KEYSIGHT | corelight

JOINT SOLUTION

Augment network visibility and accelerate incident response with Keysight and Corelight

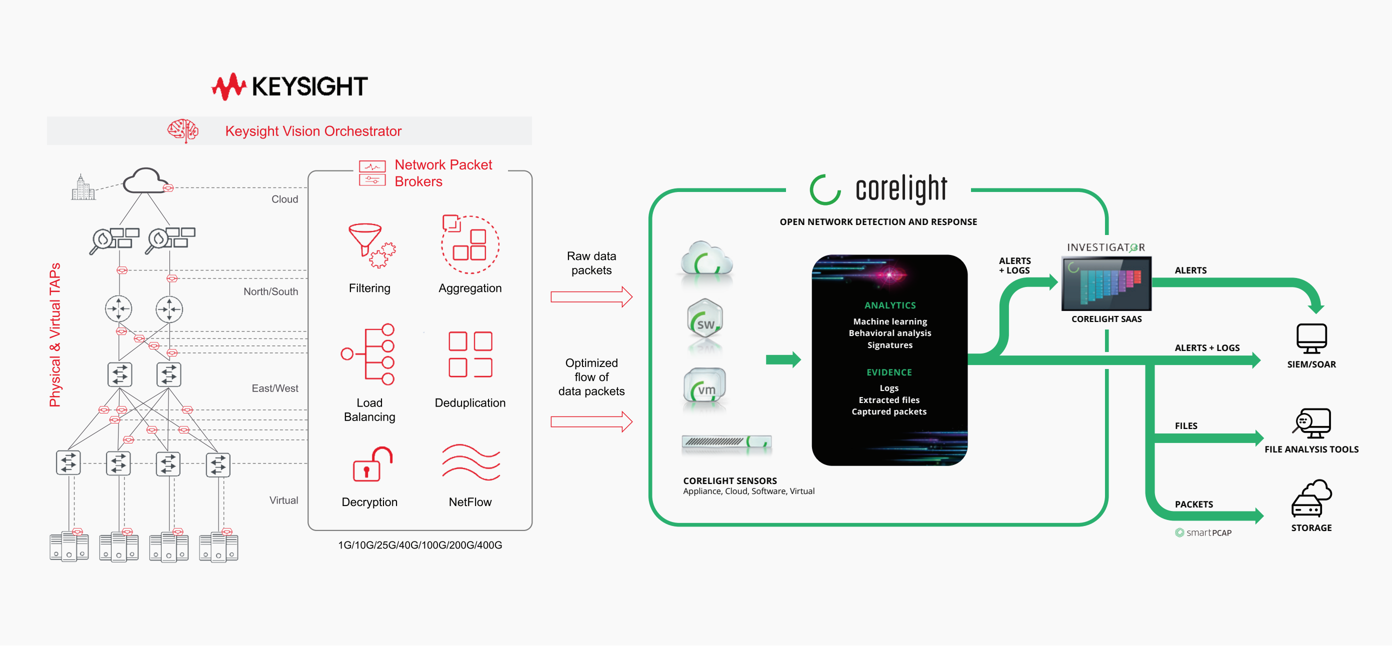
Security Operations Center (SOC) and security teams are at the forefront of ensuring an organization's safety. Here's how they can overcome key challenges:

- *Network Visibility*: By having complete access to packet data and network traffic, blind spots are eliminated.
- *Analytics*: Through correlating context and integrating information, the team gets a complete picture, streamlining their processes.
- *Investigations*: By effectively prioritizing alerts, investigation times are significantly reduced.
- *Threat Hunting*: With increased agility and context for hunting, disruptive strategies are created, adding an additional layer of security.

INTEGRATION HIGHLIGHTS

- Real-time, pervasive visibility into network activity across physical, virtual, public, and hybrid infrastructures
- Efficient, intelligent and scalable delivery of just the right data to Corelight Sensors for analysis
- Comprehensive detections with network context lower response times
- Lightweight network metadata enables threat hunting and speeds incident response

THE KEYSIGHT AND CORELIGHT END-TO-END NETWORK SECURITY SOLUTION



KEYSIGHT ENABLES SCALABLE EFFICIENT ACCESS TO ALL NETWORK TRAFFIC FOR SECURITY ANALYSIS

The Keysight intelligent network visibility platform complements and augments Corelight's Open NDR Platform by extending efficient access to all physical, virtual, and cloud traffic needed for analysis.

Keysight network TAPs (copper, fiber, industrial, virtual, or cloud) are deployed for reliable access to 100% of the traffic anywhere in the network. Purpose-built Keysight Vision network packet brokers (NPBs) are positioned out-of-band between the traffic acquisition points and Corelight Sensors, and they can perform several functions:

- Aggregate traffic from multiple network TAPs and switched port analyzer (SPAN) ports
- Optimize flow of aggregated traffic by eliminating duplicate packets and and filtering unnecessary traffic data that is not needed for security analysis
- Replicate, load balance, and forward optimized traffic to one or multiple Corelight Sensors and other tools as needed

Keysight Vision Orchestrator acts as the central point of management, automation, and orchestration of all Keysight visibility solutions. This enables organizations to scale and operate their Keysight visibility solutions across their entire environment with ease.

DISRUPT ATTACKS WITH NETWORK EVIDENCE

Corelight's Open NDR Platform takes the network and cloud traffic acquired and optimized by Keysight and transforms it into comprehensive, correlated evidence that provides unparalleled visibility into the network. This evidence allows security teams to unlock new analytics, investigate faster, hunt like an expert, and even disrupt future attacks.

SOLUTION BENEFITS

COMPLETE VISIBILITY

Keysight TAPs and intelligent NPBs deliver efficient and scalable access to all data traffic across physical, virtual, cloud and hybrid infrastructure. Corelight out-of-band sensors parse all the copied traffic turning it into rich, correlated, security-specific evidence that goes back months, not days.

NEXT-LEVEL ANALYTICS

Corelight delivers a comprehensive suite of network security analytics that help organizations identify more than 75 adversarial TTPs across the MITRE ATT&CK® spectrum. These detections reveal known and unknown threats via hundreds of unique insights and alerts across machine learning, behavioral analysis, and signature-based approaches.

FASTER INVESTIGATION

Corelight's rich, pivotable telemetry covers everything that crosses your network, so analysts can make connections and find out what really happened quickly and confidently.

EXPERT HUNTING

Corelight's rich telemetry provides the context that SOC teams need to reduce dwell time and find hidden attacks—yet it is lightweight enough to be stored for years. Improve SOC performance and accelerate threat hunting and response with next-level analytics powered by open source.

MAXIMUM EFFICIENCY

Keysight's network packet brokers remove unnecessary and duplicate packets before forwarding traffic to Corelight Sensors, reducing the processing burden and ensuring maximum efficiency.

To learn more about the Keysight integration, request a demo at **https://corelight.com/contact**

Keysight Technologies, Inc. (NYSE: KEYS) is a leading technology company that helps enterprises, service providers and governments accelerate innovation to connect and secure the world. Keysight's solutions optimize networks and bring electronic products to market faster and at a lower cost with offerings from design simulation, to prototype validation, to manufacturing test, to optimization in networks and cloud environments. Customers span the worldwide communications ecosystem, aerospace and defense, automotive, energy, semiconductor and general electronics end markets. More information is available at www.keysight.com. Contact us at 1-800-829-4444 | usa_orders@keysight.com

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

The Z and Design mark and the ZEEK mark are trademarks and/or registered trademarks of the International Computer Science Institute in the United States and certain other countries. The Licensed Marks are being used pursuant to a license agreement with the Institute.