Nominee: Ixia

Nomination title: CloudLens Public - visibility as a service in public clouds

As organizations migrate to the cloud, they have more network segments to manage and more potential blind spots in their networks. Regardless of where infrastructure and applications reside, the demands for security and compliance remain the same, but organizations are finding that their traditional network visibility solutions are unable to meet their needs for complete visibility of cloud-based data.

Cloud visibility & security concerns

As the public cloud infrastructure is owned by the cloud service provider, customers don't have access to application and network data. And without granular access to cloud traffic, blind spots in a network are created that compromise application monitoring, as well as overall security.

In February 2017, Ixia surveyed over 220 senior IT staff at enterprises that use network visibility solutions, on their top cloud security concerns and the role network visibility plays in security: 76% of respondents were 'very concerned' or 'concerned' about security in their cloud environment. The top security concerns with cloud was 'loss of control over network data' (56%) and achieving full visibility across their networks (47%).

Ixia's CloudLens Public addresses these concerns. It is the first network-level solution that provides Visibility-as-a-Service (VaaS) through a Software-as-a-Service (SaaS) offering.

Why CloudLens Public matters

Designed from the ground up to retain the elastic scale, flexibility, and agility benefits of the cloud, CloudLens Public provides an intelligent and automated cloud VaaS that scales with public cloud infrastructures. It helps security and monitoring tools to ensure the reliability, security, and performance of mission-critical applications in public cloud environments.

CloudLens Public addresses the challenges of capturing and filtering traffic in the public cloud because it scales horizontally as instances are created and destroyed. CloudLens Public uses metadata from cloud platform instances to classify them; because metadata inherently exists for each new instance that is created, the platform automatically knows how to treat it and which security and monitoring policies need to be applied.

Consequently, traffic from instances is appropriately filtered and routed to security and monitoring tools, without requiring human intervention.

With a security and monitoring tool partner ecosystem, CloudLens Public ensures that tool instances also scale. An auto-scaling solution eliminates the burden of management to save time and money. It also mitigates the inherent risk of error with manual configuration. CloudLens Public has been tested to support thousands of instances.

CloudLens Public aligns to one of the core tenets and drivers for why organizations move to cloud: No guesswork with regards to sizing for peak use, optimizing how resources are allocated.

"Adoption of public cloud services will be limited by the performance and security of enterprise applications and workloads processed in cloud environments," said Jim Duffy, Senior Analyst, 451 Research. "Ixia's CloudLens Public offers enterprises 'visibility-as-a-service,' where all of the packet brokering takes place at the source. This could enhance scalability and network agility."

"Ixia CloudLens Public was designed and built for the cloud and as a result, it is inherently elastic and scalable," said Sushil Kumar, Senior Vice President of Product Management and Strategy, Agile Operations, CA Technologies. "CloudLens provides CA's network monitoring solutions the visibility needed to monitor end-to-end response times to track and optimize the end user experience, no matter where an application is deployed."

Why nominee should win

-- CloudLens Public boosts cloud security by giving customers visibility into public clouds that they cannot get from the public cloud provider

-- It automates cloud visibility management by providing it as a service – so no architectural changes required

-- It elastically scales on-demand – so visibility auto-scales horizontally along with the instances monitored and the cluster of instances that are needed to do the monitoring

-- It reduces errors by eliminating manual configuration, and is easy to use and setup with a drag and drop interface

-- Reduces bandwidth to tools by filtering packets at the source instances, eliminating unwanted traffic so tools operate optimally