WHITE PAPER

Achieve Network Visibility in the Public Cloud

Introduction

Organizations in every market sector, even those not typically associated with technology, are migrating workloads to the public cloud. This trend is growing because of the increased flexibility and agility the cloud offers. Whether cloud workloads represent web services or business-critical applications, they must execute with the same level of performance, security, and compliance as in traditional data centers.

Challenges

In the data center, network engineers make copies of packets that pass through their physical network devices and forward them to monitoring tools for inspection and analysis. When an organization moves workloads from the data center to the public cloud, the IT team no longer has physical access to the infrastructure. However, the need to monitor packets remains —to identify active threats, monitor network performance, and diagnose application issues. How do the teams responsible for security and network operations get visibility to the data they need?

KEYSIGHT TECHNOLOGIES

Characteristics of Cloud Services

To understand these challenges within the context of a cloud environment, let us take a step back to see why organizations opt to move to the cloud.

There are several advantages:

1. **Flexibility and agility** – In the cloud, end users get the resources they need without the delays and limitations that characterize internal IT requests. Users can request new computing resources with specific configurations from anywhere in the world and providers deliver the requested services according to preset service level agreements (SLAs).
2. **Elasticity and scale** – Cloud-based resources are deployable on-demand and quickly deactivate when the resource is no longer required. Users pay only for the resources utilized. Cloud providers leverage the scale of their operations to offer competitive prices to end users.

The advantages of the cloud come at the cost of not having the same level of access and control. A significant challenge preventing many companies from moving critical workloads to the cloud is the absence of independent application-level monitoring and analysis of workload behavior.

Also, the services offered by cloud providers for security and performance monitoring may not include access to packet data. This data is a requirement for most security and performance monitoring. Cloud providers move workloads as needed to maximize the use of their infrastructure and often cannot isolate a specific client's packets within their network.

Visibility Challenges

There are three main challenges to enabling visibility to monitor public cloud infrastructure:

1. **Capturing and filtering traffic** – In a traditional data center, there is physical access to the network. The operations team can deploy network taps and packet brokers to have full access and control over packet monitoring. However, when IT chooses public cloud infrastructure, they can no longer use physical packet capture technology.
2. **Ensuring immediate visibility to every new cloud** – Cloud services scale on-demand, letting users create new instances and destroy old data dynamically. A cloud-specific visibility solution needs to similarly scale on-demand with zero delay for new infrastructure deployment. Retrofitted cloud visibility solutions with a single, monolithic collection point do not scale easily. This is because as traffic volume grows, at some point the collection point will require an upgrade and some level of human intervention.

3. **Providing consistent delivery of cloud data to monitoring tools** – Cloud visibility solutions with a monolithic design are less secure because they have a single point of failure. If the central collection point goes offline for any reason, traffic will stop flowing to monitoring tools. This can result in lost packets and blind spots in network visibility.

Solution: Cloud-Native Visibility

The solution to address these challenges is a cloud-native visibility platform that operates completely in the cloud and requires no physical infrastructure. Ixia is the only network visibility provider to offer a cloud-native solution. Enterprises can deploy Ixia CloudLens either as a service in the cloud or as a self-hosted private cloud solution. At its core, CloudLens is a containerized microservice that provides users with access to the packets processed in their clouds (Figure 1). CloudLens is a serverless design that enables unlimited scalability. The architecture has two major components.

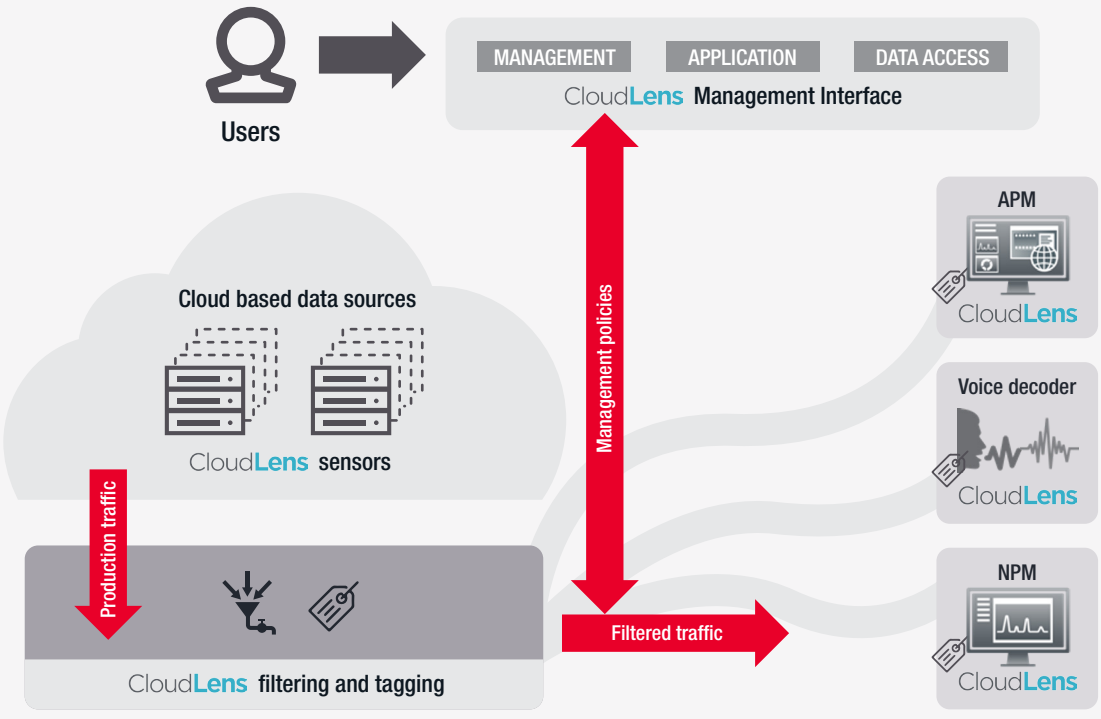

Figure 1. Cloud based management interface controls data access, filtering, and delivery

1. Source and Tool Sensors

You install CloudLens visibility sensors as Docker containers on both your data sources (which require monitoring) and tool instances (which analyze the data). Container technology allows the sensors to access packet traffic flowing through your cloud instances, filter the traffic, and forward it as metadata to the CloudLens central management platform.

Gathering traffic

- Data gathering in the cloud is possible because packets from the source machines are accessible directly at the OS layer.
- Data gathering is secure because the sensors inherit the existing security context of the packet, preventing cross-tenant security violations.
- Blind spots due to passive SSL-encryption disappear because the sensors operate directly on your data sources, which run behind the SSL-encryption services.

Filtering traffic

- Security and performance monitoring tools work more efficiently when you only send them the traffic that is relevant to their function. Preset filters streamline the flow of traffic to your tools, relieve tool congestion, and help you make the most of your tool capacity.
- The sensor has access to instance-level metadata, which gives administrators a broader set of options for creating filtering rules. For example, filtering decisions could include OS, instance metadata, or even metrics, like CPU and memory load. Filtered traffic can be sent directly to your data center or cloud-based security and performance monitoring tools.

Scaling to match cloud elasticity

- Visibility sensors scale dynamically along with the source instances based on application needs.

2. Centralized Management Interface

CloudLens users manage the sensors installed in the data source and tools instances from a centralized management interface that runs in the cloud and is remotely accessible. CloudLens takes a comprehensive approach to managing cloud visibility.

Configuring visibility

- Users set up cloud visibility by logging into the management portal and creating a “project” that automatically creates a unique “project key.” The key is available within the visibility sensors running in the source and tool instances.
- The sensors send metadata about each cloud instance to the central management platform. Examples of cloud instance metadata include:
  - underlying architecture
  - operating system

- hypervisor type
- kernel version or other software version
- prepopulated user data
- CPU and memory utilization and performance metrics

Creating source data and tool groups

- The management interface allows users to create source groups and tool groups based on metadata. The process enables easier management of similar instances by applying policies across a group (Figure 2).
- The metadata can be auto-populated or user-defined.
- New instances automatically join groups based on their metadata. This process ensures the visibility platform retains scalability and elasticity. For example, a user can create a tag group of all instances as “Web Server.” Every instance with that tag automatically adds to this management group, regardless of the creation date.

Creating an encrypted data delivery path

- The next step is for users to associate source data groups with tool groups to create an encrypted secure visibility path. In CloudLens, this is done using a point-and-click visual interface.
- Once defined, the secure visibility path automatically transfers filtered packet data from the data source to tool instances.

Working together, the source and tool sensors, the centralized management platform, and the secure visibility path address the challenge of providing visibility within the public cloud.

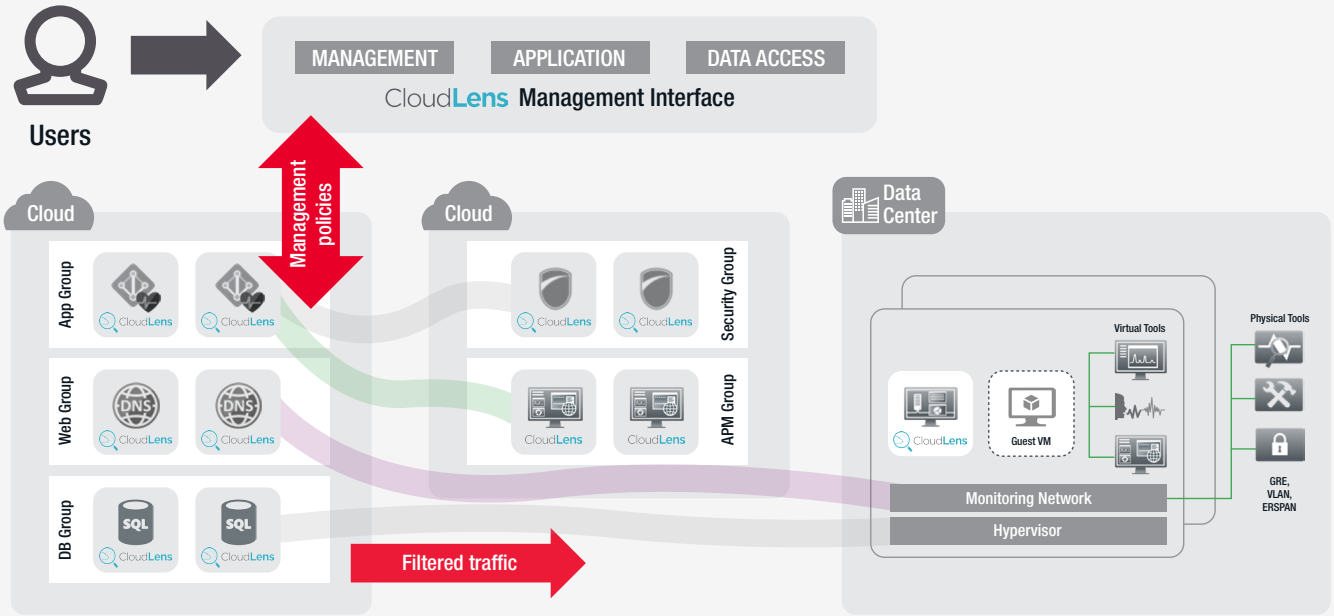

Figure 2. Filtering and delivery policies can be applied to predefined groups

Cloud Agnostic Visibility

Ixia's cloud visibility solution is platform-agnostic to minimize complexity. Whether you are using public clouds from different vendors or operating private clouds on different hypervisor platforms, CloudLens lets you access all the packet data you that flows through your clouds.

Conclusion

As enterprises move key workloads to shared cloud infrastructure, they must have access to cloud traffic to maintain network security and optimize performance. In the cloud, the filtering rules you use to select packets for monitoring must be dynamically applied as clouds instances appear and disappear. Ixia CloudLens has a serverless architecture with a cloud based management interface to ensure the right traffic gets to the right tool continuously. This design delivers intelligent, resilient, and proactive public cloud visibility.

Learn how you can eliminate the visibility of blind spots of your public cloud environment and access the data you need at www.ixiacom.com/solutions/cloud.

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

KEYSIGHT TECHNOLOGIES