Seconds matter during cyber attacks, and rapid response depends on being able to see what’s happening everywhere in your network. You need to know who’s interacting with your systems, and what actions your systems and devices are taking, even in the cloud.

Real-time breach investigation starts with two crucial steps: accessing the right traffic from your hybrid network and automatically applying intelligence to analyze it. Together, Ixia and FireEye deliver the complete visibility, automation, and insights your security experts need to investigate and respond to threats across your networks, clouds, and data centers.

FireEye solutions detect and stop attacks traditional and next-generation firewalls, intrusion prevention systems (IPS), and web gateways miss to promote faster response and deeper forensics. Ixia’s intelligent visibility architecture captures and delivers exactly the right data to each element of the FireEye Security Suite deployed inline or out-of-band.

Ixia: It All Starts with the Right Data
Cyber security requires complete visibility from the premise to the data center to the cloud, and back. Combining intelligent visibility from Ixia with FireEye Security Suite creates scalable, reliable access to vital data from your hybrid network.

Visibility begins with using taps or other devices to capture packets from the network or cloud. Ixia’s wide variety of network and virtual taps (vTaps) delivers data to the Vision network packet brokers (NPBs) that aggregate, filter, and shape traffic for rapid analysis by FireEye security solutions.

Vision network packet brokers (NPBs) optimize the use of FireEye Network Security and other monitoring solutions by distributing or “load balancing” traffic to multiple tools. This promotes rapid scalability and fast response.

Ixia’s external iBypass solutions bring additional visibility to inline deployments, monitoring the health of FireEye appliances and adding failover protection. iBypass sends heartbeat packets to FireEye appliances and automatically re-routes traffic when heartbeats are not returned as expected due to link or power failure, devices being taken out of service for maintenance and other unforeseen events.

FireEye Security Suite stops threats and attacks across hybrid networks with simplified, interoperable, multi-vector security. The suite features network, cloud, endpoint and email security as well as forensics to detect, block, investigate and prevent future attacks.

Amidst a fast-changing threat landscape, FireEye helps organizations defend their networks against any attack at any stage:

- At headquarters, branch and home offices
- Hidden within inbound Internet traffic or outbound communications
- Exploits targeting Microsoft Windows, Apple macOS operating systems, or application vulnerabilities

**Figure 1.** Architecture diagram of the joint solution from Ixia and FireEye.
Over the years, FireEye has gathered evidence on how lack of visibility has impaired investigations. Tools must be optimized so investigators can perform relevant queries efficiently and effectively.

FireEye Security Suite includes:

- **Cloud-based Multi-Vector Virtual Execution (MVX) engine:** This dynamic FireEye analysis engine inspects suspicious network traffic to identify attacks that evade traditional signature- and policy-based defenses. The MVX engine stops advanced malicious attacks, accurately confirms zero-day attacks and creates real-time protections.

- **Intelligence-Driven Analysis (IDA) technologies:** IDA uses multiple contextual, dynamic rules engines to detect and block malicious activity in real time and retroactively. Solutions use the latest machine-, attacker- and victim intelligence from frontline attacks.

- **Network Security appliances:** FireEye Network Security appliances include the MVX engine, integrated IPS, as well as zero-day and signature-less malware attack detection. Network Security devices can be deployed inline to confirm zero-day attacks and create real-time threat intelligence. They can also be deployed out-of-band to block suspicious TCP, UDP or HTTP connections.

- **Network forensics:** Solutions provide continuous high-speed packet capture and querying to pinpoint data and speed investigations. Rich attack context and insights gained while responding to real-world threats delivers everything security teams need to detect, triage, and minimize the impact of attacks.

- **Email security:** FireEye Email Security comes in cloud- and server-based versions to guards against sophisticated spear-phishing and impersonation attacks, unknown malware and spam. This solution blocks threats and makes it easy to manage policies and prioritize responses.

**About Keysight Technologies**

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. More information is available at www.keysight.com.

**About FireEye**

FireEye is the intelligence-led security company. Working as a seamless, scalable extension of customer security operations, FireEye offers a single platform that blends innovation in security technologies, national-state grade threat intelligence and world-renowned FireEye Mandiant consulting. With this approach, FireEye eliminates the complexity and burden of cyber security for organizations struggling to prepare for, prevent and respond to cyber attacks.