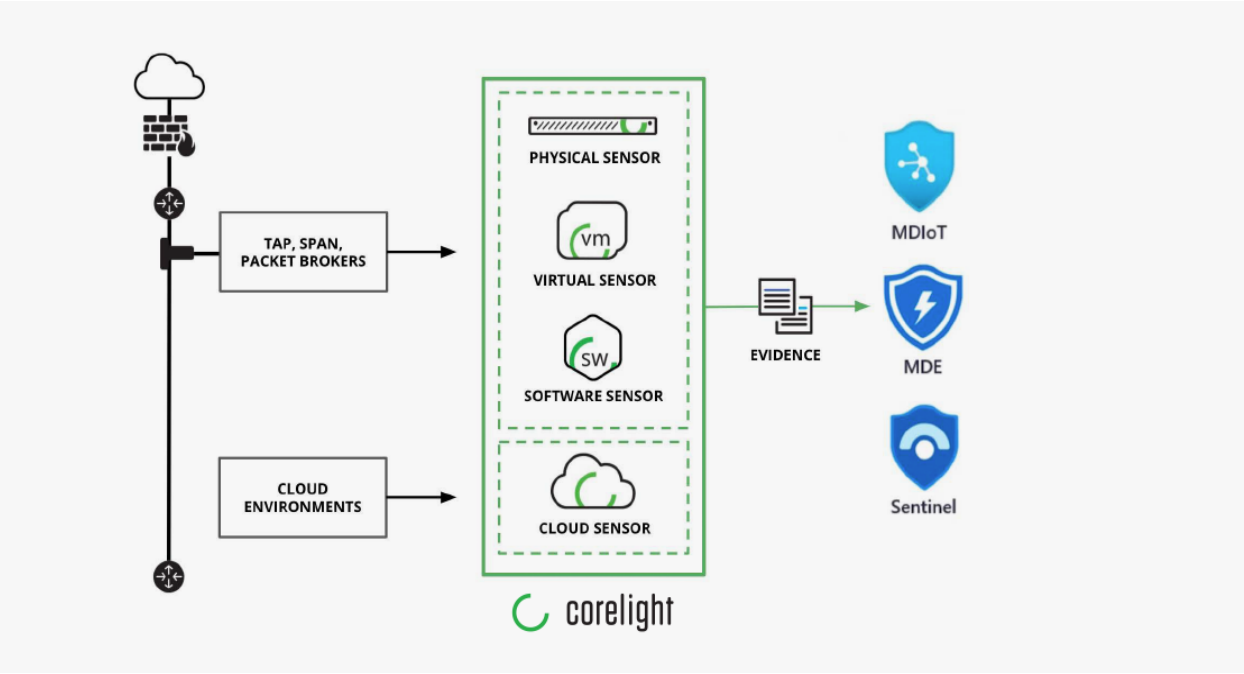
Joint Solution

Endpoint protection is not enough

As attackers become more sophisticated, protecting your devices gets harder. Endpoint protection alone is no longer the sole answer as advanced adversaries can evade agent-based solutions and leverage unmanaged devices. For companies looking for better visibility of potential threats on their network, Corelight delivers complete, correlated network evidence. Corelight's Network Detection and Response (NDR) platform uses open, universal standards as the foundation of seamless integrations across Microsoft Defender for IoT, Microsoft Sentinel, and Defender for Endpoint

The Corelight / Microsoft Security solution:



Defend with the insights you need with Corelight evidence and Microsoft Security products

Expand visibility

Gain insight into network traffic to and from any device on your network — even when that traffic is encrypted.

Enhance analytics

Correlate rich network evidence from Corelight with a multitude of analytics tools, including Microsoft Defender and Microsoft Sentinel. Gain more value from a joint solution with Corelight and Microsoft.

Accelerate investigations

Reduce your incident response time by providing essential evidence that speeds up analyst workflows.

Hunt and disrupt

Capture rich, structured network data from 50+ protocols to provide additional context for threat hunting in Microsoft Sentinel.[1]

A global firm with 40,000 employees was able to resolve incidents up to 20x faster with Corelight Open NDR.[2]

Access the evidence you need to disrupt future attacks

- Gain comprehensive network visibility with insights across 50+ network protocols.[1]
- Easily investigate security alerts to identify true and false positives.
- Replace legacy log sources with a standardized source of network truth for Microsoft Sentinel.
- Augment device inventory in Microsoft 365 Defender to improve situational awareness.
- Set up the Corelight NDR platform with Microsoft technologies quickly using jointly developed integrations.
- Significantly reduce incident response time.

[1] Corelight Internal Source
[2] Corelight Education First Case Study

Microsoft enables digital transformation for the era of an intelligent cloud and an intelligent edge. Its mission is to empower every person and every organization on the planet to achieve more.

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 and 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.

info@corelight.com | 888-547-9497