VECTRA | KEYSIGHT

# Vectra AI and Keysight: Gain complete visibility into cyberthreats inside the network

## Key Challenges

Ever-growing hybrid environments are now the norm for many organizations in today's cybersecurity space. The rapid expansion of environments leads to the increased traffic of network data, leaving elusive blind spots for attackers to leverage. From these blind spots, attackers can enact stealthy attacks including hidden command-and-control communications, internal reconnaissance, botnet monetization, lateral movement, and data exfiltration.

## Solution Overview

The Keysight Network Visibility Architecture and Vectra AI Platform work together to eliminate network blind spots that allow attackers to hide. Utilizing Keysight's Vision series of Network Packet Brokers (NPBs) aggregates data from all network access points including SPANs, taps, and virtual taps (vTaps). When integrating Keysight with Vectra AI, SOC analysts leveraging the Vectra AI Platform can get full, comprehensive network visibility, uncovering the spots in which attackers tend to hide.

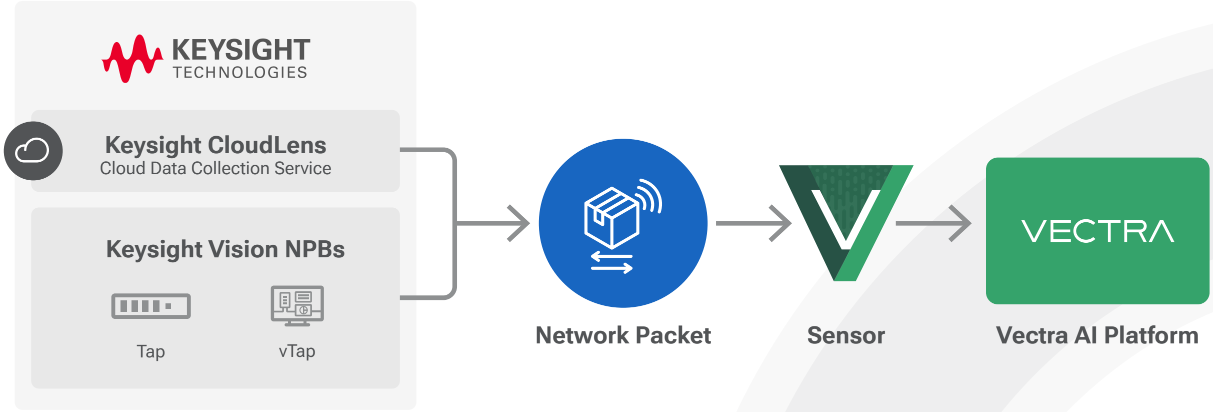
## Solution Components:

- **Keysight Vision network packet brokers (NPBs)**: direct and optimize network traffic from multiple access points like SPANs, taps and vTaps
- **Vectra AI Platform**: inspects, analyzes, and correlates network data to bring comprehensive network visibility to SOC analysts

## Key Benefits:

- **Simplified deployment** – Leverage joint solutions in any network environment with Keysight's intuitive GUI enabling drag-and-drop virtual connections between SPANs/ taps and the Vectra AI Platform
- **Rapid scale** – Add 1-, 10-, 40-, or 100-gigabit ports as needed; dynamically adjust filters to meet bandwidth requirements
- **Maximum efficiency** – Filter and remove unneeded traffic so the Vectra AI Platform always operates at full efficiency
- **Higher utilization** – Load-balance traffic across multiple ports
- **Real visibility into virtual risk** – Gain visibility into potential threats hidden in east-west traffic across your virtual environments

## How it Works



1. Set up virtual and physical connections between SPANs/taps, NPBs and Vectra AI Platform via Keysight GUI control panel.
2. Keysight CloudLens gathers traffic from public cloud, private cloud, or a hybrid setup.
3. Keysight Vision NPBs aggregate network traffic from SPANs, taps, and vTaps.
4. Keysight Vision NPBs remove duplicate packets.
5. Network data packets are sent to the Vectra AI Platform where metadata is correlated and triaged into entity-based prioritization.

## About Vectra AI

Vectra AI is the leader and pioneer in AI-driven Attack Signal Intelligence. Only Vectra AI natively delivers hybrid attack telemetry across public cloud, SaaS, identity, and networks in a single XDR platform. The Vectra AI Platform with Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks to their hybrid environment. Vectra AI has 35 patents in AI-driven threat detection and is the most referenced vendor by MITRE D3FEND. Organizations worldwide rely on the Vectra AI Platform and MXDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

## About Keysight

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. Keysight generated revenues of $4.2B in fiscal year 2020. More information is available at www.keysight.com.

**For more information please contact us:**
Email: info@vectra.ai | vectra.ai