Microsoft | corelight

Joint solution brief

Corelight for Microsoft Defender

Accelerate investigations and prioritize alerts based on risk with integrated network, endpoint, and vulnerability data directly within the network sensor.

Security teams face challenges in maintaining a strong security posture because legacy tools often fall short in supporting today's modern infrastructures and countering increasingly sophisticated threats. This is further compounded by the limited visibility into unsecured and unknown endpoints, as well as the torrent of alerts generated from an increasingly complex security stack.

SOLUTION HIGHLIGHTS

- Extensive visibility into network traffic across all devices
- Faster investigations with risk-based alert prioritization
- Higher analyst productivity with real-time contextualized alerts
- Improved mean time to detection and remediation

Integrated Corelight and Microsoft Defender data in a single view.

Accelerate investigations and prioritize alerts based on risk by enriching Corelight logs in real-time with Microsoft Defender endpoint and vulnerability data.

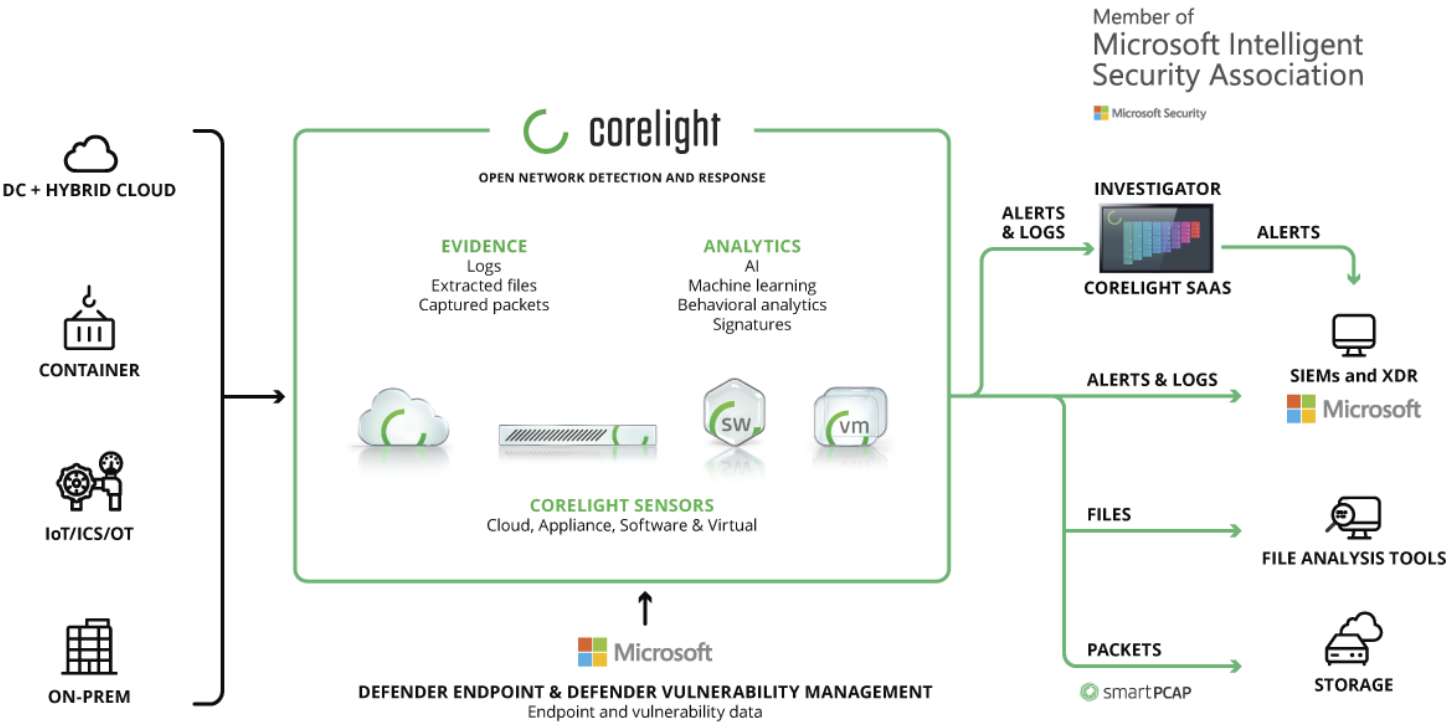
STREAMLINE INCIDENT RESPONSE WITH ENRICHED NETWORK EVIDENCE

Native Corelight integration with Microsoft Defender for Endpoint and Microsoft Defender Vulnerability Management can address these common problems. Based on the design pattern of elite defenders, Corelight's Open NDR Platform provides network evidence, detections, and insights that amplify the speed and efficiency of threat investigations. By enriching Corelight logs with Microsoft Defender endpoint and vulnerability data, security teams have the integrated data and context they need to defend against the most sophisticated adversaries.

This unique endpoint data enrichment in Corelight sensors at the point of observation helps analysts accelerate investigations, streamline incident response, and prioritize the most critical vulnerabilities and risks to the enterprise. In addition to providing insight into an organization's most vulnerable endpoints, prioritizing alerts with integrated network and endpoint telemetry can also greatly reduce analyst fatigue caused by the overwhelming volume of alerts streaming into the Security Operations Center (SOC). What's more, Corelight's advanced network telemetry can easily identify unknown systems across the environment that can then be inventoried and managed by Microsoft Defender.

Easily deployed and available in on-premise, cloud, and SaaS-based formats, Corelight combines the power of open source and proprietary technologies to deliver a complete Open NDR Platform that includes modern intrusion detection (IDS), network security monitoring, and Smart PCAP solutions for complete visibility and protection.

Native integration streamlines and accelerates investigations



Simplify investigations and prioritize alerts according to actual risk to the enterprise with integrated network, endpoint, and vulnerability data.

SOLUTION BENEFITS

With full contextual and integrated endpoint, vulnerability, and network data now available directly from Corelight network sensors, analysts can simplify and accelerate their investigations for a more secure posture across the enterprise.

GET COMPLETE VISIBILITY

Detect early, mid, and late-stage indicators of network compromise with comprehensive visibility into all network traffic across the enterprise, including support for unmanaged and unknown devices, as well as those that can't accommodate endpoint agents.

IMPROVE NETWORK DETECTION AND COVERAGE

Enhance detections with prioritized alerts based on verified environmental risks by enriching Corelight network telemetry with Microsoft Defender endpoint and vulnerability data, all at the point of observation within the network sensor.

ACCELERATE RESPONSE

By enriching Corelight logs with unique device IDs from Microsoft Defender for Endpoint, SOC teams can pivot seamlessly between NDR and EDR telemetry to accelerate investigations and streamline incident response.

INCREASE OPERATIONAL EFFICIENCY

Corelight consolidates multiple legacy tools—including network monitoring, IDS, and intelligent packet capture—into a unified NDR platform that can reduce SOC complexity across on-premise, hybrid, and multi-cloud environments, while enabling higher analyst productivity.

corelight

To learn more about Corelight for Microsoft, request a demo at

https://corelight.com/contact

info@corelight.com | 888-547-9497