Detect. Decrypt. Deter.

JOINT SOLUTION BRIEF

Empowering Comprehensive Security and Visibility with Mira Security's ETO and Corelight's Open NDR Platform

Business Problem

The pervasive adoption of encrypted SSL traffic has been an ongoing trend, establishing itself as the expected standard for both users and applications. This user-friendly integration has enabled businesses of all sizes to embrace it. However, this widespread adoption has inadvertently generated a challenge for security operations teams. While effectively shielding data from unauthorized access, it has also introduced a blind spot that conceals potential malicious files from network security tools, granting covert entry into the network. It is now evident that organizations must attain insight into encrypted SSL traffic to ensure the safeguarding of workforces, clientele, and operational integrity. Yet, the pursuit of traffic visibility must not compromise performance or security. The end-user experience must remain unaffected, underscoring the necessity for transparent, seamless, and secure visibility measures.

Joint Solution Benefits

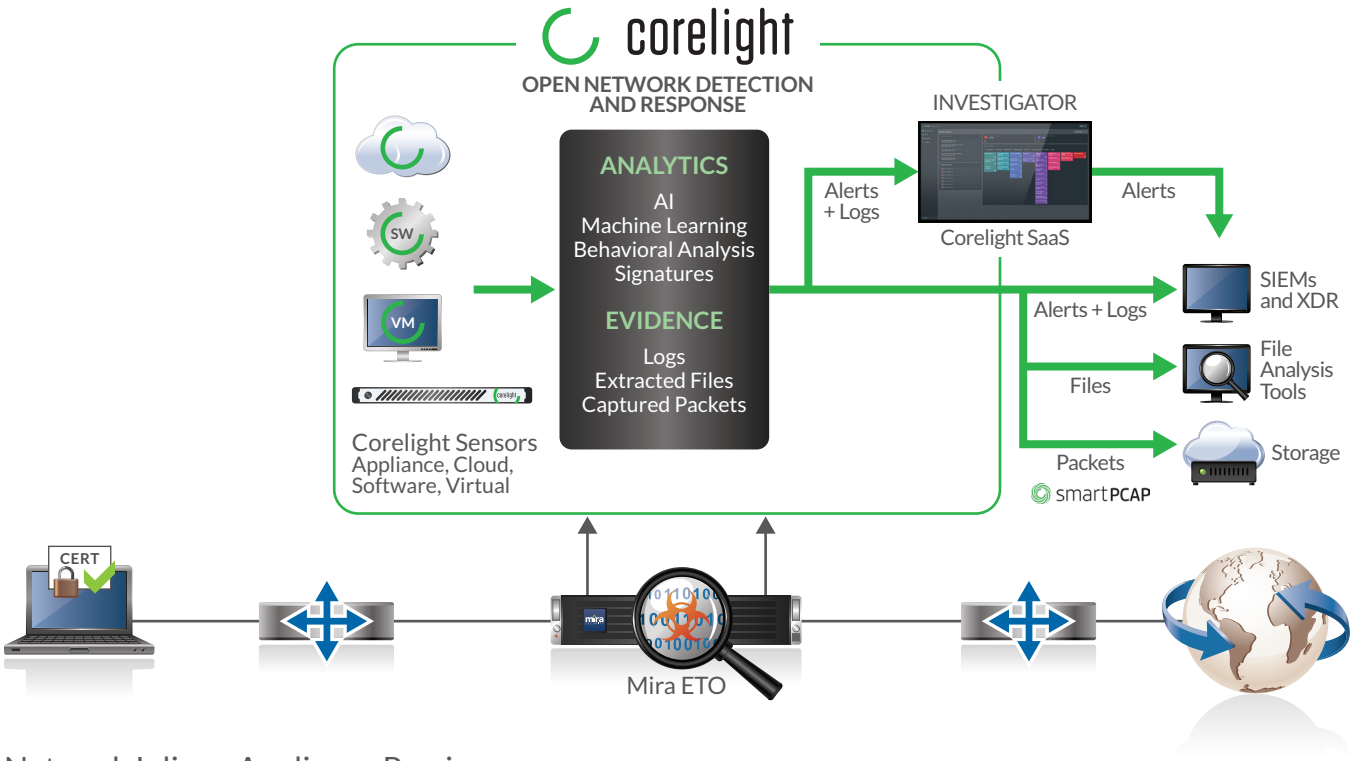
- **Visibility:** The ETO will remove the SSL/TLS blind spots, allowing the Corelight Open NDR Platform to analyze traffic and generate additional insights that might otherwise be hidden by encryption.
- **Ease of Use & Simplicity:** Both the ETO and Open NDR Platform solutions are easy to install, configure, and integrate with other elements of your security tech stack.
- **Flexible Rules & Policies:** Use the ETO's Category Database to selectively bypass decryption of certain categories of traffic and safeguard sensitive user data. In the Open NDR Platform, Corelight's detections reveal known and unknown threats via hundreds of unique insights and alerts across machine learning, behavioral analysis, and rule-based approaches.
- **Scalability & Speed:** The ETO supports decrypting from 0.5 to 100 Gbps of traffic and allows for high throughput by supporting 1, 10, 25, and 40 Gbps interface speeds. A single Corelight Sensor appliance can handle up to 100 Gbps of traffic.
- **Platform Versatility:** Tailoring themselves to diverse network requirements, both the ETO and Open NDR Platform are available in physical hardware or virtual appliance forms, compatible with both private and public cloud settings.
- **Efficiency Amplified:** ETO can decrypt traffic once and distribute it to attached Open NDR appliances and/or other passive security tools through app ports and mirror ports. Corelight's Open NDR Platform consolidates NSM, IDS, and PCAP functionality while seamlessly integrating with your toolstack — from ticketing systems to your SIEM and XDR solutions.

Corelight and Mira Joint Solution

Corelight transforms network and cloud activity into evidence so defenders can stay ahead of ever-changing attacks. Easily deployed and available in on-prem and SaaS-based formats, Corelight combines the power of open source and proprietary technologies to deliver a complete Open Network Detection & Response (NDR) Platform, while seamlessly integrating with Mira's Encrypted Traffic Orchestrator (ETO). Mira's advanced TLS/SSL decryption technology, available as either a virtual or physical appliance, significantly enhances the capabilities of Corelight's Open NDR Platform. It empowers users to gain full insights into encrypted traffic by decrypting the flows of TLS/SSL and SSH traffic, bolstering visibility and control.

Together, Corelight's Open NDR and Mira's ETO form an exceptional solution, offering both scalability and adaptability. By residing between the client and server, Mira Security's ETO provides complete visibility into previously concealed traffic. This process involves traffic decryption, transmission of plaintext to the attached Corelight Sensor for analysis, and subsequent re-encryption before forwarding it to the intended destination. This strategic approach enables Corelight's Open NDR Platform to reveal threats by receiving a complete copy of decrypted network traffic from the inline Mira ETO to the out-of-band Corelight Sensor. Corelight's Open NDR Platform takes the decrypted traffic and transforms it into comprehensive, correlated evidence that provides unparalleled visibility into the network. This evidence allows security teams to unlock new analytics, investigative faster, hunt like an expert, and even disrupt future attacks.

The convenience of managing both solutions through user-friendly web interfaces further enhances the overall experience. This integration reliably removes blind spots in the network and reduces the risk of malicious data on the wire.



Network Inline - Appliance Passive

The ETO sits in the middle of the traffic flow. When the SSL/TLS handshake occurs, the ETO actively decrypts the traffic and passes the plaintext data over to the Corelight Sensor to analyze it and detect security threats. The ETO then re-encrypts the data and sends it on to the destination, maintaining the end-to-end connection in an encrypted form. The Corelight Sensor will generate comprehensive alerts and protocol logs via the power of Suricata Intrusion Detection System (IDS), the Zeek Network Security Monitor, and proprietary enhancements including Smart PCAP.

About Corelight

Corelight provides security teams with network evidence so they can protect the world's most critical organizations and companies. On-prem and in the cloud, our Open Network Detection & Response Platform enhances visibility and analytics, leading to faster investigations and expanded threat hunting. Corelight's global customers include Fortune 500 companies, major government agencies, and large research universities. Based in San Francisco, Corelight is an open-core security company founded by the creators of Zeek®, the widely-used network security technology. For more information, please visit corelight.com.

MiraSecurity.com

mira SECURITY

info@mirasecurity.com

Mira Security
330 Perry Highway, Suite A
Harmony, PA 16037
Phone: +1 (412) 533-7830

Email: info@mirasecurity.com
mirasecurity.com

MIRA-CORELIGHT-4/24