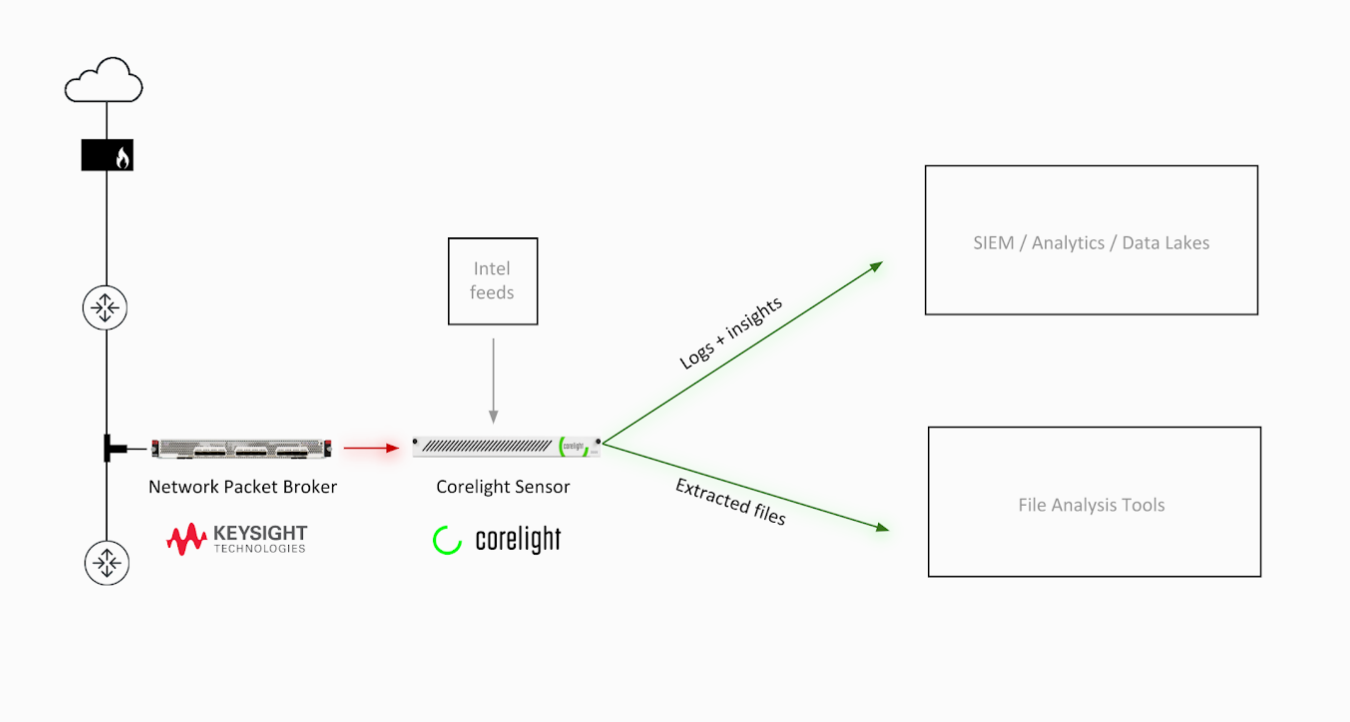
Joint Solution

Augment network visibility and defense with Keysight and Corelight

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.

The Corelight / Keysight solution:



A joint packet capture and network security monitoring solution from Keysight 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.

Joint Solution: Corelight and Keysight

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.

With Keysight's advanced 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, Keysight 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.

Use Cases & Benefits

With this joint solution security teams can substantially reduce risk by resolving incidents more efficiently and uncovering hidden adversary activity, with innumerable security use cases like:

- **Fast pivots into packets for security investigations:** when you need packet-level detail, you can use Corelight's logs to understand the context of the issue and to locate the exact Keysight-captured packets needed by correlating the super accurate timestamps between Corelight's logs and Keysight's packets, which can save analyst's hours of manual packet searching.
- **Detecting data exfiltration via DNS queries:** deploying the joint Keysight & Corelight solution at the perimeter will capture and log all DNS requests, which can reveal abnormally-long character lengths that may indicate attackers exfiltrating stolen data inside of DNS traffic.
- **Extracting files to automate malware detection:** deploying this joint solution allows you to capture and extract all files in east-west traffic, which you can then stream to a file analysis or intelligence framework to detect exploit-laden files as attackers attempt to move laterally within your environment.

Keysight Network Packet Brokers

Keysight's Vision Network Packet Brokers provide real-time, end-to-end visibility into physical, virtual, SDN and NFV based networks, and can aggregate traffic from multiple TAPs or SPAN ports, with purpose-built dedicated hardware in their physical packet brokers that ensure zero packet loss.

Key capabilities include:

- Zero-loss packet capture for 1G, 10G, 40G, 100G networks
- Deduplication, packet trimming, protocol stripping, burst protection, and time-stamping
- Centralized filter templates and custom dynamic filtering
- High availability with redundant management ports, power supplies and fan trays

Corelight Sensors

Corelight Sensor transforms raw traffic into comprehensive logs, extracted files, and security insights, via a specialized version of the open-source Zeek framework. Available in both physical (1U), cloud, and virtual form factors (VMware & Hyper-V), Corelight Sensors are sized to support 100s of Mbps of traffic to throughput speeds in excess of 25 Gbps. Key capabilities include:

- Comprehensive, security-optimized traffic logging across 35+ protocols
- Flexible data export & filtering controls to manage SIEM performance & cost
- File reassembly and extraction at wire speed
- Customizable traffic monitoring and detection via a scripting language

KEYSIGHT TECHNOLOGIES

Keysight Technologies Inc. (NYSE: KEYS) is the world's leading electronic measurement company, transforming today's measurement experience through innovations in wireless, modular, and software solutions. With its Hewlett-Packard and Agilent legacy, Keysight delivers solutions in wireless communications, aerospace and defense and semiconductor markets with world-class platforms, software and consistent measurement science. The company's nearly 12,600 employees serve customers in more than 100 countries.

corelight

Defenders have always sought the high ground in order to see farther and turn back attacks. Corelight delivers a commanding view of your network so you can outsmart and outlast adversaries. We capture, interpret, and connect the data that means everything to defenders.

info@corelight.com | 888-547-9497