VECTRA | KEYSIGHT

SOLUTION BRIEF

Vectra AI and Keysight Technologies Deliver Advanced Network Threat Visibility and Response

Eliminate blind spots that allow attackers to hide.

Blind spots in your network can impact security and performance. The new business environment demands IT support for a wider range of monitoring, security and compliance requirements. This creates significant burdens on network performance and network security as more appliances need access to incoming data.

3 Key Challenges Addressed

- Securing hybrid cloud attack surface
- Unknown threats
- SOC team workload and burnout

Our Approach

The Keysight Network Visibility Architecture and Vectra AI Attack Signal Intelligence™ can eliminate blind spots that allow attackers to hide.

Complete visibility into cyberthreats

- The Keysight Network Visibility Architecture delivers all required traffic from anywhere in the network or cloud to the Vectra AI Platform. 100% of traffic can be monitored, inspected and analyzed.

Simplified deployment

- The Keysight/Vectra AI solution is flexible across hybrid cloud environments and shares access with deployed monitoring and security tools.

Easily scalable

- Add additional 1-, 10-, 40- or 100-gigabit ports as needed and dynamically adjusts filters to meet any bandwidth requirements.

Maximum efficiency

- The Keysight solution filters and removes unneeded traffic, so the Vectra AI Platform always operates at full efficiency.

Our Product

The Keysight Network Visibility Architecture and the Vectra AI Platform with Attack Signal Intelligence work together to detect cyberattacks in progress amid the chatter of your network, so security teams can quickly mitigate and prevent data loss.

Keysight's Vision series of Network Packet Brokers (NPBs) passively direct out-of-band network traffic from multiple network access points — like SPANs, taps and virtual taps (vTaps) — to the Vectra AI Platform for inspection and analysis.

Traffic data is aggregated from all network access points to provide comprehensive visibility.

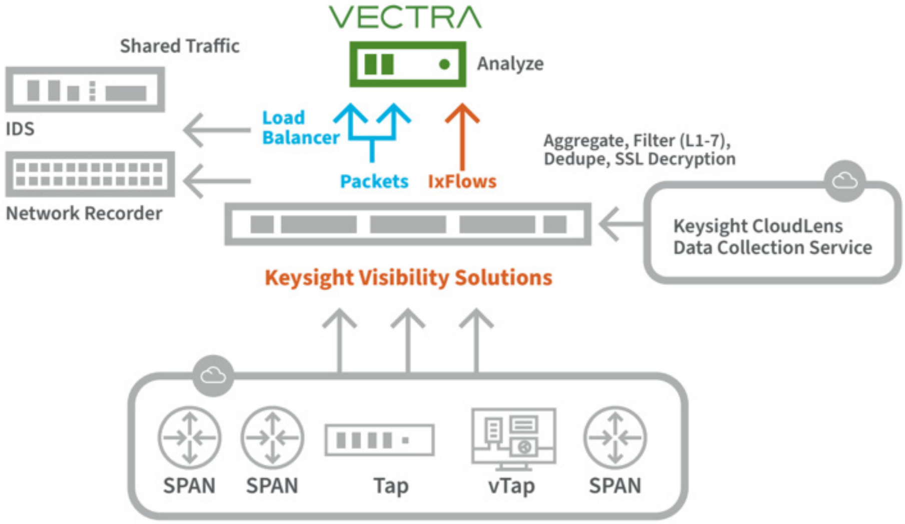
The Vectra AI Platform collects and stores the right network and cloud metadata and augments it with machine learning to detect all phases of persistent stealthy attacks, including hidden command-and-control communications, internal reconnaissance, botnet monetization, lateral movement and data exfiltration.

The automation capability in the Keysight Visibility Architecture integrates seamlessly with Vectra AI to enable a wide range of applications, including:

- Load-balancing traffic across multiple ports.
- Dynamically tightening filters to ensure that critical transactions are always analyzed when total traffic spikes over 10 Gbps.
- Redirecting traffic among multiple instances on a network to ensure high availability.
- Complete visibility into east-west traffic from virtual environments.

An intuitive GUI control panel makes Keysight NPBs easy to set up and use.

Simply drag-and-drop a virtual connection between SPANs/taps and the Vectra AI Platform to make a live connection.


VECTRA
Analyze
Shared Traffic
IDS
Network Recorder
Load Balancer
Packets
IxFlows
Aggregate, Filter (L1-7), Dedupe, SSL Decryption
Keysight CloudLens Data Collection Service
Keysight Visibility Solutions
SPAN
SPAN
Tap
vTap
SPAN

Summary

Keysight's intelligent visibility solutions complement the Vectra AI Platform with fast, easy access to all required traffic anywhere:

- Eliminate blind spots and improve attack surface coverage.
- Detect and respond rapidly to unknown threats.
- Streamline security team workloads and reduce burnout.

Learn more about the Vectra AI Platform

About Vectra AI

Vectra AI is the pioneer of AI-driven threat detection and response for hybrid and multi-cloud enterprises. The Vectra AI Platform delivers integrated signal across public cloud, SaaS, identity, and data center networks in a single Open XDR platform. The Vectra AI Platform with patented Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks in 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 MDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

About Keysight

Sponsored by Keysight, Get Network Visibility (GNV) helps large enterprises and government entities eliminate network blind spots that are among the top 5 leading reasons for network security and performance issues. GNV is built upon the visionary work from companies such as: Ixia, NetOptics, and Anue. GNV provides insights, consulting and demoes of packet-based solutions working alongside popular tool vendors such as: Vectra, Nozomi, Trellix, including for cloud deployments with Azure, Nutanix and Kubernetes, and many others to keep your networks safe and performing. For more information or to contact us, please visit: www.getnetworkvisibility.com

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