

Joint Solution Brief

Corelight for Mandiant expert-led services

Well-financed adversaries are creating an unprecedented level of sophisticated attacks that often circumvent an organization's advanced security defenses. And with the wide adoption of cloud, the proliferation of smart devices, and the trend of microservices development architectures, visibility gaps are growing and making it more difficult for security teams to keep up.

Not surprisingly, this has led to a growing trend of security operations center (SOC) teams turning to outside specialists to augment their internal resources. Google Cloud Security is addressing this need by offering organizations Mandiant's frontline intelligence and expert-led services, including managed detection and response (MDR). These services provide real-time threat awareness, helping organizations strengthen their resilience against cyber attacks.

Google Cloud Security customers can now take advantage of a superior level of attack visibility, protection, and threat hunting capabilities across their on-premise and multicloud environments by integrating Corelight Open NDR with Mandiant Managed Defense and the Google Security Operations Platform. Corelight's unique ability to transform network data into comprehensive and correlated evidence helps SOC teams tame the exponential growth of security alerts and incidents to understand the interrelated details of even the most sophisticated attacks.

INTEGRATION HIGHLIGHTS

Superior visibility into all network traffic with rich, correlated data

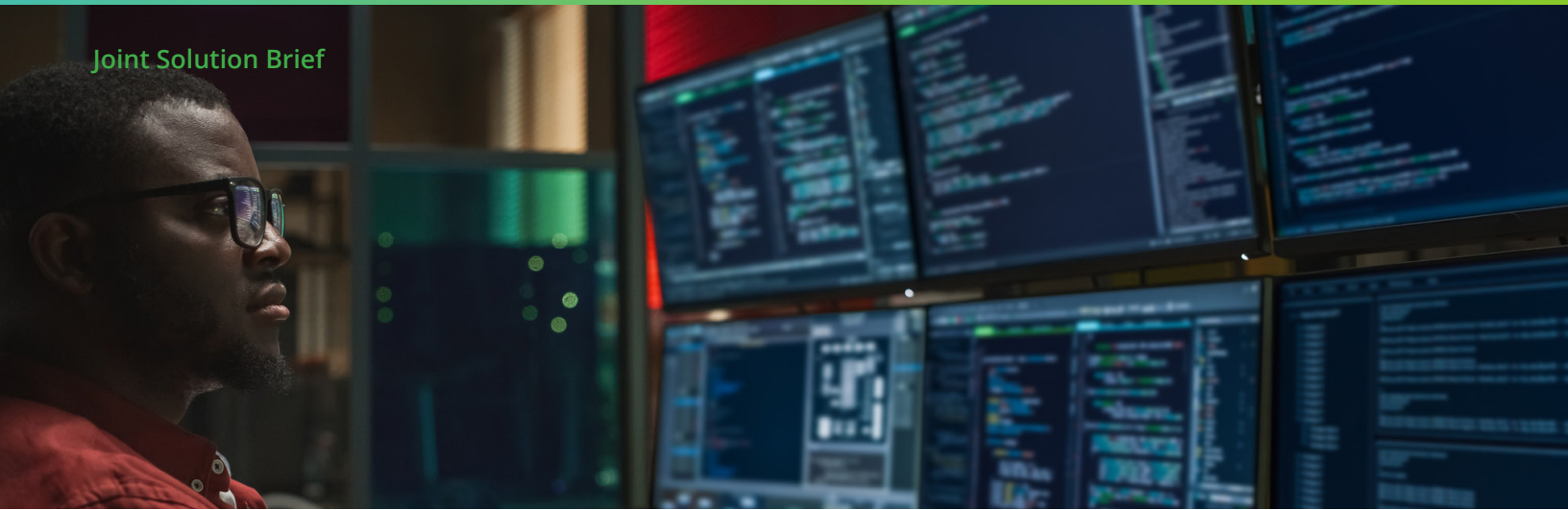
Immutable network evidence that goes back months for compliance

Advanced protection for existing Mandiant Managed Defense customers

Massive scalability and lightning-fast search with Google Security Operations

WHY MANDIANT CHOSE CORELIGHT

Mandiant Managed Defense can deliver peace of mind to customers with 24x7 seamless monitoring for Corelight Open NDR Platform through the Google Security Operations Platform to detect and respond to threats before they impact the business. By incorporating Managed Defense in the cyber defense strategy, organizations gain access to advanced security capabilities, such as attacker behavior investigation and analysis, proactive threat hunting, and incident response. Managed Defense uses the Google Security Operations sub-second querying capabilities, world-class threat intelligence enrichment, and Corelight's high-fidelity logs and alerts to uncover hidden threats, accelerate investigations, and outpace sophisticated adversaries.



KEY SOLUTION BENEFITS

Corelight enables organizations to increase detection coverage, accelerate response times and improve visibility of threats by transforming all network data into comprehensive, correlated evidence, alerts, and detections.



COMPLETE VISIBILITY

Spot early-, mid-, and late-stage signs of network compromise with superior visibility into all network traffic, including across hybrid, multi-cloud, and distributed environments, as well as for devices that can't support endpoint agents. Rich, correlated, security-specific evidence goes back months, not days.



IMPROVE NETWORK DETECTION AND COVERAGE

Identify known attacks and expose novel techniques with advanced threat detections and Corelight's extended coverage of 80 MITRE ATT&CK TTPs. The Managed Defense team can also prioritize alerts for faster response with the enrichment of Corelight logs with Mandiant Threat Intelligence.



ACCELERATE RESPONSE

Accelerate investigations with correlated alerts, logs, and data packets that help analysts respond quickly and accurately with the scope and severity of adversary activity. Corelight can power Google Security Operations SOAR playbooks and existing workflows to slash false positives and alert backlogs that enable analysts to focus on higher-value activities.



INCREASE OPERATIONAL EFFICIENCY

Boost analyst efficiency and reduce data costs in downstream analytics with 4:1 tool consolidation that provides uniform network telemetry. Simplify compliance requirements across on-prem and cloud environments.



To learn more about Corelight for Google Cloud Security, request a demo at

<https://corelight.com/contact>

info@corelight.com | 888-547-9497