

NDR FOR THE FINANCIAL SECTOR

ASSET MANAGEMENT | BANKING | BROKERAGES | HIGH FREQUENCY TRADING | INSURANCE | WEALTH MANAGEMENT

As AI-equipped cybercriminals intensify attacks on financial services firms by leveraging sophisticated techniques like living-off-the-land alongside credential theft and ransomware, organizations are rapidly adopting Network Detection and Response (NDR). With client and proprietary data—as well as business operations—increasingly targeted, real-time detection capabilities and comprehensive network visibility are now non-negotiable for preventing potentially catastrophic breaches.

By closing visibility gaps and turning every packet into actionable intelligence, Corelight helps financial institutions protect data, support compliance requirements, and maintain market trust.

Corelight Open NDR extends visibility across the network. From hybrid cloud and legacy systems to third-party connections and other environments endpoints can't see, NDR defends what others miss. It detects and identifies advanced persistent threats, emerging attacks that evade traditional security, and more than 80 network-based TTPs.

Fueled by forensic-grade network telemetry, Corelight's multi-layered detection stack, combining signatures, behavioral analytics, file and encrypted traffic analysis, and AI/ML, empowers SOCs to uncover lateral movement, command-and-control activity, and data exfiltration attempts before they escalate.

BENEFITS OF CORELIGHT NDR

VISIBILITY

- Visualize your expanded attack surfaces
- Monitor all network connections with out-of-band optical taps
- Expedite data collection in financial services protocols, e.g., MPLS, Multicast, FIX

DETECTIONS

- Precisely detect network-based threats in real time
- Identify sophisticated attacks that evade EDR
- Disrupt kill chain activity, including C2 and exfiltration

RESPONSE

- Interrupt data exfiltration and unauthorized data transfers
- Mitigate phishing and ransomware incidents
- Reduce triage time by 50%

FORENSICS + OPERATIONS

- Extend data retention periods in support of regulatory compliance
- Streamline forensic analysis
- Supports DORA and NIS2 monitoring needs

FIGHT BACK AGAINST FINANCE'S BIGGEST CYBERSECURITY THREATS



Minimize data breaches

Real-time monitoring continuously analyzes network traffic and identifies suspicious data movement patterns and connections. This enables your SOC to swiftly identify, contain, and stop unauthorized data access or data exfiltration, without impacting network performance.



Detect intrusions missed by other defenses

Novel, AI-driven attacks and groups like FIN7 and D0nut use EDR bypass tools and living off the land techniques to avoid detection. Corelight's AI-powered anomaly, behavioral, and signature-based detections uncover threats that evade endpoint tools.



Combat ransomware threats

Anomaly analysis detects deviations from normal baselines, signaling potential ransomware attacks before they escalate. Corelight Open NDR gives security teams the visibility to see exactly what data was accessed or taken in a ransomware attack. This empowers them to make a rapid assessment of its value and sensitivity, helping teams decide whether paying the ransom is warranted.



Contain and remediate with precision

Corelight network evidence identifies suspicious attachments that may indicate spear phishing. Built-in YARA integration detects malware through static file analysis, allowing teams to mitigate malicious emails and contain threats early, preventing further spread and reducing potential damage to systems and data.

STRENGTHENING CYBERSECURITY FOR THE FINANCIAL SECTOR

WE HELP PROTECT

\$1B+

IN DAILY TRADES

WE DEFEND

\$10T+

IN COMBINED
MANAGED ASSETS

TRUSTED BY

50+

FINANCIAL SERVICE
ENTERPRISES

OPERATING ACROSS

150+

COUNTRIES
AND SIX CONTINENTS

ACTIVE IN ASSET MANAGEMENT,
BANKING, EXCHANGES, HEDGE
FUNDS, AND MORE

“So **THIS** is actually what is happening on our network.”

— Lead security engineer at a major mortgage lender

CORELIGHT'S OPEN NDR PLATFORM

High-performance, low-latency, built to thrive in demanding environments

Our Platform combines comprehensive network detections, AI, intrusion detection (IDS), network security monitoring (NSM), static file analysis, and packet capture (PCAP) in a single security tool powered by proprietary and open-source technologies, including Zeek®, Suricata®, and YARA. Seamlessly connecting alerts to investigative evidence, Open NDR is enhanced by guided triage, threat intelligence, community detections, and AI-powered analyst tools for fast threat identification and mitigation that will transform your SOC's ability to defend against rising attacks. [Learn more.](#)

ENHANCE VISIBILITY AND MONITORING

- Low-latency performance complements high-frequency trading environments
- Monitor north-south and east-west network traffic using out-of-band optical taps
- Detect unauthorized data retrieval
- Baseline and compare data flows to identify deviations
- Transform traffic into correlated security evidence; Corelight data includes full content, transactional, alert data, and extracted content
- Utilize unified telemetry across on-premises and cloud for consistent management in AWS, Azure, and GCP environments

ACCELERATE DETECTION AND IR

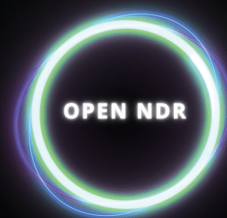
- Supervised ML, unsupervised anomaly, behavioral, and signature detections provide extensive network threat coverage
- Uncover unauthorized access points, expired certificates, and unauthorized protocol activity
- Identify malware at scale in hybrid and encrypted traffic environments using integrated static file analysis
- Accelerate incident response through native integration with existing tools across security stacks, including EDRs, firewalls, and IT ticketing
- Create custom detections to identify unauthorized access to sensitive data and other security threats
- Support for industry-specific protocols such as Multicast, MPLS, and encrypted protocols, including SSL and IPSec

IMPROVE ACCOUNTABILITY

- Strengthen control integrity, including access and network segmentation for Zero Trust compliance
- Automate alerts and reports for supervisory tasks and compliance requests
- Maintain detailed, easily searchable Zeek logs to simplify audit trails
- Rapidly estimate and verify incident scope
- Improve governance via cost-effective data storage and retrieval
- Extend lookback windows for deep forensics
- Support compliance initiatives, including addressing FINRA rules and financial regulations (DORA and NYDFS cybersecurity requirements, and NIS2 and NIST)

STREAMLINE 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

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

Integration-ready with SIEMs, SOAR, and XDR tools



SUPPORT AUDIT READINESS AND FORENSICS WITH UP TO 10X LONGER LOOKBACK WINDOWS

Expand **historical data storage** from days to weeks or months at low cost. Corelight's logs deliver rich metadata for rapid investigations, enabling faster searches and supporting audits, incident reporting, resilience testing, and deep forensic analysis.

- Storage-efficient Zeek® logs for quick retrieval of months of records
- Indexed data is 1-2% the size of a full packet capture for 50× faster searches
- Supports audits, reporting, risk assessments, and resilience testing

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. © 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.