

CloudLens Public — Visibility-as-a-Service for public cloud



Data Sheet



VISIBILITY SOLUTION FOR THE PUBLIC CLOUD

PROBLEM: ORGANIZATIONS NEED VISIBILITY IN THE CLOUD FOR SECURITY AND MONITORING

Organizations are migrating workloads to the cloud because the cloud offers scale, agility and flexibility. These organizations will require visibility to adhere to their security, compliance and monitoring policies in the public, private and hybrid cloud. However, traditional network visibility solutions are unable to address the key considerations of providing visibility in the cloud:

- Customers do not have access to the physical infrastructure when using public cloud – so traditional, physical solutions cannot be used
- Public cloud is a multi-tenant, distributed architecture. There is no defined space where an organization's data exists, making it difficult to capture
- Cloud is scalable, so instances are transient by nature – a moving target that is hard to track
- East-West (web-to-app and app-to-database) traffic is difficult to track with transience and multi-tenancy considerations
- Cloud benefits of flexibility, elasticity, and agility must be retained.

HIGHLIGHTS

- Auto-scales elastically, on-demand with cloud instances
- Handles cloud scale – tested to thousands of instances
- No additional infrastructure or any architectural changes
- Provided Software-as-a-Service (SaaS) – requires minimal management and is always available.
- Reduces error with minimal setup and ongoing management
- Easy-to-use, drag-and-drop interface with a network to tools layout
- Cloud service provider agnostic
- Multi-cloud & hybrid cloud capable
- Incremental implementation – only use and pay for what you need

SOLUTION: CLOUDLENS™ PUBLIC IS THE FIRST SOFTWARE-AS-A- SERVICE NETWORK VISIBILITY SOLUTION

Ixia's CloudLens Public, part of the broader CloudLens platform, is the first software-as-a-service (SaaS), network-level solution that provides [Visibility-as-a-Service \(VaaS\)](#). Designed from the ground up to retain the elastic scale, flexibility, and

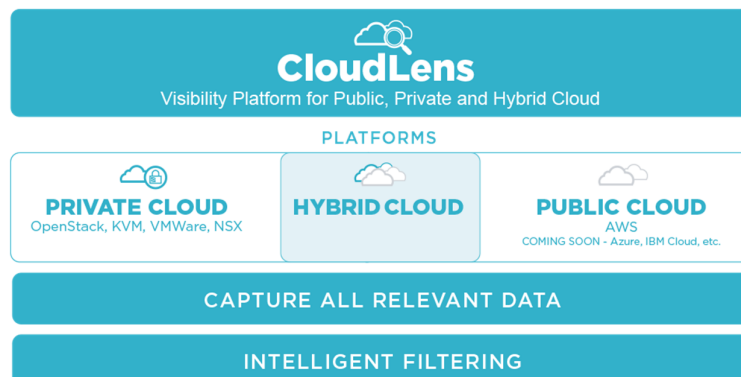


Figure 1: CCloudLens, Ixia's cloud visibility platform

agility benefits of the cloud, CloudLens Public provides intelligent and automated cloud VaaS that scales with public cloud infrastructures.

- It is low impact – it requires no architectural or infrastructure changes
- Has a cloud visibility ecosystem – for seamless operation with leading security, performance and monitoring tools.
- Setup and ongoing management are minimal.
- Auto-scales elastically, on-demand with cloud instances
- Is cloud service provider/platform agnostic

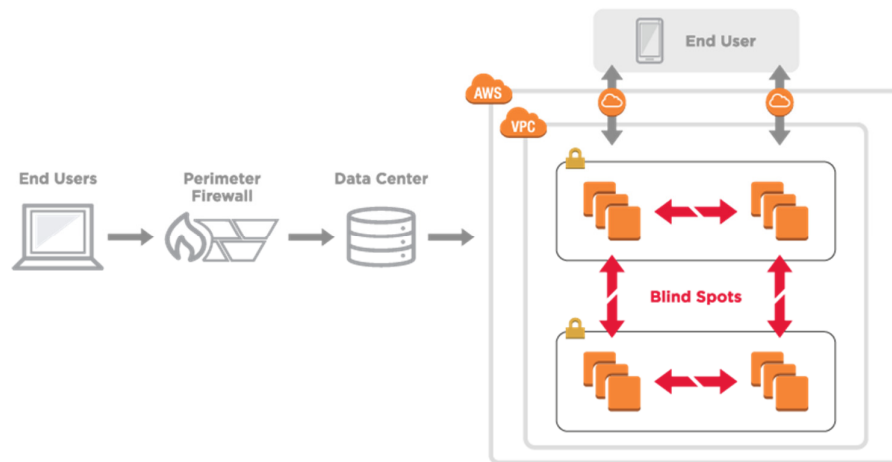


Figure 2 Public and Hybrid Cloud Monitoring – Addressing East-West, or inter-instance traffic visibility

CloudLens Public is ideal for the following scenarios:

- Large enterprises applying a hybrid model using public cloud, private cloud and on premise environments.
- Organizations with a multi-cloud strategy using many cloud service providers' offerings as because CloudLens Public is cloud service provider agnostic.
- Organization that have fully migrated to a public cloud implementation – CloudLens Public is cloud-native and offers the scale, flexibility and agility of cloud.

PRODUCT CAPABILITIES:

There are two components of CloudLens Public which work together to enable visibility in the public cloud:

A SaaS visibility management platform. This is where users can configure visibility and define filtering.

Sensors and connectors that are containerized, Docker-based software that sit within the source and tool instances respectively, with full access to rich metadata about those instances.

PURPOSE BUILT FOR CLOUD

A CLOUD-NATIVE, SERVERLESS DESIGN

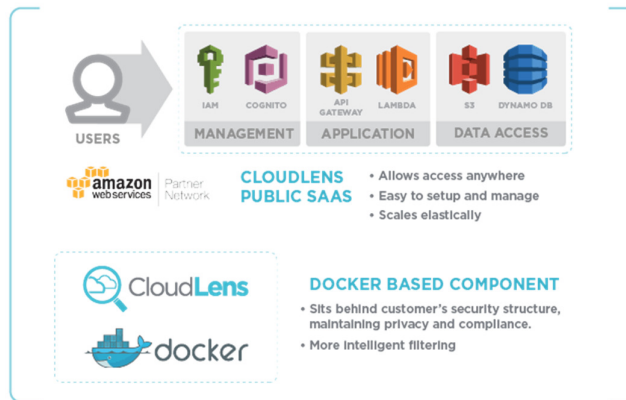


Figure 3: CloudLens Components

Using CloudLens Public is simple – a user must identify instances, create a project, load sensors to the source instances, draw a visibility path and configure filters. After that, it auto-scales.

Since CloudLens Public has Docker-container that sit in a customer's instances, it has access to metadata, which is information about them that a cloud service provider provides. From the source instance, we can identify the Cloud Service Provider (AWS, Azure, IBM), Region, AZ, Kernel module, CPU and memory etc. and from the tool instance, we can determine if the tool is an APM, NPM, IDS or SIEM. This metadata is sent from the sensors/connectors to the management platform. CloudLens Public uses this metadata and makes it available to users as searchable criteria – a way for users to easily organize their instances into named groups. Once instances are grouped, data paths are easily configured in the SaaS management platform and filters can be applied. Filters are set at the sensor in the tool instance, so only filtered packet data goes to the tools.

Also, because CloudLens Public uses metadata, when new instances appear or disappear, the platform knows where it belongs based on group criteria. Consequently, the correct security and monitoring policies can be applied: for example, which instances' traffic need to go an IDS vs. a SIEM. That data is then routed to the correct tools without the need for human intervention– reducing chance of error and saving time. It also means that customers are only using and paying for what they need, which eliminates the guesswork around peak-demand sizing.

Filtered packet data is sent from source to tool instances via a secure visibility path – an encrypted overlay tunnel via a peer-to-peer VPN. This guarantees security and confidentiality when data goes inter-cloud or across the Internet.

Finally, Ixia further simplifies use with its growing [Cloud Visibility Ecosystem](#) – technology partners who have integrated with CloudLens Public, so the Docker-based component is already loaded to their tool instances. All users need to do is set up their source instances and the rest is done. Again, this reduces error and eliminates manual configuration.

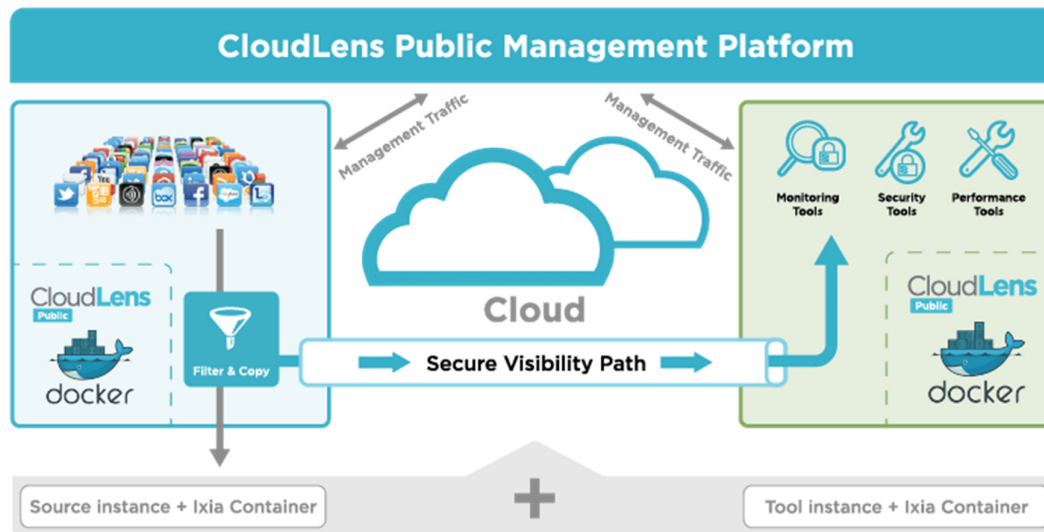


Figure 4: Overview of CloudLens in action

KEY FEATURES:

CLOUD-NATIVE SERVERLESS ARCHITECTURE	
Elastic scale, on-demand <ul style="list-style-type: none"> Elastically scales on-demand – so visibility auto-scales along with the instances monitored and the cluster of instances that are needed to do the monitoring Tested to handle thousands of instances in large-scale implementations 	Cloud service provider agnostic <ul style="list-style-type: none"> Capable of using metadata from any cloud service provider platform to provide visibility Does not require architectural changes <ul style="list-style-type: none"> SaaS implementation means Ixia does the heavy lifting behind the scenes. So, you don't have to change anything.
DOCKER-BASED CONTAINERIZED COMPONENT	
Inherent security <ul style="list-style-type: none"> Uses a secure visibility path to transfer filtered packets. It is an encrypted overlay tunnel via a peer-to-peer VPN Embedded within the instance structure, so it eliminates the risk of cross tenant violations Runs from behind SSL offload services, eliminating the need for decryption 	Filter at the source <ul style="list-style-type: none"> Eliminates single point of failure: filters packet data at each source instance, so an inline virtual packet broker does not become a single point of failure in the network Reduces bandwidth to tools by filtering packets at the source instances, eliminating unwanted traffic so tools to operate optimally

	Metadata Access <ul style="list-style-type: none"> Improves scalability because instances can be grouped automatically as they spin-up, ensuring the correct security monitoring policies are affected immediately
EASY TO USE INTERFACE	
Easy setup & management <ul style="list-style-type: none"> Simple, 5-step setup that takes minutes not hours. 	Reduce Error <ul style="list-style-type: none"> No CLI, mapping or anything like that. Just drag-and-drop.
CLOUD VISIBILITY ECOSYSTEM	
Easy setup & management <ul style="list-style-type: none"> One less step in the setup process. 	Reduce Error <ul style="list-style-type: none"> Leading security, monitoring and performance tools, pre-configured to work with CloudLens Public.

SPECIFICATIONS

- Browsers: Chrome & Firefox
- Linux OS: Amazon AMI, CentOS 7, Ubuntu
 - All Linux AMI are tested on x86_64 architect
 - Host Linux kernel must be version 3.1 or higher

IXIA WORLDWIDE HEADQUARTERS

26601 AGOURA ROAD
CALABASAS, CA 91302

(TOLL FREE NORTH AMERICA)

1.877.367.4942

(OUTSIDE NORTH AMERICA)

+1.818.871.1800

(FAX) 818.871.1805

www.ixiacom.com

IXIA EUROPEAN HEADQUARTERS

IXIA TECHNOLOGIES EUROPE LTD
CLARION HOUSE, NORREYS DRIVE
MAIDENHEAD SL6 4FL
UNITED KINGDOM

SALES +44.1628.408750

(FAX) +44.1628.639916

IXIA ASIA PACIFIC HEADQUARTERS

101 THOMSON ROAD,
#29-04/05 UNITED SQUARE,
SINGAPORE 307591

SALES +65.6332.0125

(FAX) +65.6332.0127