New Visibility Platform Enables Security and Control in the Cloud

In many industries and organizations, outsourcing of information technology and data processing to third-party specialists is common practice. This particular IT provider suffered a major setback during the past year when unexpected flooding damaged their data center facility and forced them to rebuild. In the true spirit of making the best of a bad situation, the IT team decided to embrace public cloud infrastructure as part of their recovery. The problem was: how would they achieve the same level of security protection in the cloud as they had in their on-premises data center?

VISIBILITY AND CONTROL IN THE CLOUD

This organization already relied on network visibility to increase the efficiency of their network monitoring. Their Gigamon packet processor installed several years ago needed an upgrade. They had run out of onboard capacity enhancements and needed to expand to a new chassis. It was the right time to consider whether their current visibility solution offered the features and functionality necessary to support their expected growth and use of the public cloud. They took a serious look at the architecture of Ixia’s solution and compared it with their existing Gigamon platform.

The team understood the value of establishing a visibility and control layer for the management of diverse IT environments. Critically, their lead security architect wanted to continue using the company’s existing set of on-premises security monitoring tools, which had been tuned and configured over time to their unique

Company
Provider of IT services to a large, regional auto dealership

Key Issues
• Enable robust security monitoring of public cloud workloads
• Update network visibility platform to increase flexibility and scalability

Challenge
• No ability to directly tap public cloud infrastructure
• Security monitoring solutions require packet data

Solution
• Ixia CloudLens SaaS
• Ixia Vision ONE network packet broker (on-premises)
• Existing monitoring solutions from Cisco and Forcepoint

Results
• Single interface for managing the access and filtering of packet data from both AWS and Azure clouds
• Visibility platform now capable of supporting line-rate inline security monitoring
• Eliminated a year’s worth of visibility support costs ($40,000)
needs. The team questioned whether they could achieve the same results with an all-cloud security architecture. Although it would require the backhaul of cloud traffic to the data center for processing, they felt the potential risk of an attack or data breach outweighed the cost of transferring data from the cloud to the data center.

SWITCHING TO A NEW VISIBILITY PLATFORM
The company’s new data center design began with a closer look at the cloud offering of their existing visibility vendor, Gigamon. Ultimately, the IT team determined that the architecture, which was not cloud-native, would not scale efficiently, and the administrative interface was not conducive to efficient management. The team then turned to an examination of Ixia’s visibility platform and cloud-focused virtual taps. They noted several important benefits of the Ixia platform:

Automatic Visibility and Unlimited Scalability
Ixia CloudLens, a fully distributed, container-based solution, deploys automatically inside each new public cloud instance. CloudLens requires no additional infrastructure or manual configuration to begin collecting cloud packet data. With visibility automatically installed in each cloud instance, deployment is consistent and errors are eliminated.

Integration with Popular Security Solutions
Overall, a broad range of security monitoring solutions can leverage the filtered packet data provided by the Ixia Vision ONE and CloudLens visibility solutions. The company can collect packet data in the cloud and send it directly to security and monitoring tools in the cloud or transfer it back to the data center to continue using solutions on-premises, for maximum flexibility. Ixia integrates with a Visibility Ecosystem of pre-validated Technology Partners that are already configured to receive data from CloudLens in the cloud. No backhaul is required.
Multi-Cloud Readiness
Due to the quick onset of the data center outage, workloads needed to be transferred quickly and apportioned between AWS and Azure cloud instances. This allowed the team to evaluate both cloud providers and maintain flexibility should one vendor prove unable to meet their requirements. The IT team appreciated that Ixia CloudLens was already integrated and certified to work in both these environments, so traffic collection and aggregation could begin as soon as Ixia’s solution came online.

Support for Inline Security
The senior security architect also wanted a visibility solution that could support inline monitoring of live traffic in the future. Inline monitoring requires a high performance engine that can process network packets at line-rate speed and not degrade responsiveness and availability. Ixia offers external bypass switches to monitor inline tools with nanosecond response technology and the fastest packet processing engines in the industry. With Vision ONE installed on-premises, the company has the foundation to deploy fast inline security monitoring with minimal application latency.

COST-SAVING BENEFITS
Easier Management Interface
Once the IT team had deployed Ixia’s management interface — used for configuring both the on-premises Vision ONE packet broker and CloudLens — they discovered how much easier it could be to configure new data filters and set up data delivery to monitoring solutions. They quickly became fans of Ixia’s powerful, drag-and-drop interface, which required no coding, testing, or specialized training.

Automatic Maintenance of Filter Overlaps
Previously, one of the most time-consuming and error-prone tasks was manually maintaining a table of each security tool’s data requirements and the overlaps between tools. The team was relieved to learn that Ixia CloudLens and Ixia Vision ONE
“We no longer have to worry about missing something in the cloud because packet data from our cloud infrastructure is automatically collected by CloudLens, transferred securely to our data center, and delivered as needed to our monitoring solutions.”

- Manager of Network Operations Center

automatically create a filter overlap table and update it each time a new network segment or security solution is added. Now, the staff has less work and tools receive exactly the data they need with far fewer errors.

Support Cost Savings
The company’s new Ixia visibility platform includes the first year of support and maintenance in the initial contract, so the IT team reassigned the funds originally set aside for maintenance of its Gigamon platform to another project waiting for resources.

**ROLLOUT OF SECOND DATA CENTER**
Successful implementation paved the way to deploy a second data center. The company’s new Ixia-based visibility and control layer lets them easily take the configuration rules and policies they developed and apply them to a second environment in much less time. Once deployed, their second location will help them achieve geographic diversity and enable faster disaster recovery.

**CONCLUSION**
This provider of IT services has successfully incorporated public cloud infrastructure into their IT environment while extending the protection of their on-premises security solutions to their cloud instances. The visibility platform created with Ixia CloudLens SaaS and Ixia Vision ONE makes sure every packet entering or leaving their enterprise data system is available for inspection and analysis. Their security solutions now have access to packet details that help isolate suspicious traffic more quickly and take action before vulnerabilities are exploited. The security team can resolve more alerts more efficiently, and the operations staff does not have to manually configure traffic access for each cloud deployed.

Learn more at: [www.ixiacom.com](http://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](http://www.ixiacom.com/contact/info)