corelight
NETWORK DETECTION & RESPONSE

NDR FOR MANUFACTURING

INTELLIGENT & SMART MANUFACTURING | CONSUMER GOODS | ELECTRONICS | INDUSTRIAL & CHEMICAL | MEDICAL & PHARMACEUTICAL | TRANSPORTATION + MORE

AI-powered attacks are accelerating threats against manufacturing, and adversaries have many reasons to target the industry. Intellectual property and trade secrets command high value among financially-motivated attackers and nation-state actors. Low tolerance for downtime and supply chain disruptions gives ransomware operators extra leverage.

Countering these threats demands defenses that operate at machine speed and offer visibility that spans IT and OT—environments with complex, multi-dimensional technologies and facilities running on different protocols, priorities, and constraints. These gaps are where traditional security tools lose visibility and where adversaries can move undetected.

Corelight NDR provides an answer: unified visibility across IT and OT, passive, real-time, and built to help you detect indicators of ransomware, reconnaissance, lateral movement, and exfiltration—to support response before production may be impacted. And with agentic AI, lean teams get leverage. Corelight's agentic triage helps reduce the noise and surfaces activity that may need attention, keeping analysts focused on true threats.

BENEFITS OF CORELIGHT NDR

VISIBILITY

- **Unified visibility** of IT, OT, and cloud traffic
- **Close visibility gaps** across operations, remote sites, and corporate environments
- **Automatically inventory** network-connected assets

DETECTIONS

- **Help identify ransomware** in the recon phase
- **Quickly detect activity associated with known CVEs** and common tools like Cobalt Strike in hybrid IT/OT environments
- **Surface lateral movement from IT into OT** that may indicate attempts to reach PLCs or HMIs
- **Detect anomalies** in OT protocols to protect production continuity and support safety programs
- **Identify suspicious activity** from vendor and contractor sessions
- **Help expose data theft** and exfiltration

RESPONSE

- **Automate and accelerate IR workflows** with agentic AI
- **Reduce triage time** by up to 50%
- **Pivot from alerts** to packets in seconds
- **Rapidly contain threats** with integrated response actions
- **Reduce SOC noise** with AI-driven prioritization

FORENSICS + OPERATIONS

- **Full attack histories** and network logs behind each alert
- **Smart PCAP retention** for audits and compliance
- **Root-cause analysis** and network troubleshooting
- **Fuel AI SOC initiatives** with provably better open network data

FIGHT BACK AGAINST MANUFACTURING'S BIGGEST CYBERSECURITY THREATS

Identify ransomware staging

Threat actors know downtime is manufacturing's pressure point and aggressively target plant environments with ransomware. Identifying these attempts in early stages—before data is encrypted or stolen—is critical. Corelight helps surface the subtle precursors, including scanning patterns, enumeration attempts, and credential brute-forcing, while also identifying tools and known threats associated with ransomware and other debilitating attacks. Corelight helps surface actionable alerts during reconnaissance, giving teams time to investigate and intervene to help reduce the risk of production disruptions.

Protect operations from lateral movement

The connected systems in modern manufacturing drive efficiencies but also create risks. Attackers gain footholds in IT and pivot toward OT assets, exploiting blind spots with techniques using RPC/SMB exploits, port scanning, ARP spoofing, man-in-the-middle (MitM), and protocol tunneling (DNS/ICMP). Corelight baselines normal network activity and passively monitors convergence points, alerting you to deviations. This unified visibility helps spot lateral movement and techniques like living-off-the-land (LoTL), including activity that may be missed by tools without comparable network visibility, helping you intervene before attackers reach critical systems.

Defend against supply chain risk, data and intellectual property (IP) theft

Adversaries exploit the vast ecosystem of vendor, contractor, and remote maintenance channels to open new attack vectors. Corelight alerts your SOC to unauthorized access, unusual commands, and malware delivery while monitoring for hidden exfiltration, beaconing, and command and control (C2) activity, helping detect potential attempts to compromise intellectual property before or as data leaves your network.

DEFENDING OPERATIONS AT
30+
LEADING INDUSTRIAL ORGANIZATIONS

PROTECTING
50M+ TONS
OF CRITICAL MATERIALS PRODUCTION

SAFEGUARDING
$140B+
ACROSS INDUSTRIAL ORGANIZATIONS

PROTECTING NETWORKS FOR
360K+
INDUSTRIAL & SUPPLY CHAIN WORKERS

ACTIVE IN AEROSPACE, AUTOMOTIVE, CONSTRUCTION AND RAW MATERIALS, DEFENSE, ELECTRONICS, MEDICAL, AND CPG MANUFACTURING

"I like that there was minimal management of the policies that was needed to get **great coverage**."

— Information Technology Specialist, Major manufacturer

CORELIGHT'S OPEN NDR PLATFORM

Close cases faster, with greater efficiency

Strengthen infrastructure security with a system designed to help you detect and quickly respond to adversary activity. 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 connects alerts to evidence for rapid response, forensics, and reporting. The platform streams logs in real time to your SIEM, with integrations designed to work with existing tools across your security stack. Deployable in a range of environments and scalable up to 100 Gbps per sensor, it offers central control and management of hundreds of sensors from one dashboard. Corelight provides actionable intelligence to help defend your manufacturing enterprise. **Learn more.**

COMPREHENSIVE VISIBILITY

- Expand visibility into unmonitored assets, legacy devices, and third-party connections
- Unify network telemetry across IT, OT, and remote production sites
- Inventory active devices, certificates, and protocols without disruptive active scanning

EXPANDED DETECTION COVERAGE

- Help spot activity associated with APTs and lateral movement at IT/OT convergence points with LLM-powered behavioral detection
- Detect unauthorized commands and protocol anomalies across Modbus, PROFINET, BACnet, S7Comm and more
- Expose exfiltration attempts targeting proprietary data and IP, including evasive threats that may bypass signature-based tools

FASTER INCIDENT RESPONSE

- Lower MTTR with agentic triage that automates correlation, investigation, prioritization, and findings summaries
- Guide investigations with automated alert scoring and actionable next steps
- Uplevel analyst skills with AI-generated log summaries, response guidance, and natural language queries
- Quickly search for IOCs, entities, third-party alerts, and A2A questions
- Correlate Corelight network evidence with endpoint, vulnerability data, and threat intel
- Pivot from alert to packet-level evidence in seconds
- Trace the kill chain with fast, chainable searches to validate threat containment

STREAMLINED OPERATIONS

- Centralize management of hybrid environments across hundreds of physical, virtual, and cloud sensors
- Integrate into existing SIEMs, XDR, and AI/ML pipelines with structured, open-standard data that fuels your AI SOC
- Support IEC 62443, NIST, and CISA-aligned security programs
- Avoid vendor lock-in with an open platform and open data architecture

INCLUDES:

- Signature-based
- Behavioral
- Anomaly
- AI/ML detections
- Static file analysis
- Threat intelligence
- Integrated visuals and context
- Deep integrations with cloud control plane data
- Coverage for 80+ MITRE ATT&CK® network TTPs

ENHANCE VISIBILITY AND SECURITY FOR ICS/OT DEVICES AND PROTOCOLS

The ICS/OT Collection extends Corelight's Open NDR Platform with monitoring of BACnet, DNP3, EtherCAT, Modbus, PROFINET, S7Comm protocols and more. It helps identify new devices and services in real time, giving your team investigative evidence without active scanning and helping reduce operational disruption risk.

- Detect anomalies and unauthorized comms
- Log protocol-level activity in industrial, HVAC, access control and other systems
- Generate dashboards and queries based on organization-specific details
- Included as part of your Corelight subscription

AGENTIC AI FOR MANUFACTURING SOCs

Lean security teams can't manually triage every alert across sprawling IT/OT environments. Corelight's agentic AI automates correlation, investigation, and verdict generation, turning hours of analyst work into minutes while keeping humans in control of final decisions.

A leader in The Forrester Wave: Network Analysis and Visibility Solutions, Q4, 2025

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

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