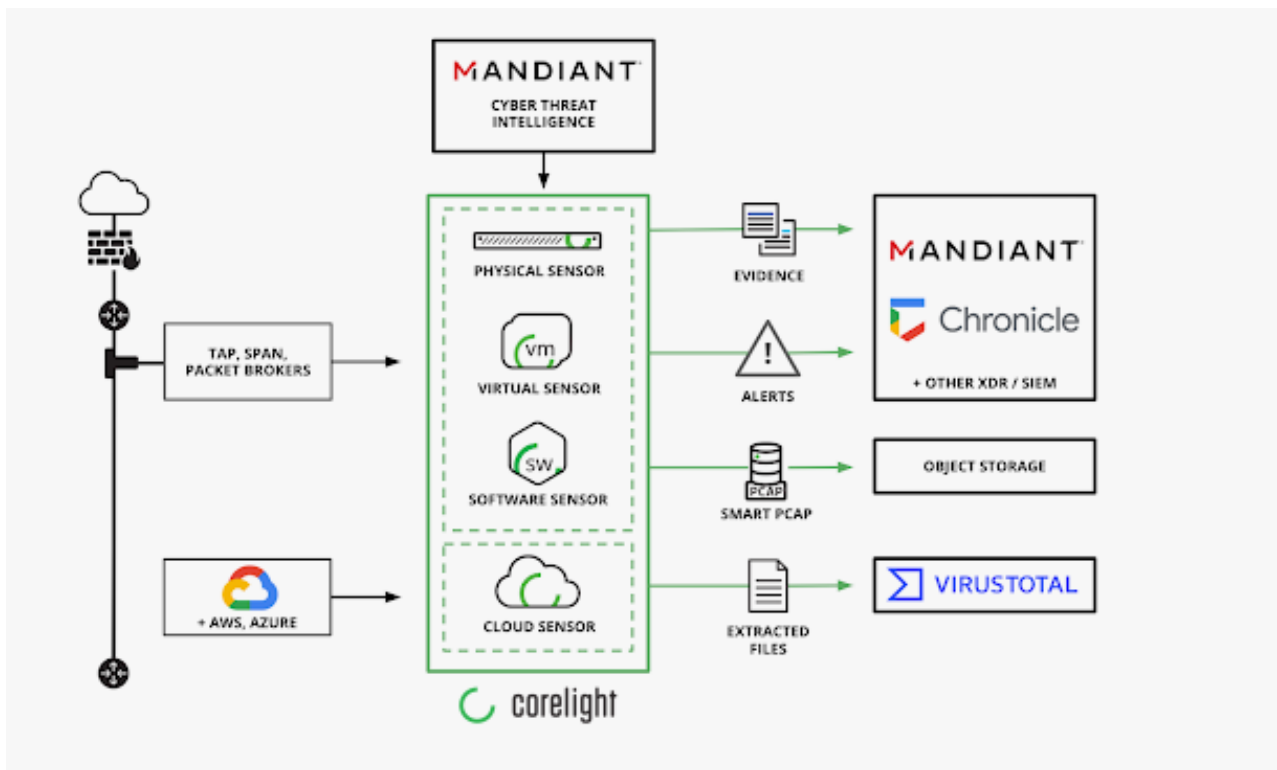**MANDIANT**® | **C corelight**

Joint Solution

Corelight + Mandiant

Mandiant is a pioneer in cyber defense with a brand respected throughout the security world, and Corelight's open network detection and response (NDR) products have been battle-tested in the world's most critical environments. Both companies share a mission-driven culture and a dedication to building a more stable and trustworthy internet. A unique partnership between both companies can help you mitigate threats faster than ever, reduce risk, and get back to business.

The Corelight / Mandiant solution:

Corelight cloud and network evidence empower Mandiant solutions to find, resolve, and disrupt attacks.

Complete visibility
Corelight gives you a commanding view of your organization and all devices that log onto your network—with access to details such as DNS responses, file hashes, SSL certificate details, and user-agent strings. These details can be correlated with Mandiant Cyber Threat Intelligence to detect threats the moment they cross your network.

Next-level analytics
Corelight's high-fidelity, correlated telemetry powers Mandiant Advantage XDR, Google Chronicle, VirusTotal, and other analytics solutions, improving their efficiency and unlocking new capabilities. Corelight Collections further amplify detections with insight into encrypted traffic, command and control, and asset inventory.

Faster investigation
Corelight correlates alerts, evidence, and packets. It allows you to establish a network baseline and store years' worth of activity so SOC analysts can trace the origins of attacks. This context integrates directly into your existing workflows to reduce false positives and your alert backlog—no redesign or retraining necessary.

Expert hunting
Corelight's structured evidence makes hunters more effective because it's clear and complete. Elite defenders worldwide use the same telemetry to find everything from intruder artifacts to critical misconfigurations. With Corelight evidence, anyone on your team can help disrupt attacks.

Since 2004, Mandiant has been a trusted partner to security-conscious organizations. Effective security is based on the right combination of expertise, intelligence, and adaptive technology, and the Mandiant Advantage SaaS platform scales decades of frontline experience and industry-leading threat intelligence to deliver a range of dynamic cyber defense solutions. Mandiant is now part of Google Cloud.

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