JOINT SOLUTION BRIEF

Respond to threats faster with Gigamon + Corelight

Accelerate security incident response and expand threat detection capabilities

Technologies like firewalls and IDS/IPS excel at generating alerts, but can't help security analysts make fast and comprehensive sense of traffic to separate fact from fiction and quickly triage and resolve alerts. For investigative answers, security teams usually turn to network flow data or packets, but both are problematic sources of truth.

In theory packets offer complete visibility, but lossless packet capture is a rare feat and packets are ultimately slow to search and cost-prohibitive to store at scale. Security analysts can spend hours manually analyzing packets just to get a single insight and they can't interrogate more than a few days or weeks of traffic due to storage costs. When initial breaches take just minutes to execute and the average attacker dwell time is more than 7.5 months, slow search and traffic memory blackouts can be devastating.

On the other hand, flow data like Netflow can be quick to search and affordable to store at scale, but these network data types have serious traffic blind spots and often lack critical detail needed by security teams. Netflow, for example, offers scant data on encrypted connections and DNS server logs lack the query responses. Why? Because these network "side-effect" logs were never designed for security teams: they were created for ops teams to troubleshoot and tune their networks.

The Corelight and Gigamon Solution

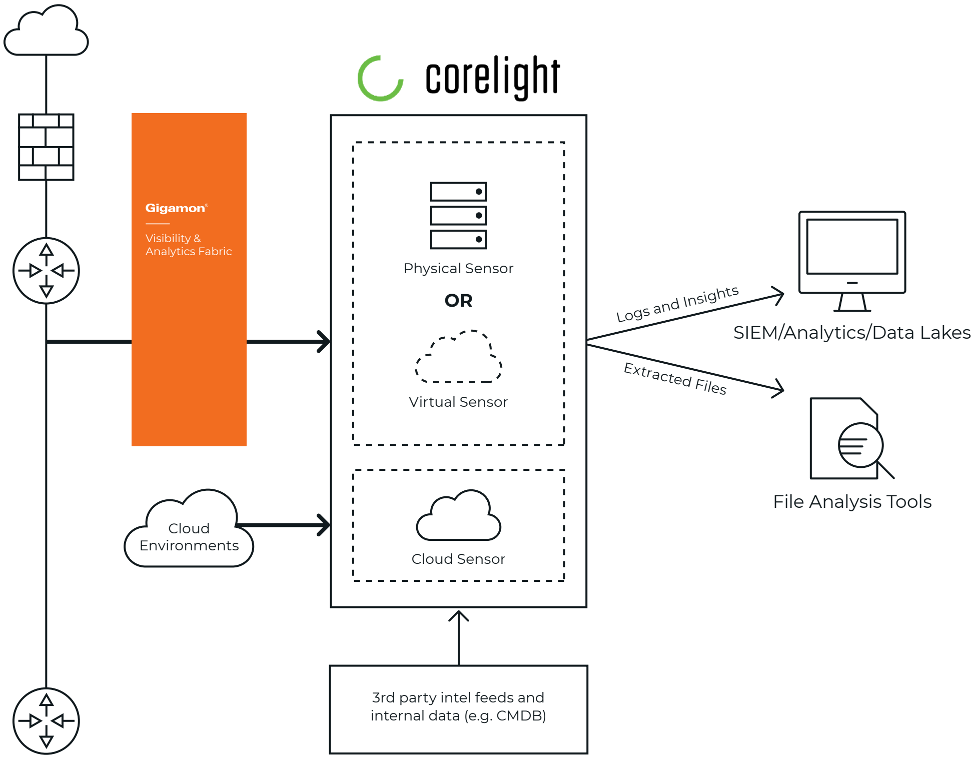

Figure 1: A joint packet capture and network security monitoring solution from Gigamon and Corelight can overcome these limitations and provide scalable, complete network visibility that accelerates incident response and unlocks powerful new threat hunting and detection capabilities.

With Gigamon's next generation network packet brokers feeding packets to Corelight's network security monitoring sensors, you can convert all of your traffic into actionable security visibility in the form of traffic logs, extracted files, and scripted insights. This reliable, comprehensive, and fast visibility can expand security team capabilities, illuminating traffic blind spots where attackers hide, such as exfiltrating data via DNS traffic or moving laterally in east-west traffic. Together, Gigamon and Corelight empower security teams to see and make sense of their network traffic at the speed of attack, leaving no stone or packet unturned.

Zeek: The gold standard for network security.

Corelight runs on Zeek, the powerful, open-source network analysis tool that has become a global standard. Thousands of the world's most critical organizations use Zeek to generate actionable, real-time data to help defend their networks.

Zeek extracts over 400 fields of data in real-time, directly from network traffic. It covers dozens of data types and protocols from Layer 3 to 7, including TCP connections, SSL certificates, HTTP traffic, emails, DHCP, and more. Zeek logs are structured and interconnected to support threat hunters and incident responders.

Corelight Sensors—available in physical, cloud and virtual formats—vastly simplify the challenges deploying open-source Zeek. They offer excellent performance, combine the capabilities large organizations need with high-end, out-of-band hardware and a specialized version of the open-source Zeek network security monitor.

Corelight Sensor capabilities include:

- Up to 25 Gbps+ of monitored traffic per sensor
- Hardware, cloud, or virtual appliance models
- A web-based sensor management GUI
- Fleet Manager to manage up to 250 Corelight Sensors
- Pre-installed collections of Zeek packages
- A comprehensive API
- On-box performance and health monitoring
- Dynamic file extraction
- Flexible export options, including popular data formats, filtering, and forking
- Shunting to handle elephant flows over 25 Gbps (AP 3000 only)
- Support from the creators and builders of Zeek

About Gigamon

Gigamon provides active visibility into physical and virtual network traffic, enabling stronger security and superior performance. Gigamon's Visibility Platform™ and GigaSECURE®, the industry's first Security Delivery Platform, deliver advanced intelligence so that security, network, and application performance management solutions in enterprise, government, and service provider networks operate more efficiently. As data volumes and network speeds grow and threats become more sophisticated, tools are increasingly overburdened. One hundred percent visibility is imperative. Gigamon is installed in more than three-quarters of the Fortune 100, more than half of the Fortune 500, and seven of the 10 largest service providers. For more information visit www.gigamon.com.

About Corelight

Corelight delivers powerful network traffic analysis (NTA) solutions that help organizations defend themselves more effectively by transforming network traffic into rich logs, extracted files, and security insights. Corelight Sensors are built on Zeek (formerly called "Bro"), the open-source NTA framework that generates actionable, real-time data for thousands of security teams worldwide. Zeek has become the 'gold standard' for incident response, threat hunting, and forensics in large enterprises and government agencies worldwide. Corelight makes a family of physical, cloud and virtual network sensors that take the pain out of deploying open-source Zeek and expand its performance and capabilities. Corelight is based in San Francisco, California and its global customers include numerous Fortune 500 companies, large government agencies, and major research universities. For more information, visit www.corelight.com.

For more information on Gigamon and Corelight, visit gigamon.com and corelight.com

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com