SOLUTION BRIEF

FireEye + Ixia: Turnkey Security and Visibility for Turnkey Private Clouds

Large government, finance and healthcare entities face strict regulations for network security. These regulations lead many to select turnkey private cloud platforms as an alternative to public clouds.

Intended to reduce risk, the use of private cloud platforms can ultimately compromise intelligence and operations because cloud providers may not supply data needed by analysis solutions — namely, packet data. FireEye and Ixia have teamed up to deliver a secure, turnkey visibility solution for operating private clouds.

TURNKEY PRIVATE CLOUDS: UNIQUE BENEFITS WITH UNIQUE CHALLENGES

While cloud computing offers significant benefits, some organizations are prohibited from connecting their computing infrastructure to the Internet or must adhere to strict security guidelines. A secure private cloud offers the best of both worlds: the flexibility and cost efficiency of cloud, with the isolation and separation required for compliance.

Major public cloud service providers are stepping up to meet the needs of organizations that cannot adopt public cloud offerings. Pre-built private cloud platforms such as Microsoft Azure Stack deliver similar features and are easy to deploy and scale but remain completely isolated from the Internet. Customers still need to keep deployments updated but doing so does not require dedicated cloud architects or developers.

Company
Government agency with centralized technology environment

Key Issues
Azure Stack private cloud platform does not provide access to traffic packets needed to detect threats in virtual traffic

Solutions:
Private cloud visibility solution:

- FireEye
- Ixia CloudLens with vTaps and Vision packet brokers

Results

- Highly secure, compliant private cloud
- Faster identification and resolution of threats
- Ability to also feed traffic to APM/NPM solutions

ixia
A Keysight Business

Setting up clouds to host applications in a centralized environment promotes stronger, easier security, but services such as Microsoft AzureStack may not give administrators access to the underlying infrastructure components, such as the hypervisor layer. This limitation means security teams do not have access to the virtual traffic in their own private cloud, a visibility gap with serious implications for security.

Complete hybrid network security

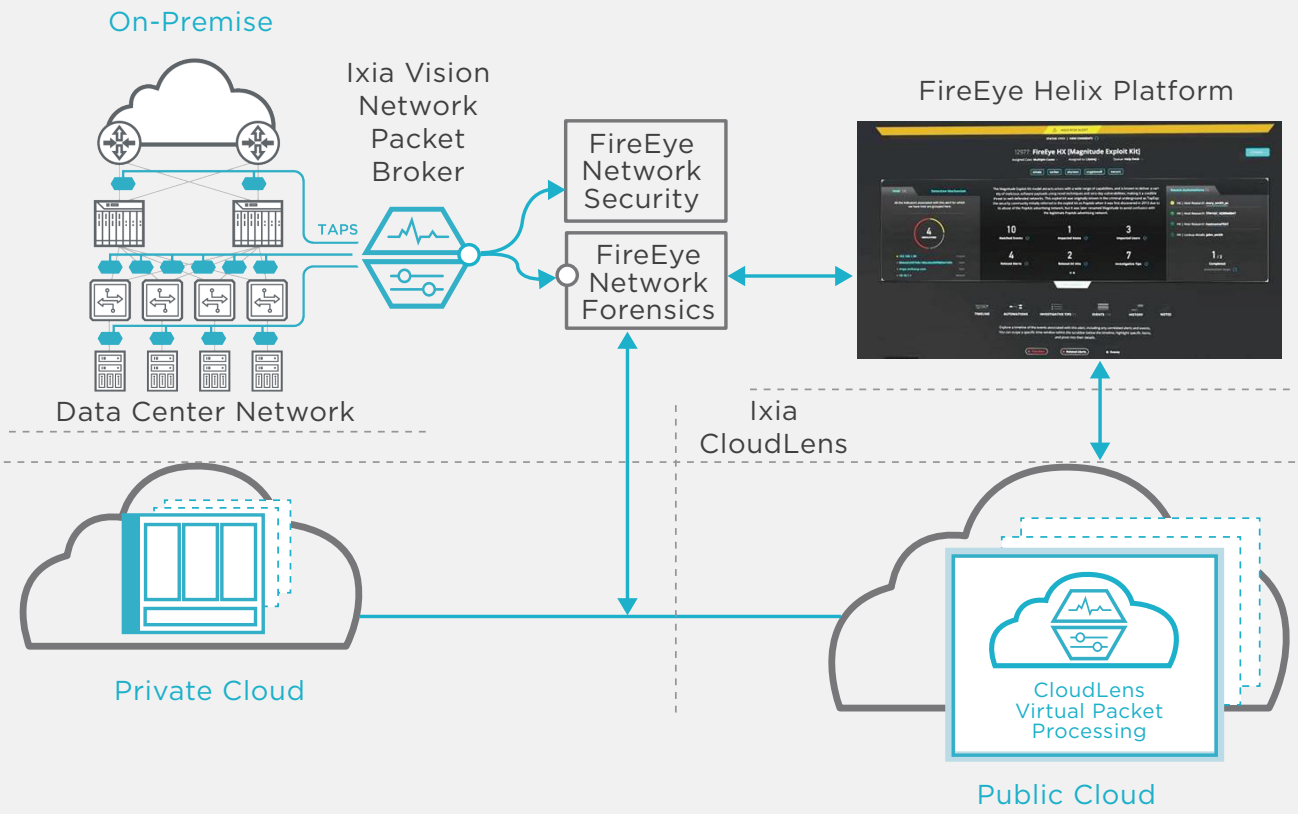
In one recent deployment scenario, a joint customer planned to send traffic to a private cloud for monitoring by best-of-breed solutions including FireEye Network Security and FireEye Network Forensics to provide network and endpoint threat detection and security forensics. FireEye solutions use deep packet inspection (DPI) to understand the context of communications moving through the network and to identify "indicators of compromise" that provide evidence of a network attack or data exfiltration.

The FireEye solution includes:

- **Multi-Vector Virtual Execution (MVX) cloud security engine:** The FireEye dynamic analysis engine inspects suspicious network traffic to identify attacks that evade traditional signature- and policy-based defenses. The MVX engine stops advanced malicious attacks, confirms zero-day attacks, and creates real-time protections.
- **FireEye Network Security appliances:** FireEye Network Security appliances include MVX, as well as an integrated intrusion prevention system (IPS) and zero-day and signature-less malware attack detection.
- **FireEye Network Forensics appliances:** These appliances enable 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.

FIREEYE™

Over the years, FireEye has cultivated anecdotes about how a lack of visibility has impeded investigations. Tools must be optimized so investigators can perform relevant queries efficiently and effectively.



Packet data is a must

Ixia's hybrid network visibility solutions provide the packet-level detail critical to analysis using physical and virtual taps (vTaps) and intelligent processing by Vision network packet brokers (NPBs). CloudLens vTap Sensors are used to access packets in the Azure Stack platform, along with CloudLens vTaps accessing virtual traffic within in the on-premises infrastructure.

In addition to packet access, the Ixia visibility platform uses a powerful processing and filtering engine inside its NPBs to strip away unnecessary data and isolate the packets that require security inspection. Pre-processing significantly reduces the load on monitoring tools and can reduce the need to add capacity. Ixia's NPBs can also decrypt secure packets for faster processing, eliminating the need for a separate decryption device.

In this case, the joint customer also chose to aggregate packets at the network edge to improve performance using the Ixia Vision Edge NPBs. In the data center, Vision ONE packet brokers ensure filtered, pre-processed traffic is delivered to security solutions without disruption. With Vision ONE's drag-and-drop interface, administrators can easily direct traffic to multiple monitoring solutions simultaneously to accelerate threat identification and resolution.

WHY THE JOINT SOLUTION?

Together, FireEye and Ixia allow the customer to monitor all traffic passing through its network, even when IT does not have access to the physical infrastructure. The customer considered using a competing network visibility platform installed in one of its data centers, but the solution did not have a way to access packets in the Azure Stack cloud. Ixia's provider-neutral CloudLens visibility solutions deploy sensors in both public and private clouds to extend visibility to every virtual packet needed for performance and security monitoring.

HOW SECURE IS YOUR CLOUD?

Customers choose the joint FireEye and Ixia solution to achieve complete cloud visibility and reliable security for Azure Stack and other private, public, and hybrid cloud environments. To learn more about tailoring solutions to your unique cloud environments, contact your FireEye or Ixia representative today.

What Experts are Saying

"As a government entity, we are not allowed to use public clouds or any solutions that require us to be connected to the internet."

— Chief Information and Security Officer, National Government

"We plan to expand the Keysight | Ixia visibility platform, to provide relevant packet data to our network and application performance monitoring solutions, as well."

— Lead Solution Architect, National Defense Agency

Learn more at: www.ixiacom.com

For more information on Ixia products, applications, or services, please contact your local Ixia or Keysight Technologies office. The complete list is available at: www.ixiacom.com/contact/info