DATA SHEET

CloudLens SaaS — Public, Private, and Hybrid Cloud Visibility

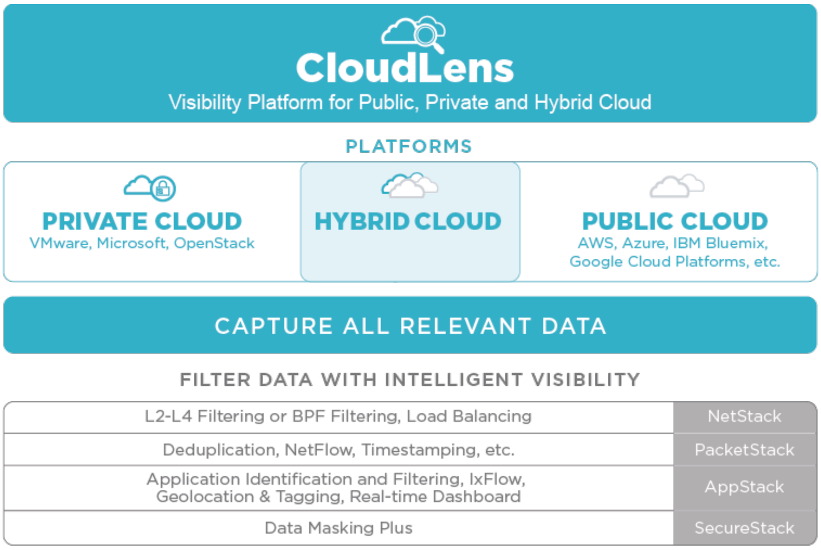
Organizations Need Visibility to Secure and Monitor their Cloud Environments

Organizations are migrating workloads to the cloud because it offers scale, agility and flexibility. These organizations 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 or hypervisors – so traditional, physical visibility 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 data
- Public cloud security is a shared and often misunderstood responsibility between CSPs and customers
- Cloud is dynamic, so instances are transient by nature – a moving target that is hard to track
- Many organizations use multiple cloud vendors, to avoid vendor lock-in, along with private data centers – requiring visibility across a complex environment
- Organizations may need to move data from one cloud provider to another, or backhaul to the data center

Highlights

- Multi-platform capable, cloud service provider and platform agnostic
- 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
- Pay-per-use model



CloudLens

Visibility Platform for Public, Private and Hybrid Cloud

PLATFORMS

PRIVATE CLOUD
VMware, Microsoft, OpenStack

HYBRID CLOUD

PUBLIC CLOUD
AWS, Azure, IBM Bluemix, Google Cloud Platforms, etc.

CAPTURE ALL RELEVANT DATA

FILTER DATA WITH INTELLIGENT VISIBILITY

L2-L4 Filtering or BPF Filtering, Load Balancing	NetStack
Deduplication, NetFlow, Timestamping, etc.	PacketStack
Application Identification and Filtering, IxFlow, Geolocation & Tagging, Real-time Dashboard	AppStack
Data Masking Plus	SecureStack

KEYSIGHT TECHNOLOGIES

- Workloads are containerized and deployed as microservices in Kubernetes clusters
- Any visibility solution must retain the cloud benefits of flexibility, elasticity, and agility

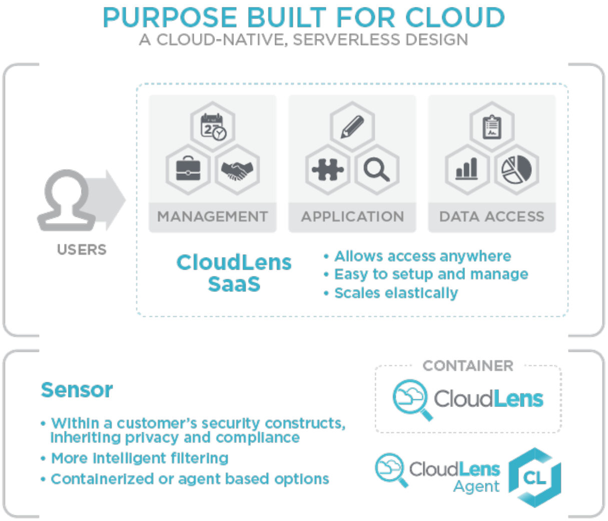
CloudLens SaaS is the First Software-as-a-Service Network Visibility Solution

Ixia's CloudLens is the first software-as-a-service (SaaS), network-level solution that provides Visibility-as-a-Service (VaaS) for public, private and hybrid cloud. Designed from scratch for those environments, it can deliver the elastic scale, flexibility, and agility benefits of the cloud in a visibility platform. CloudLens:

- Is multi-platform capable and supports all leading platforms
  - CloudLens is cloud service provider or platform agnostic and supports Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform, IBM Bluemix, Alibaba Cloud, Century Link Cloud, and any other CSP platform
  - Supports leading hypervisors including VMware and KVM/Openstack for on-premises and private cloud environments
- Supports both Windows and Linux workloads
- Is low impact – requires no architectural or infrastructure changes
- Provides packet visibility across physical, virtual, private, hybrid, and public clouds
- Supports container and Kubernetes visibility, providing security and monitoring tools with the information they need to be effective
- Has a cloud visibility ecosystem for seamless operation with leading security, performance and monitoring tools, both open-source and commercial

Use cases:

- Large enterprises applying a hybrid model using public cloud, private cloud and on premises environments – CloudLens can backhaul data securely to existing tools or route to cloud-native tools
- Organizations with a many or multi-cloud strategy, orchestrated or not, because CloudLens is cloud service provider agnostic – CloudLens can securely send data cross-CSP or collect data concurrently from multi-cloud application deployments
- Organization that have fully migrated to a public cloud implementation – CloudLens is cloud-native and offers the scale, flexibility and agility of cloud. CloudLens uses consumption-based billing, so you pay for only what you use


PURPOSE BUILT FOR CLOUD
A CLOUD-NATIVE, SERVERLESS DESIGN
USERS
MANAGEMENT
APPLICATION
DATA ACCESS
CloudLens SaaS
• Allows access anywhere
• Easy to setup and manage
• Scales elastically
Sensor
• Within a customer's security constructs, inheriting privacy and compliance
• More intelligent filtering
• Containerized or agent based options
CONTAINER
CloudLens
CloudLens Agent
CL

How it works:

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

- A SaaS visibility management platform. This is where users can configure visibility and define filtering. It is accessible from anywhere and always available.

- Sensors and connectors: software that sits within the source and tool instances respectively. The sensors and connectors are how CloudLens has full access to rich metadata because they sit within instances. They can be Docker-container or Agent based versions, and they all communicate over a secure VPN tunnel.

Using CloudLens is simple – Load sensors within the source and tool instances, create source and tool groups based on their characteristics, draw a visibility path and configure filters. After that, the solution is ready auto-scale.

Since CloudLens has Docker-containers or Agents that sit in a customer's instances, it has access to metadata, which is information about the instances that a cloud service provider provides. From the source instance, they can identify the Cloud Service Provider (AWS, Azure, IBM), Region, Availability Zone, Kernel module, CPU and memory etc. and from the tool instance, they can determine if the tool is an APM, NPM, IDS or SIEM. This metadata is sent from the sensors to the management platform. CloudLens 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 source instance, so only filtered packet data goes to the tools. No packet data is ever sent to the management portal.

Also, because CloudLens SaaS uses metadata, when a new instance appears or disappears, the platform automatically knows where it belongs based on group criteria. Consequently, the correct security and monitoring policies will 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. The sensors also have built-in load balancing and recognize immediately if a monitoring tool is taken out of service. This 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 any-cloud service provider (AWS, Azure, IBM etc.) to any-cloud (public, private or hybrid)

The sensors and connectors also work in private cloud environments and data centers, allowing seamless visibility integration across public cloud and virtualized private environments.

Applications can be containerized and deployed as micro-services within a host or across multiple hosts within a Kubernetes cluster. This communication between containers within a host never leaves the host and is not available outside the host. Since CloudLens uses Docker containers to deploy its sensors within Linux platforms, it is capable of delivering visibility into communication going on between containers operating within a host. The same level of visiblity can be extended to containers operating in Pods within a Kubernetes cluster. CloudLens sensors operate as a side-car container deployed within a Pod. Any communication to or from the Pod can be monitored by CloudLens sensors, and the data can be delivered to tools that require data for further analysis.

Finally, Ixia further simplifies use with its growing Cloud Visibility Ecosystem – technology partners who have pre-validated CloudLens, so the connector 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.

Key features:

Cloud-native serverless architecture

Elastic scale, on-demand

- 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
- Pay for only what you use

Cloud service provider agnostic

- Capable of using metadata from any cloud service provider platform to provide visibility

Does not require architectural changes

- SaaS implementation means Ixia does the heavy lifting behind the scenes. So, you don't have to change anything.

Supports Container & Kubernetes visibility

Docker Container / AGENT-Based Component

Inherent security

- Uses a secure visibility path to transfer filtered packets. It is an encrypted overlay tunnel via a peer-to-peer VPN tunnel
- 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

Works in private cloud & data center

- Easy installation of Docker-based component or Windows agent in public, hybrid, or private environments for seamless visibility

Filter at the source

- Eliminates single point of failure: filters and load-balances 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 operate optimally

Metadata Access

- 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

- Simple setup process that takes minutes not hours.

Reduce Error

- No CLI, mapping or per-instance configuration. Just drag-and-drop.

Cloud Visibility Ecosystem

Easy setup & management

- One less step in the setup process.

Reduce Error

- Leading security, monitoring and performance tools, pre-configured to work with CloudLens.

Specifications

Browsers	Chrome & Firefox
Operating Systems	• Linux OS: Amazon AMI, CentOS 7, Ubuntu, RHEL ∘ All Linux AMI are tested on x86_64 architect ∘ Host Linux kernel must be version 3.1 or higher • Windows OS ∘ All 64-bit Windows OS
Cloud Service Provider platforms	• Amazon Web Services (AWS) • Microsoft Azure • Google Cloud Platform • IBM Bluemix • Alibaba Cloud • Century Link Cloud • Other – CloudLens can support any cloud, contact us to learn more
Container-orchestration	• Amazon Elastic Container Services for Kubernetes (EKS) • Google Kubernetes Engine (GKE) • Azure Kubernetes Service (AKS)

Learn more at: www.keysight.com

For more information on Keysight Technologies' products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus