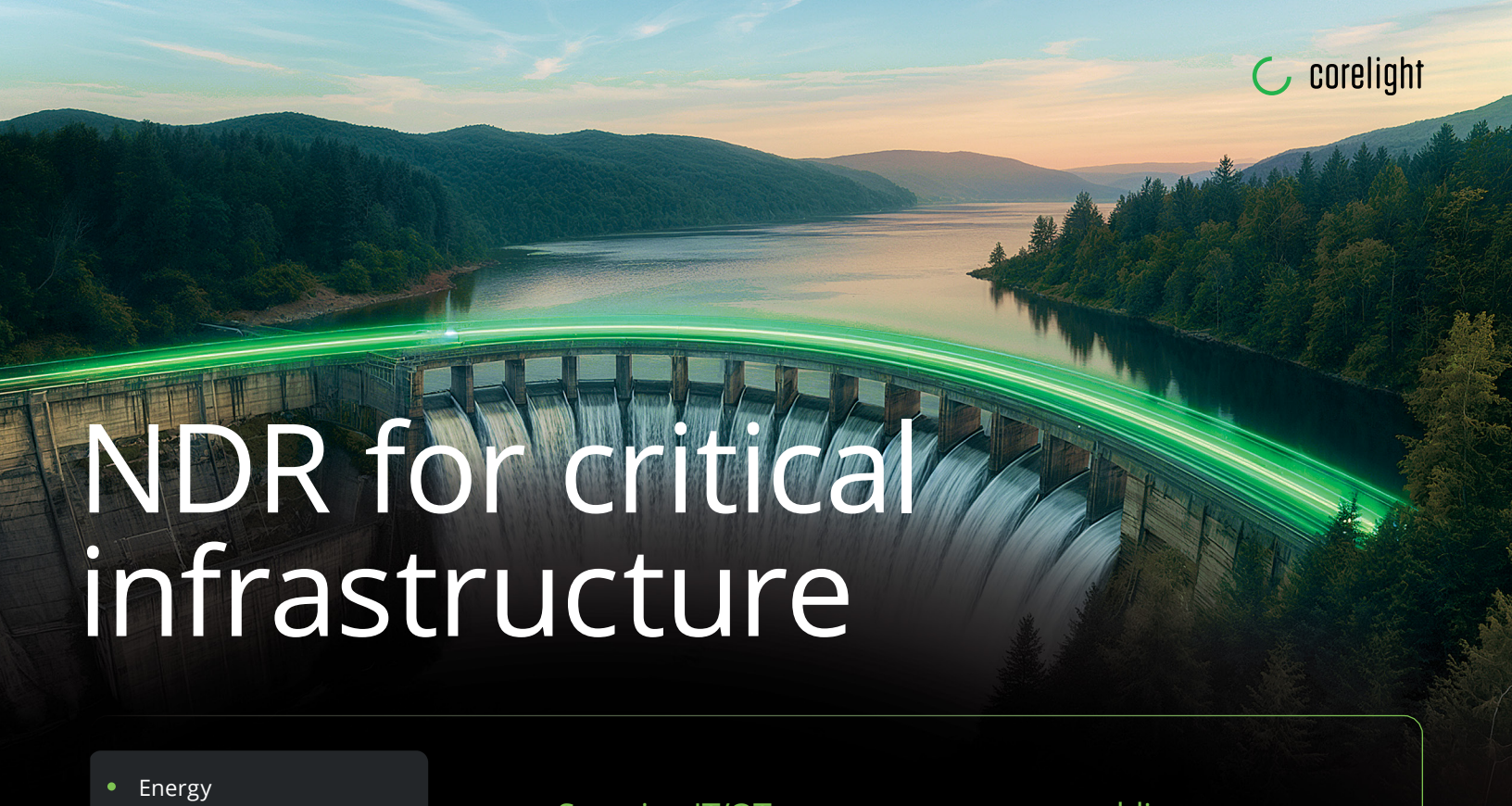

NDR for critical infrastructure

- Energy
- Transportation
- Communications & IT
- Water
- Healthcare
- Financial Services
- Food & Agriculture

Securing IT/OT convergence across public sector & commercial networks

Energy, water, communications, and a variety of other sectors have become prime targets for nation state threat actors that want to take down critical infrastructure. With complex, converging networks and sophisticated threat actors targeting operational infrastructure, modern security teams need absolute network ground truth.

Corelight transforms raw IT and OT network traffic into high-fidelity, actionable evidence that empowers security teams to uncover hidden threats that other tools miss, accelerate incident response, and provide the concrete proof of compliance required by auditors and regulators.

The Corelight difference

Passive-by-design monitoring

Corelight operates purely out-of-band to ensure zero operational risk. By tapping network mirrors (SPAN ports or network TAPs), it acts as a 100% passive monitoring solution. It silently ingests copies of network traffic without injecting a single packet into the operational data stream, eliminating any risk of disrupting sensitive industrial equipment.

The ICS / OT collection

Corelight's ICS/OT Collection uses native Zeek protocol analyzers to passively decode industrial traffic—including Modbus, DNP3, BACnet, EtherCAT, and PROFINET—converting raw industrial packets into clean, structured logs. Security teams gain real-time visibility into unauthorized function calls, PLC-to-PLC scanning, and abnormal register changes.

Detection-ready telemetry for threat hunting & compliance

Corelight generates highly structured, high-fidelity telemetry including connection metadata, DNS, SMB, RDP, file activity, certificates, and behavioral indicators that integrate directly into your existing security stack.

Open NDR platform

corelight

Data aggregation: maximizing visibility & minimizing cost

Corelight transforms network monitoring by moving beyond traditional, high-volume logging to a data summarization model. By intelligently aggregating network traffic metadata directly at the sensor level, Corelight allows security teams to reduce log volume sent to your SIEM by 60–80% without sacrificing critical forensic evidence.

Logical data reduction: Using advanced logic, Corelight condenses repetitive events into singular, high-fidelity records.

Strategic operational efficiency: This approach eliminates "log bloat," resulting in significantly lower SIEM ingestion costs and faster query performance for threat hunters. By streaming summarized logs to the SIEM for real-time alerting while offloading high-fidelity raw data to affordable long-term storage, organizations achieve a balance between immediate visibility and comprehensive, cost-effective forensic readiness.

Unprecedented OT / ICS / IoT protocol visibility: Comprehensively inventory unmanaged devices, services, credentials, and active industrial protocols across hybrid environments.

Expanded threat & anomaly coverage: Detect Living-off-the-Land (LOTL) techniques, state-sponsored APT behaviors, and lateral movement between corporate IT networks and operational ICS segments.

Ground truth for incident response: Lower MTTR by triaging alerts up to 50% faster. Automatically capture evidence from suspicious flows using Smart PCAP to provide investigators with irrefutable historical evidence.

Streamlined compliance: Effortlessly support reporting, audit trail generation, and perimeter monitoring for stringent cybersecurity frameworks including NERC CIP, IEC 62443, NIS2, and CEER.

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

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

Detection

- 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

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

Built to integrate & scale

Flexible deployment Deploy as physical ruggedized hardware for harsh on-site ICS environments, virtual appliances, cloud sensors, or in air-gapped networks.

Open ecosystem Powered by open-source industry standards (Zeek, Suricata®, and YARA) to eliminate vendor lock-in and accelerate threat hunting innovation.

SIEM & SOAR ready Native, real-time log streaming into Splunk, Elastic, Microsoft Sentinel, and other major security platforms.

Massive scalability Seamless performance that easily scales from 1 Mbps to 1 Tbps per sensor, managed via a single central dashboard.

Open NDR platform

corelight

Expanded detection coverage

- Detections
- Signature-based
- Behavioral
- Anomaly
- AI / ML

Lateral movement	PLC-to-PLC scanning, abnormal function calls
Command injection	Unauthorized Modbus writes, unexpected register changes
Replay attacks	Timed ICS command sequences replays Reconnaissance
Reconnaissance	Port sweeps, unauthorized device enumeration
Protocol anomalies	Invalid function codes, malformed packets
IT/OT bridge setection	Traffic from IT-originating hosts in ICS VLANs

- 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

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

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

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

Defending the world's most sensitive networks

corelight

Trusted globally to protect critical infrastructure, transit networks, massive utility providers, and government agencies across 6 continents.

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

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

Defending the world's most sensitive networks in the Public Sector

32M+
SAFEGUARDING SYSTEMS RELIED ON U.S. CUSTOMERS

Gulf
ENHANCING CYBER RESILENCE ENERGY HUBS

20
TRUSTED BY ENERGY SECTOR CLIENTS

6
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

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

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