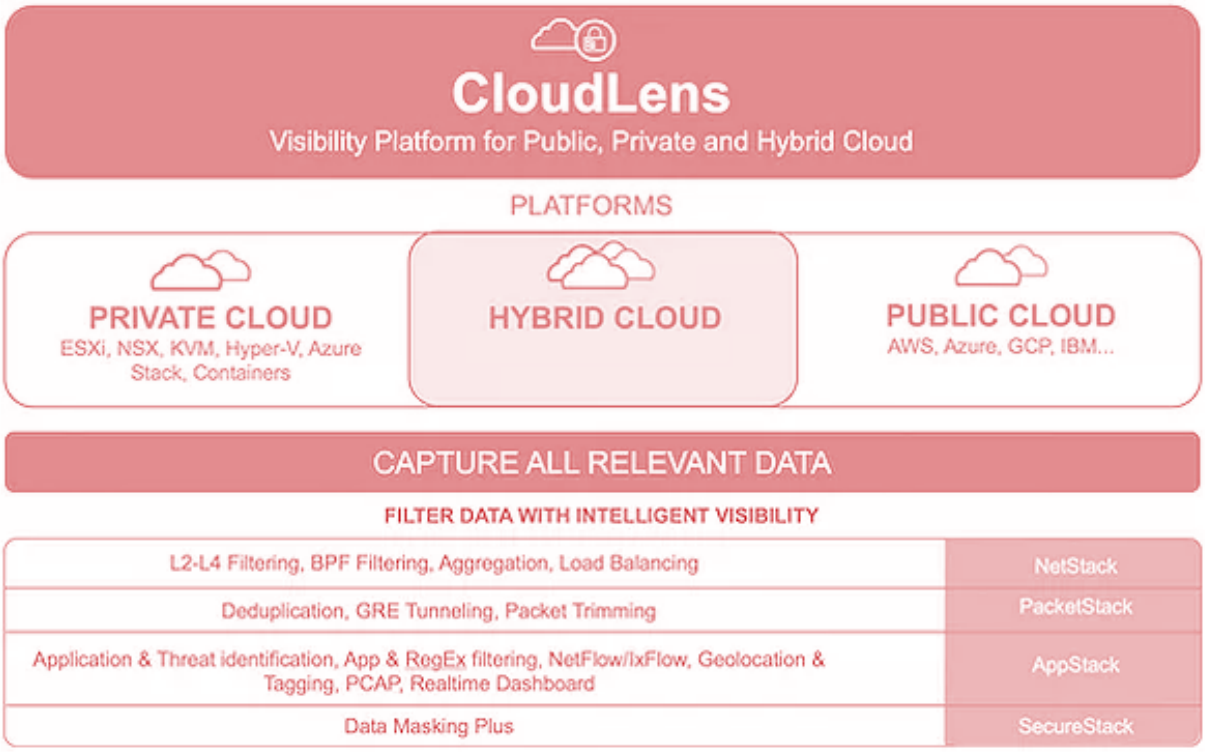
CloudLens

Public, Private, Hybrid Cloud Visibility

Enabling Visibility to Secure and Monitor 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.



KEYSIGHT

Highlights

- Capture and forward Full Packets and/or Netflow from Virtual Machine (VM), containers or inter-Pod network traffic and forward it to tools, or physical and/or virtual packet brokers for aggregation, advanced filtering, and deduplication
- Virtual packet processing and aggregation in your cloud which traditionally relies on physical packet brokers
- Aggregate and deduplicate packet data; originate and terminate tunnels without the need for physical hardware
- Virtual packet processing with AppStack capabilities leverages Keysight's advanced application intelligence with signature-based application detection, geolocation, NetFlow and IxFlow (enhanced NetFlow)
- Management UI that can be deployed in any cloud, for better control and security
- Multi-platform capable, cloud service provider and platform agnostic
- Auto-scales elastically, on-demand with cloud instances
- Handles cloud scale (thousands of instances). Auto-scales elastically, on-demand with cloud instances
- Easy-to-use, drag-and-drop interface with a network to tools layout

The Cloud Visibility Challenge

All networks are inevitably exposed to increasingly complex and advanced security risks and threats. The key is to identify the risks and threats as quickly as possible and take effective action. The goal of a total visibility architecture is to give you access to all the data that crosses your networks, so you can.

There are two main aspects to every network visibility solution:

1. Capturing all network traffic, and

Aggregating, filtering, de-duplicating and modifying the collected network traffic prior to it being forwarded to performance, monitoring and security tools

For collecting the network traffic, traditionally the best method to capture all traffic on a network link is by using a network tap. Taps provide continuous, non-disruptive network access and have these characteristics:

- Receive all traffic on a network link
- Require little to no configuration and can be installed at any time
- Are not IP addressable so they aren't vulnerable to remote attacker access
- Do not introduce delay or alter the content of the data

For aggregating, filtering, de-duplicating and modifying network traffic the traditional approach is a physical network packet broker (NPB). NPBs are used to process packets and send select packets to specific tools, based on what they are designed to monitor and inspect. NPBs aggregate raw or filtered traffic from multiple monitoring points across your network and filter and de-duplicate packets so your tools receive only relevant traffic. This reduces data congestion, minimizes false positives, and allows you to handle traffic with fewer monitoring devices.

However, in today's virtualized deployments, both aspects are a challenge:

1. Collecting virtualized network traffic, between virtual workloads or east-west (inter-VM or inter-container/Pod), where a traditional physical tap has no visibility.
2. Ensuring that the visibility solution scales with the dynamic nature of the private and public cloud. If virtualized network traffic must be processed by a physical network packet broker, then manual intervention is required to add new resources, and complexities increase.

CloudLens addresses both problems with two main components, a virtual tapping (vTap) capability which gathers, filters and forwards virtual workload traffic, and a virtual packet processing capability which aggregates, filters, deduplicates and forwards traffic to both virtual and physical datacenter tools. Additionally, CloudLens offers the ability to dynamically detect specific applications, and threats, not just application types or categories, filtering and forwarding real-time network traffic to appropriate tools for further security, performance, or forensic analysis.

The CloudLens Solution

Keysight CloudLens™ provides a complete cloud-based visibility solution for virtual network traffic. With CloudLens you can mirror data, filter and forward traffic between virtual machines, containers or Kubernetes Pods, and tools. It includes two core capabilities. First, an ability to virtually tap (vTap) or capture, filter and forward a copy of network traffic directly to either tools or a network packet broker. Second, it can operate as a virtualized network packet broker, allowing aggregation, filtering, deduplication of virtual network traffic all within the cloud.

CloudLens vTap

CloudLens provides a vTap service which monitors all inter-virtual workload traffic and forward packets to any endpoint of choice, whether virtual or physical security, monitoring or analytics tools, as well as physical network packet brokers, to achieve full visibility and verification across networks.

Capture virtual traffic

Remove visibility blind spots by providing total visibility into all inter-VM and/or inter-Pod traffic, capturing and forwarding traffic of interest to physical or virtual packet brokers, or directly to monitoring tools.

- Enables complete visibility of east-west, inter-VM, inter-Pod traffic through virtual tapping, filtering and traffic forwarding
- Offers a solution with full access to network packets passing between VMs on hypervisor stacks
- Sends traffic to any existing endpoint, physical or virtual (tool agnostic)
- Follows VMs for continuous visibility throughout migration (VM-level monitoring)
- Supports vMotion and DRS
  - Meets SLAs and compliance requirements (SOX, PCI, HIPAA)
- Enables proactive monitoring and security of virtual data centers

Tap filtering

Integrated filtering reduces vSwitch, vNet, VPC and LAN bandwidth consumption by filtering at the vTap point (source), providing a multi-layer L2-L4 filtering engine allowing for filtering based on IP address, subnet, protocols, port numbers, and/or individual workloads.

CloudLens vTap – Hypervisor based environments

Monitoring east-west traffic in a type 2 hypervisor environment (VMware ESXi, Microsoft Hyper-V, KVM) is usually done at the virtual switch level. In such environments, the administrator has the right permissions to deploy vTaps in the hosts to monitor, and to leverage vSwitch mirroring capabilities to get a copy of the network traffic.

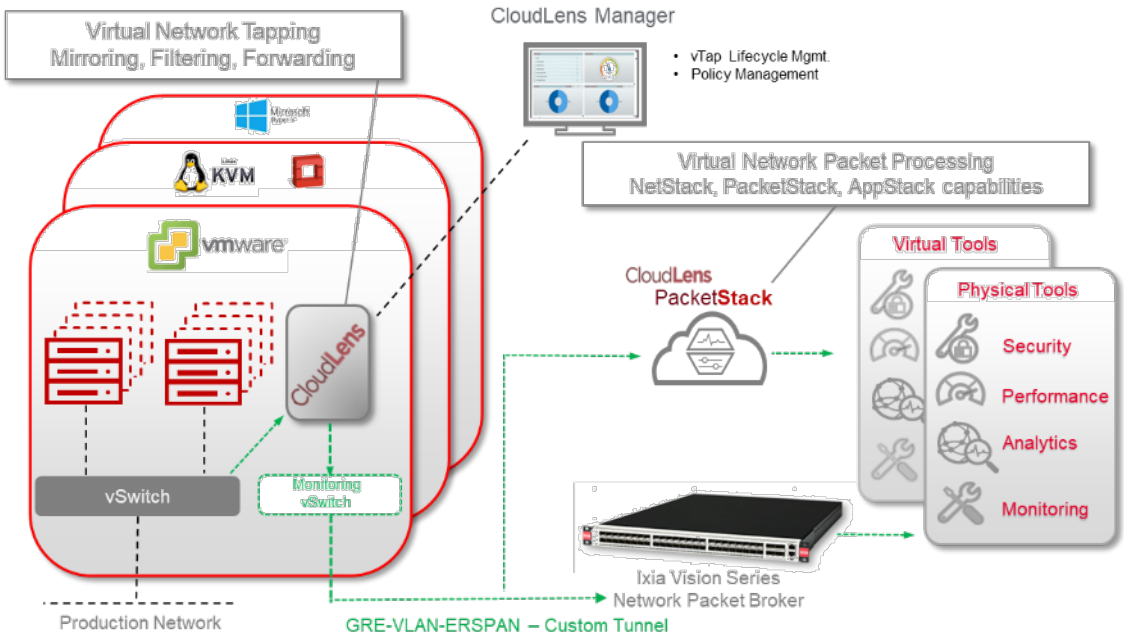


Figure 1. Private cloud network vTAP

CloudLens vTap – Sensor based deployments

For virtual environments where the administrator does not have access to the underlying hypervisor and virtual switches, like AWS, Azure, GCP and others, Keysight has introduced a virtual tap in the form of a Sensor, available for Windows and Linux.

This implementation, where the CloudLens Sensor vTap runs in the workload to monitor, offers a hypervisor agnostic solution.

The management of the sensors is done via CloudLens Manager, which can run in practically any virtual or containerized environment and can be deployed in security tight environments.

The CloudLens Sensors vTap can be used in containerized environments (i.e. Kubernetes), when there is a need to monitorinter-Pod traffic. The Sensors are then installed as a “sidecar” in the Kubernetes container Pods

The virtual tap ecosystem includes the following components:

- CloudLens Manager, deployed as a virtual appliance or within a Kubernetes Cluster, provides capture and filter management, and monitoring.
- CloudLens Sensor vTaps, installed in the virtual workloads to monitor traffic, within AWS, Azure, GCP for example, are the sources of the traffic to mirror. The sensors BPF filtering options and forward the tapped traffic via GRE, VxLAN or Encrypted tunnel to aggregation points. The sensors can send traffic over any interface available in the virtual workload.

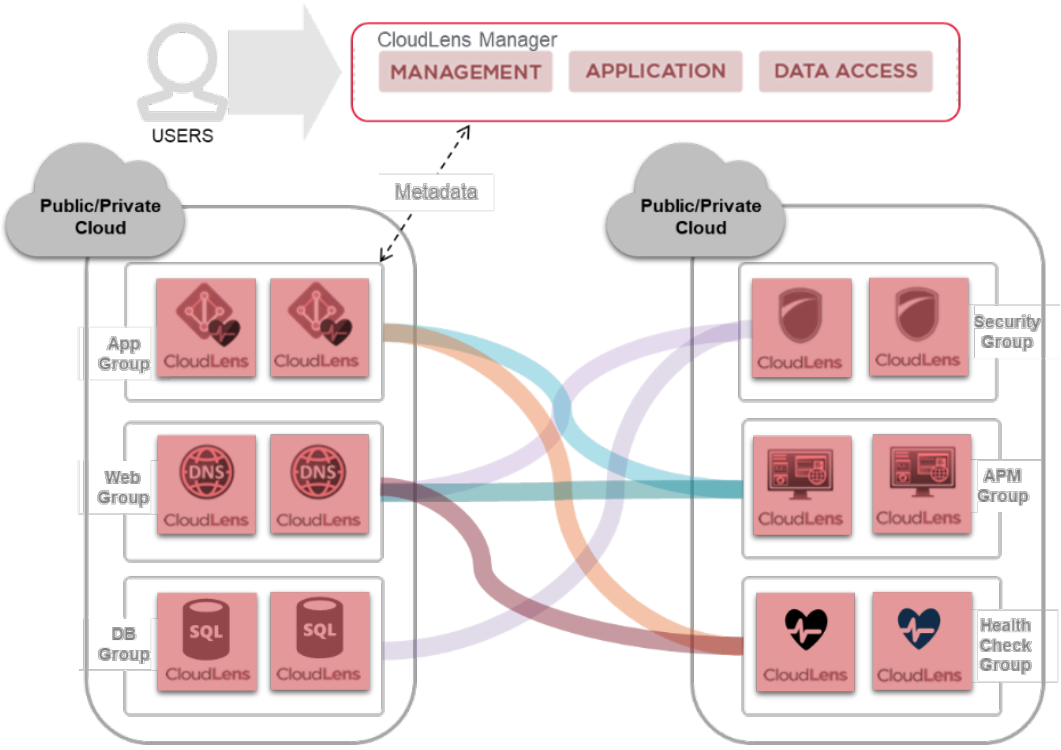


Figure 2. Sensor vTap at the application level

CloudLens vTap for VMware NSX

Keysight CloudLens is a VMware certified solution that offers a specific integration of its CloudLens vTap to virtually tap NSX for vSphere and NSX Data Center (NSX-T) environments.

In NSX Data Center CloudLens leverages NSX service chain mechanism to insert the CloudLens as a network introspection service, the service then integrates with NSX Security Groups and Policies to become part of the NSX architecture. To simplify the administrator's tasks, the deployment lifecycle is managed from the NSX Manager. The network administrator can choose between deploying CloudLens virtual taps service virtual machine (SVM), per host or per cluster of hosts.

The "Copy Packet" feature mirrors the East-West traffic of select VMs to CloudLens vTap (traffic capture is based on NSX Security Groups and Policies).

The CloudLens service provides L2-L4 filtering capabilities and can also generate metadata in the form of NetFlow (V9 and V10). The mirrored traffic can either be forwarded directly to a monitoring tool or sent to an aggregator/network packet broker (NPB – virtual or physical) for additional processing. Such integration allows VMware NSX to benefit from the Keysight global visibility solution, and its advanced packet processing and application identification and filtering capabilities (replication, deduplication, application identification and filtering)

CloudLens vTap Specifications

The following table summarizes the specifications for vTap v5.5 and vTap v6.2.1

Network vTap specifications – v 5.5			
VMware	ESXi 5.0 & 5.1	ESXi 5.5	ESXi 6.0 – 7.0
ESXi - vDS	YES	YES1	YES1
ESXi - vSS	NO	YES1	YES1
NSX for vSphere	v6.3-6.4		
NSX Data Center (NSX-T)	v2.5-3.x		
Microsoft Hyper-V	Windows Server 2012-2019		
KVM	v.2.01 and above with Open vSwitch (OVS with or without DPDK) 2.5 and above		
OpenStack KVM	Mitaka and newer (Keystone v3) with KVM OVS (see above)		
Network Connectivity	Management Server VM must be accessible via HTTP/HTTPS to access Web UI (Please refer to the User Guide for specific platform information)		
Disk Storage	Manager: 4 GB - vTap Service (SVM): 2-4GB – NSX: Refer to User Guide		
CPU	Manager: 2 vCPU - vTap Service (SVM): 1-2v CPU, NSX: Refer to User Guide		
Memory	Manager: 8GB (recommended) – vTap Service (SVM): 512MB to 3GB (Hyper-V), 3GB (ESXi) - KVM (integrated with OVS, no additional resource), NSX: Refer to User Guide		
Web Browser	Google Chrome, Internet Explorer, and Firefox		
Sensor vTap specifications – v 6.2.1			
Sensor vTap	Deployed on customer workloads (VMs or Kubernetes cluster). Requires containerd for deployment (typically Docker or Kubernetes but can work with others).		
CloudLens Sensors	Windows 10, Windows Server 2012-2019, Most Linux based OS with Docker		
Sensor-based SVM	Nutanix AHV 5.0+		
Network Connectivity	Management Server VM must be accessible via HTTP/HTTPS to access Web UI (Please refer to the User Guide for specific platform information)		
Disk Storage	Manager: 100 GB – Sensor vTap 1 GB		
CPU	Manager: 4 vCPU – Sensor vTap 1 vCPU		
Memory	Manager: 16 GB – Sensor vTap 256 MB		
Web Browser	Google Chrome, Internet Explorer, and Firefox		

CloudLens vPacketStack (vPB)

In addition to tapping capabilities, CloudLens supports packet processing within a private or public cloud environment allowing virtual network traffic aggregation, filtering, deduplication, NetFlow generation, and access to Keysight's application intelligence capabilities without the need of a physical packet broker.

Keysight's CloudLens virtual packet processing is delivered through a dedicated virtual machine and is an intermediate component in the virtual visibility architecture that "sits" between vTap points and performance and monitoring tools to which can do the following:

- Terminate/Strip GRE, VxLAN, Geneve and VLAN
- Aggregate network packets
- Re-Assemble network packets
- Filter and deduplicate traffic
- Duplicate and forward traffic
- Load-Balancing

Such processing traditionally required a physical network packet broker appliance. With CloudLens, these features are available in a cloud format, offering flexibility and simple deployment in dynamic virtual environments.

There are multiple virtual packet processing options available, CloudLens Virtual Packet Processing Standard or Advanced which offers packet manipulation capabilities like header stripping and packet trimming, or CloudLens with AppStack which offers Keysight's best-of-class application and geolocation filtering, NetFlow and IxFlow generation, and data masking (see CloudLens feature table below for more details).

Note: CloudLens Virtual Packet Processing resides in a separate instance than CloudLens Virtual Packet Processing with AppStack.

Aggregation, replication, deduplication and filtering with virtual packet processing

Aggregating, replicating, filtering and deduplication of data within the private or public cloud allows more effective and efficient use of network bandwidth. Traditionally, all virtual visibility network traffic would be required to leave the private or public cloud to be aggregated and sanitized before forwarded to monitoring tools. With CloudLens™, aggregation can occur in the private or public cloud where it can then be further deduplicated and filtered, allowing much more efficient use of both virtual and physical network capacity.

Load balancing

CloudLens vPB can be deployed as an packet brokering (or processing) VM that can load balance select traffic from the virtual network to virtual tools such as virtual WAN optimization appliances. It operates much like a physical network packet broker. It forwards any workload not selected for optimization, thus bypassing the WAN optimization systems. It forwards the rest of the workload to optimization tools. After optimization, the traffic is sent back to the packet processing VM, which forwards it on the original path.

CloudLens vAppStack (vATIP)

Keysight's CloudLens™ with AppStack includes Application Intelligence Processing for virtual environments and includes patent-pending capabilities to allow user point-and-click selection of applications, application groups as well as capabilities to dynamically detect new and even unknown applications. It also provides granular application behavior, user geo-location, mobile device identifier,and browser information.

Gathering virtual network traffic data

Private cloud implementations can leverage CloudLens™ packet processing with AppStack for analysis of the virtual traffic sent from CloudLens™ tapping capabilities.

Application filtering

CloudLens vAppStack can match hundreds of application signatures to identify applications individually. This also means that application types, segments/groupings e.g., Netflix and Hulu, Microsoft Outlook and Hotmail, Facebook or Snapchat, SAP and Oracle, can be determined. Once an app is matched, CloudLens applies filters and rules to this traffic to provide IT organizations the ability to dramatically improve the efficiency of their downstream tools. For example, because there is little value in forwarding media streaming traffic to intrusion detection systems (IDS) systems, AppStack capabilities allow an organization to curtail this application traffic from flowing to specific monitors and network appliances – reducing bandwidth to these tools.

Keysight's AppStack detects applications by matching signatures: static, dynamic or even customized with a patent pending technology. With Keysight doing the heavy lifting of figuring out application signatures and maintaining a database, you or your team don't have to become RegEx experts or track changing applications.

Keysight regularly updates its application database, tracks leading and new applications, as well as manually analyzing unknown applications to develop signatures applications where it's unpublished.

As part of the application signature identification function, AppStack features allow you to identify and flag unknown applications. Rules and filters can then be applied for that traffic to be evaluated for further action. This capability further enhances your security infrastructure, and could indicate the presence of malware, unwanted transmissions, or even hijacked data.

The CloudLens™ Packet Processing with AppStack Dashboard features easy to use graphical displays and offers an overview of the network traffic map. The administrator can quickly see where the traffic is coming from, what are the most active applications, and countries in a certain period of time. Which operating systems, and devices are active on the network.

While the Dashboard provides extremely useful information on one screen, CloudLens™ is built toprovide third party applications (IPS, IDS, Netflow collectors) the right information at the right time.

The application dashboard shows the following fields:

1. **Traffic**: Real-time traffic volume
2. **App Distribution**: Per-application bandwidth
3. **Top Threats information**: A summary of the number of threats present on the network,sorted by threat category (malware, phishing, hijacked IP, botnet, IoT exploits)
4. **Latest Dynamic Apps**: Most recently dynamically discovered applications and thegenerated traffic, in bytes and sessions.
5. **Top Countries**: Countries that generated the largest amount of traffic
6. **World**: A world view, with countries that originate traffic shown highlighted.
7. **Top Devices by OS**: Aggregated per-OS traffic, by bytes and sessions, for the last hour.
8. **Top Filters**: Aggregated per-filter traffic for the last 24 hours.
9. **Top Apps**: Aggregated per-application traffic, by used bandwidth, bytes, and sessions.
10. **Top Browsers**: Per-browser traffic percentage for the last hour.

NetFlow / IxFlow generation

To expose hidden attacks, CloudLens™ with Appstack capabilities can generate metadata which can be exported as enhanced NetFlow. Additionally, it allows you to enrich NetFlow records with more that one hundred value-add extensions. You can determine what additional information to send to your tools.

- Include geographical information such as region IP, latitude and city name. Application IDor name, device, and even browser type as part of extra information sent to tools.
- Subscriber-aware reporting provides detail on application and handset (device) type for mobile users
- HTTP URL and hostname for web activity tracking
- HTTP and DNS metadata for rapid breach detection
- Transaction Latency for application performance tracking
- Threat Information
- TLS/SSL information

Geo-location and tagging

Separate traffic by location – pre-defined parameters and signature detection allows for application filtering based on geography so tools can zoom in for close-range visibility. Quickly troubleshoot application issues for a specific remote site by pinpointing a location and application (like VoIP problems from your UK office). If you want to block traffic from specific locations, use Keysight's ATI Research Center to let you block all traffic to and from untrusted countries, dramatically reducing your attack surface.

- Forward application session traffic based on region, country, city, and in many cases latitude/longitude to the correct tools in your portfolio
- Quickly configure filters, no manual scripting needed
- Support custom locations, such as private IP addresses

Data masking plus for credit card and social security numbers

Achieve Payment Card Industry Data Security Standard (PCI-DSS), HIPAA and other regulatory compliance by leveraging pre-defined data patterns. With personally identifiable information traversing the network, security is key to keeping your consumers and your organization safe.

- Pre-defined patterns to mask – including major credit card, SSN and email addresses
- Reduce false positives with the built-in credit card number validation using the Luhn algorithm
- Leverage in addition to standard data masking at the packet level using a user configurable offset with any number of bytes.

CloudLens Product Requirements

CloudLens vTAP requirements – v6.2.1	
Supported Environments	AWS, Azure, GCP, VMware, KVM, OpenStack, Nutanix, Kubernetes
CPU	4 vCPUs
Disk Storage	100 GB
Memory	16 GB
Network Connectivity	1 interface
Licenses	SUB-CL-STD, SUB-CL-ENT, SUB-CL-LEN, SUB-CL-ADD-50, SUB-CL-STD2ENT
CloudLens vTap requirements – v5.5	
Supported Environments	VMware vDS/vSS, VMware NSX/NSX-T, OpenStack, KVM, Hyper-V
CPU	2 vCPUs
Disk Storage	20 GB
Memory	8 GB
Network Connectivity	1 interface
Licenses	LIC-CL-VTAP-10 LIC-CL-VTAP-50 LIC-CL-VTAP-100 LIC-CL-VTAP-250 LIC-CL-VTAP-1000 LIC-CL-VTAP-NSX
CloudLens vPacketStack (vPB) requirements – v2.3	
Supported Environments	VMware, OpenStack, KVM (see User Guide for more details)
CPU	4 vCPU - Haswell or later processor
Disk Storage	8 GB
Memory	16 GB
Network Connectivity	6 predefined interfaces (customizable after installation)
Licenses	LIC-CL-VPP-STD-1 SUB-CL-VPP-STD-1 LIC-CL-VPP-AD-1 SUB-CL-VPP-AD-1
CloudLens vAppStack (vATIP) – v4.3	
Supported Environments	VMware, OpenStack, KVM (see User Guide for more details)
CPU	6 vCPUs - Westmere or later processor
Disk Storage	30 GB
Memory	16 GB
Network Connectivity	3 interfaces
Licenses	SUB-CL-AS-1-F, LIC-CL-AS-1-F

CloudLens Product Features

	vTap (v6.2.1)	vTap (v5.5)	vPacketStack (v2.3 standard)	vPacketStack (v2.3 Advanced)	vAppStack (vATIP v4.3)
# Virtual Network Interfaces supported	Not Applicable	Not Applicable	2	6	8
Max # of filtering rules	Unlimited	Unlimited	20	2000	100
L2-L3 filtering	Yes (BPF)	Yes	Yes	Yes	Yes
(Eth type, VLAN, IP)					(IP)
L2-L4 filtering	Yes (BPF)	Yes	-	Yes	Yes
(Eth type, VLAN, IP, Ports, IP protocol)					(IP, IP Protocol)
Mirroring/forwarding	Yes	Yes	-	-	-
Aggregation	-	-	Yes	Yes	Yes
Replication	-	-	Yes	Yes	Yes
					(1 GRE Tunnel)
Load balancing	-	-	-	Yes	-
Deduplication	-	-	-	Yes	Yes
Header stripping	-	-	-	Yes	Yes
				MPLS, FabricPath, VXLAN, PPPoE, GRE, ERSPAN, GTP, Geneve	GRE & ERSPAN
Packet trimming	-	-	-	Yes	-
Data masking	-	-	-	-	Yes
Tunnel origination	Yes (GRE, ERSPAN, VLAN, VxLAN, Encrypted)	Yes (GRE, ERSPAN, VLAN, VxLAN)	Yes (GRE, ERSPAN, VxLAN)	Yes (GRE, ERSPAN, VxLAN)	Yes (GRE only)
Tunnel termination	-	-	Yes (GRE, ERSPAN, VxLAN)	Yes (GRE, Geneve, ERSPAN, VxLAN)	Yes (GRE only)
GRE, ERSPAN, VxLAN, ZT					
Application filtering	-	-	-	-	Yes
Real-Time application dashboard	-	-	-	-	Yes
Data masking plus	-	-	-	-	Yes
Geo-location and tagging	-	-	-	-	Yes
NetFlow	Yes	Yes (NSX)	-	-	Yes
IxFlow (enhanced NetFlow)	-	-	-	-	Yes
Available part numbers (see ordering section for more details)	See “Licenses” in specification table and ordering	See “Licenses” in specification table and ordering	LIC-CL-VPP-STD-1 SUB-CL-VPP-STD-1	LIC-CL-VPP-AD-1 SUB-CL-VPP-AD-1	LIC-CL-AS-1-F SUB-CL-AS-1-F

CloudLens Product Licensing

Product	License	Description
vTap v6.0+	SUB-CL-STD	Ixia CloudLens Standard Edition one (1) year subscription, package includes 50 credits. This SKU is only valid for CloudLens 6.0 and above. Standard Support included.
vTap v6.0+	SUB-CL-ENT	Ixia CloudLens Enterprise Edition one (1) year subscription includes 150 credits. This SKU is for CloudLens 6.0 and above. Standard support included.
vTap v6.0+	SUB-CL-LEN	Ixia CloudLens Large Enterprise and Reseller/MSP Edition one (1) year subscription, package includes 500 credits. Credits are distributed individually. 1 credit required per active sensor vTap. This SKU is only valid for CloudLens 6.0 and above. Standard support for the purchaser included.
vTap v6.0+	SUB-CL-ADD-50	Ixia CloudLens add-on pack includes 50 credits, valid for (1) one year. Use this SKU to add 50 credits to CloudLens Standard or Enterprise Editions. (Requires license of SUB-CL-ENT, SUB-CL-LEN or SUB-CL-STD)
vTap v6.0+	SUB-CL-STD2ENT	Ixia CloudLens Upgrade from Standard to Enterprise Edition. This license enables the additional features of CloudLens Enterprise Edition and includes 100 additional credits. By adding SUB-CL-STD2ENT to SUB-CL-STD the customer gets the full functionalities of CloudLens Enterprise Edition (SUB-CL-ENT) for the remainder of the term.
vTap v5.5	LIC-CL-VTAP-10	Ixia 10 licenses pack includes 10 CloudLens vTap licenses. - The license applies to the number of installed Service VMs or SVMs (1 license per SVM), 1 license per host for native KVM OVS installations. - There is no additional cost for the CloudLens Manager. - Applies to all VMware ESXi,Microsoft Hyper-V, KVM, OpenStack KVM. Also includes software updates for one (1) year - Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours with best effort response time.
vTap v5.5	LIC-CL-VTAP-50	Ixia 50 licenses pack includes 50 CloudLens vTap licenses. - The license applies to the number of installed Service VMs or SVMs (1 license per SVM), 1 license per host for native KVM OVS installations. - There is no additional cost for the CloudLens Manager. - Applies to all VMware ESXi,Microsoft Hyper-V, KVM, OpenStack KVM. Also includes software updates for one (1) year - Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours with best effort response time.

Product	License	Description
vTap v5.5	LIC-CL-VTAP-100	Ixia 100 licenses pack includes 100 CloudLens vTap licenses. - The license applies to the number of installed Service VMs or SVMs (1 license per SVM), 1 license per host for native KVM OVS installations. - There is no additional cost for the CloudLens Manager. - Applies to all VMware ESXi,Microsoft Hyper-V, KVM, OpenStack KVM. Also includes software updates for one (1) year - Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours with best effort response time.
vTap v5.5	LIC-CL-VTAP-250	Ixia 250 licenses pack includes 250 CloudLens vTap licenses. - The license applies to the number of installed Service VMs or SVMs (1 license per SVM), 1 license per host for native KVM OVS installations. - There is no additional cost for the CloudLens Manager. - Applies to all VMware ESXi,Microsoft Hyper-V, KVM, OpenStack KVM. Also includes software updates for one (1) year - Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours with best effort response time.
vTap v5.5	LIC-CL-VTAP-1000	Ixia 1000 licenses pack includes 1000 CloudLens vTap licenses. - The license applies to the number of installed Service VMs or SVMs (1 license per SVM), 1 license per host for native KVM OVS installations. - There is no additional cost for the CloudLens Manager. - Applies to all VMware ESXi,Microsoft Hyper-V, KVM, OpenStack KVM. Also includes software updates for one (1) year - Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours with best effort response time.
vTap v5.5	LIC-CL-VTAP-NSX	IXIA The Ixia CloudLens vTap Add-on for VMware NSX integration is required to deploy CloudLens vTap on VMware NSX environments. This add-on is valid for one (1) NSX Manager.The add-on includes 3 vTaps (service VMs - SVM) One (1) SVM is required per ESXi host managed by NSX. For additional SVMs, order the CloudLens SVM vTap License packs.
vPB 2.3	LIC-CL-VPP-STD-1	Ixia CloudLens Virtual Packet Processing with PacketStack - Standard, perpetual license, 1 instance. Includes: 2 virtual interfaces, NetStack: L2-3 Filtering (Eth type, VLAN, IP), 20 rules ; PacketStack: Multiple GRE tunnel termination, and origination. Also includes software updates for one (1) year - Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours with best effort response time.
vPB 2.3	SUB-CL-VPP-STD-1	Ixia CloudLens Virtual Packet Processing with PacketStack - Standard, 1 instance. Includes: 2 virtual interfaces NetStack: L2-3 Filtering (Eth type, VLAN, IP), 20 rules PacketStack: Multiple GRE tunnel termination, and origination. Also includes software updates for one (1) year - Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours with best effort response time. Annual license. Can be sold in multi-year increments.

Product	License	Description
vPB 2.3	LIC-CL-VPP-AD-1	Ixia CloudLens Virtual Packet Processing with PacketStack - Advanced, perpetual license, 1 instance. Includes: 6 virtual interfaces- NetStack: Aggregation, Replication - L2-4 filtering (Eth type, VLAN, IP, Ports, IP Protocol), Up to 9999 rules, Load balancing; PacketStack: Deduplication - 12 GRE originating tunnels, Header stripping. Also includes software updates for one (1) year - Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours with best effort response time.
vPB 2.3	SUB-CL-VPP-AD-1	Ixia CloudLens Virtual Packet Processing with PacketStack - Advanced, 1 instance. Includes: 6 virtual interfaces NetStack: Aggregation, Replication - L2-4 filtering (Eth type, VLAN, IP, Ports, IP Protocol), Up to 3000 rules, Load balancing PacketStack: Deduplication - 12 GRE originating tunnels, Header stripping Also includes software updates for one (1) year - Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours with best effort response time. Annual license. Can be sold in multi-year increments.
vAppStack (vATIP)	LIC-CL-AS-1-F	Ixia CloudLens Private virtual packet processing with AppStack. Full Feature pack, 1 instance, perpetual license. Features included: - PacketStack: GRE Termination, Deduplication - AppStack: NetFlow generation - Application Filtering, Geolocation and tagging, Data masking, IxFlow generation. - SecureStack: Threat Insights Also includes software updates for one (1) year - Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours with best effort response time.
vAppStack (vATIP)	SUB-CL-AS-1-F	Ixia CloudLens Private virtual packet processing with AppStack. Full Feature pack, 1 instance. Features included: PacketStack: GRE Termination, Deduplication AppStack: NetFlow generation - Application Filtering, Geolocation and tagging, Data masking, IxFlow generation SecureStack: Threat Insights Also includes software updates for one (1) year - Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours with best effort response time. Annual license. Can be sold in multi-year increments.

For more information

For more insights on how to improve your cloud visibility, check the following links:

CloudLens: Visibility in Public Cloud (White Paper)

Security and Performance Monitoring in Public Cloud (White Paper)

RSA & Keysight: Secure Visibility within your Public Cloud

KEYSIGHT

Keysight enables innovators to push the boundaries of engineering by quickly solving design, emulation, and test challenges to create the best product experiences. Start your innovation journey at www.keysight.com.

This information is subject to change without notice. © Keysight Technologies, 2020 – 2023, Published in USA, June 2, 2023, 3121-1320.EN