VECTRA®

ixia

The Ixia Visibility Architecture provides complete network access for Cognito

JOINT SOLUTION BENEFITS

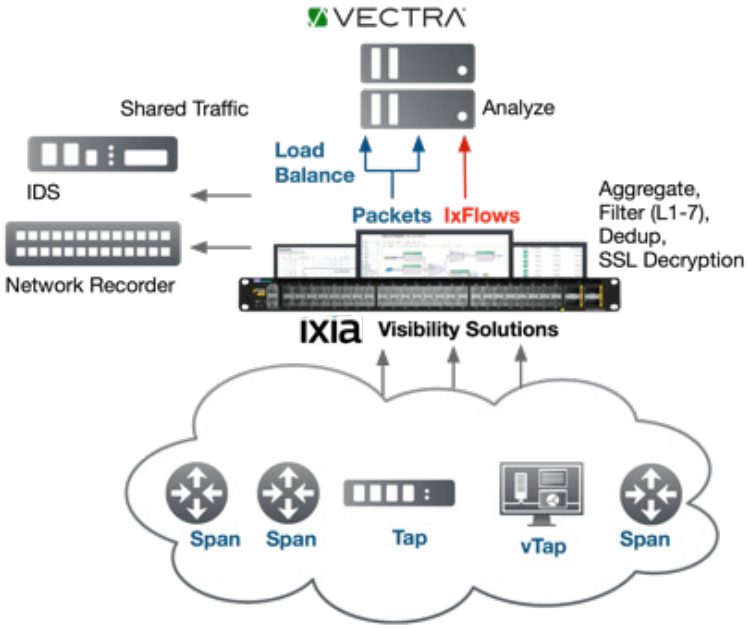
- Complete visibility of cyber threats inside the network – The Ixia Visibility Architecture delivers to Vectra all required traffic from anywhere in the network; 100% of traffic can be monitored, inspected, and analyzed
- Simplified deployment – The Ixia/Cognito solution is flexible to work in any network environment and share 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™ automated threat detection and response platform from Vectra® work together to detect cyber attacks in progress amid the chatter of your network so security teams can quickly mitigate and prevent data loss.

Ixia 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.

Cognito then performs continuous analysis of internal network traffic to automatically 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

Using artificial intelligence, Cognito automates the real-time detection and response to active cyber attacks that evade perimeter security defenses and spread inside networks.

Cognito picks up where perimeter security ends by providing deep, continuous analysis of both internal (east-west) and Internet (north-south) network traffic to detect all phases of an attack during which hackers spy, spread, and steal inside your network.

The Cognito platform continuously listens, identifies, learns and follows latent attack behaviors to detect threats and anticipate a cyber criminal's next move. A unique combination of data science, machine learning, and behavioral analysis enables Cognito to detect known and unknown zero-day threats without signatures or reputation lists.

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

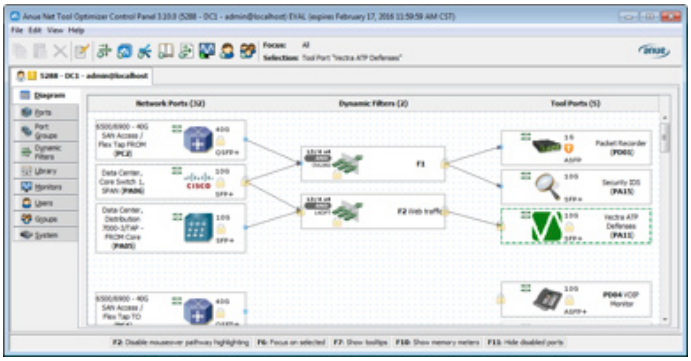
The Ixia NPB simultaneously aggregates traffic from multiple SPANs, taps, and vTaps in the network and directs it to Cognito and the Vectra X-series appliance. This ensures efficient access to asymmetric traffic across large heterogeneous networks.

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 APs 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.

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

- Load-balancing traffic across multiple X-series input ports
- Dynamically tightening filters as needed 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.



Cognito offers a wide range of automated threat detection and response capabilities

- Detects known and unknown threats in real-time anywhere in the network, including remote locations and network segments
- 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 that are 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 an artificial intelligence company that is transforming cybersecurity. Its Cognito™ platform is the fastest, most efficient way to detect and respond to cyberattacks, reducing security operations workload by 168X. Cognito performs real-time attack hunting by analyzing rich metadata from network traffic, relevant logs and cloud events to detect attacker behaviors within all cloud and data center workloads, and user and IoT devices. Cognito correlates threats, prioritizes hosts based on risk and provides rich context to empower response. Cognito integrates with endpoint, NAC, firewall security to automate containment, and provides a clear starting point for searches within SIEM and forensic tools.

About the Ixia Visibility Architecture

The Ixia Visibility Architecture 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 http://www.ixiacom.com/solutions/visibility.

VECTRA®
Security that thinks®

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