VECTRA®

ixia
A Keysight Business

Gain complete visibility into cyberthreats inside the network with Vectra and Ixia

CHALLENGE

Blindspots in your network can impact security and performance

SOLUTION

The Ixia Network Visibility Architecture and the Cognito network detection and response platform can eliminate blindspots that allow attackers to hide in network traffic.

BENEFITS

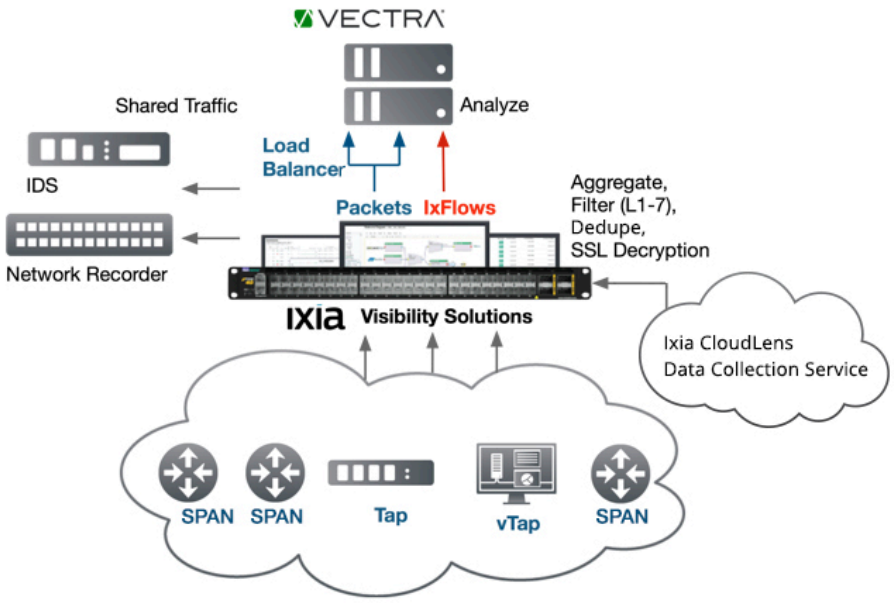
- **Complete visibility into cyberthreats inside the network** – The Ixia Network Visibility Architecture delivers to the Vectra Cognito platform all required traffic from anywhere in the network or cloud; 100% of traffic can be monitored, inspected and analyzed
- **Simplified deployment** – The Ixia/Cognito solution works flexibly in any network environment and shares access with deployed monitoring and security tools
- **Easily scalable** – Add additional 1-, 10-, 40-, or 100-gigabit ports as needed and dynamically adjust filters to meet any bandwidth requirements
- **Maximum efficiency** – The Ixia solution filters and removes unneeded traffic so the Cognito platform always operates at full efficiency

Solution

The Ixia Network Visibility Architecture and the Cognito® network detection and response platform from Vectra® work together to detect cyberattacks in progress amid the chatter of your network so security teams can quickly mitigate and prevent data loss.

Ixia'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 Cognito platform for inspection and analysis. Traffic is aggregated from all network access points to provide comprehensive visibility.

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



Network-based threat detection

The Vectra Cognito network detection and response platform delivers high-fidelity network metadata – knowledge of what's happening in every conversation – enriched with context specific to security applications, such as the names of hosts, existence of beacons and the privilege level of accounts. The genesis of the Cognito platform is based on a simple principle for finding hidden threats: Use an authoritative source of data and seek out the fundamental threat behaviors that cybercriminals can't avoid when they carry out an attack.

To do this, the Cognito platform relies on the only source of truth during a cyberattack – network traffic. Only traffic on the wire – in cloud, data center and enterprise environments – reveals the truth with fidelity and independence. Low-fidelity perimeter security only shows what you've already seen, not the hidden attacks that were missed.

The Cognito platform delivers a far more efficient way of analyzing network traffic at scale. Instead of traditional payload inspection, it uses AI, machine learning and behavioral traffic analysis to expose the fundamental behaviors of attackers as they spy, spread, and steal in the network – even in encrypted traffic.

Ixia directs traffic to Cognito and the Vectra X-series appliance

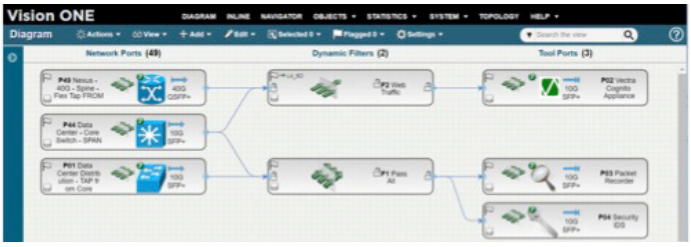
Ixia's intelligent visibility solutions complement the Cognito platform with fast, easy access to all required traffic anywhere in your hybrid environment—networks and data centers, or public clouds. The Ixia Vision NPBs simultaneously aggregate traffic from multiple SPANs, taps and vTaps in the network and direct it to Cognito and the Vectra X-series appliance. This ensures efficient access to asymmetric traffic across large heterogeneous networks.

Traffic that does not require analysis can be filtered out by the Ixia Visibility Architecture to prevent Cognito resources from being unnecessarily consumed. With the Ixia Visibility Architecture, traffic from network access points can be shared with multiple monitoring tools. This eliminates common SPAN/tap shortages that occur when another tool is attached to a needed access point. Ixia CloudLens also gathers traffic from public clouds thereby extending visibility into the cloud.

Additionally, by removing duplicate packets, Ixia NPBs can enhance throughput capacity. The automation capability in the Ixia Visibility Architecture integrates seamlessly with Cognito to enable a wide range of applications, including:

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

An intuitive GUI control panel makes Ixia NPBs easy to set up and use. Simply drag-and-drop a virtual connection between SPANs/taps and the Cognito platform to make a live connection.



The Cognito platform uses AI to detect attackers in real time and perform conclusive incident investigations. Cognito:

- Detects known and unknown threats in real-time anywhere in the network, including remote locations, network segments and cloud environments
- Exposes encrypted and hidden attack communications without decrypting traffic
- Reports threats throughout every phase of an advanced targeted attack
- Reports are only one click away and include threat severity and certainty scores, hosts under attack, and context about what attackers are doing
- Identifies all attacks without relying on signatures or reputation lists and on all devices, operating systems, and applications
- Deploys in passive mode on a SPAN or network tap

About Vectra

Vectra® is the leader in network detection and response – from cloud and data center workloads to user and IoT devices. Its Cognito® platform accelerates threat detection and investigation using artificial intelligence to enrich network metadata it collects and stores with the right context to detect, hunt and investigate known and unknown threats in real time. Vectra offers three applications on the Cognito platform to address high-priority use cases. Cognito Stream™ sends security-enriched metadata to data lakes and SIEMs. Cognito Recall™ is a cloud-based application to store and investigate threats in enriched metadata. And Cognito Detect™ uses AI to reveal and prioritize hidden and unknown attackers at speed. For more information, visit vectra.ai.

About Ixia's Network Visibility Solutions

Ixia provides complete network visibility into physical and virtual networks, improves network security, and optimizes monitoring tool performance. Ixia's solution ensures that each monitoring tool gets exactly the right data needed for analysis. This improves the way you manage your data center and maximizes return on investment. Our customers include large enterprises, service providers, educational institutions, and government agencies.

Additional information about the Ixia Visibility Architecture can be found at https://www.ixiacom.com/solutions/visibility-architecture.

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai