CloudLens Self-Hosted

Keysight CloudLens™ Self-Hosted, part of the broader CloudLens platform, provides a complete cloud-based visibility solution for virtual network traffic.



KEYSIGHT

Table of Contents

Overview 3

CloudLens Virtual Tapping (vTap) 7

Capture Virtual Machine Traffic 7

Tap Filtering 7

CloudLens Virtual Taps for Hypervisor Environments 7

CloudLens Virtual Taps for Containerized Environments and Environments with Limited Hypervisor Access 8

CloudLens vTap for VMware NSX 9

CloudLens Self-Hosted Virtual Packet Processing 9

Aggregation, Replication, Deduplication and Filtering with Virtual Packet Processing 10

Load Balancing 10

CloudLens Self-Hosted Virtual Packet Processing with AppStack 10

Gathering Virtual Network Traffic Data 11

Application Filtering 11

NetFlow / IxFlow Generation 13

Geo-Location & Tagging 15

Data Masking Plus for Credit Card and Social Security Numbers 16

Specifications 17

Ordering Information: Virtual Tapping 18

Ordering Information: Packet Processing - Basic 20

Ordering Information: Packet Processing - Advanced 20

Ordering Information: Packet Processing – with AppStack 22

Overview

Enterprises are adopting cloud technologies in order to leverage the flexibility and power advantages of virtualized environments; they are adopting private cloud technology in order to increase control and reduce costs. However, the limited view of virtualized network traffic creates network blind spots for virtual or physical datacenter security, monitoring and analytics tools.

Keysight CloudLens™ Self-Hosted, part of the broader CloudLens platform, provides a complete cloud-based visibility solution for virtual network traffic. With CloudLens Self-Hosted you can mirror data, filter and forward traffic between virtual machines, or Kubernetes container Pods, and data center tools. It includes two core capabilities. First, an ability to virtually tap (vTap) or capture, filter and forward a copy 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 a private cloud.

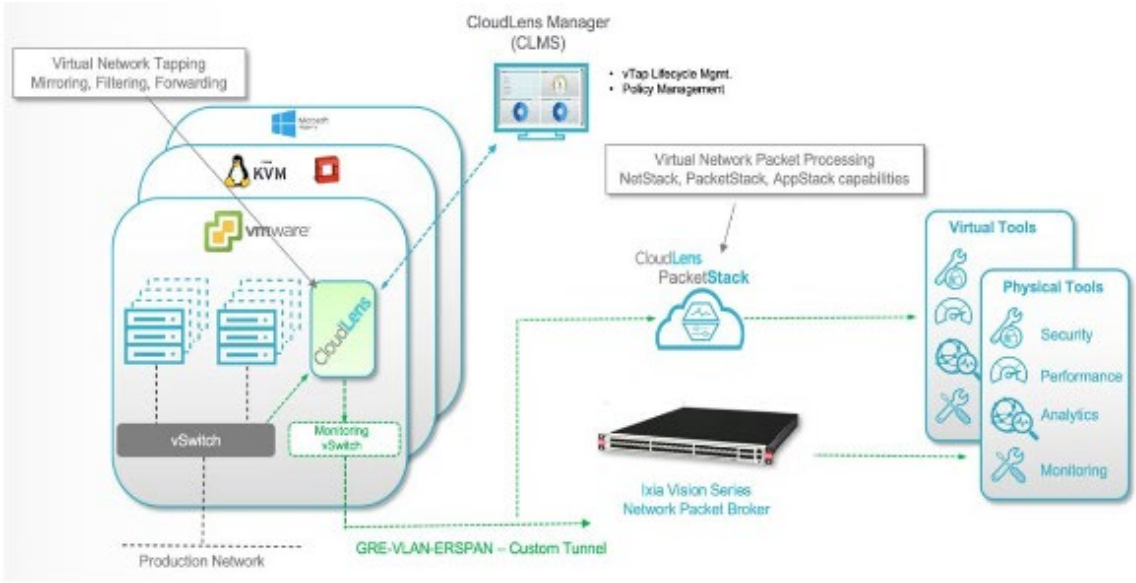


Figure 1. Private Cloud Monitoring – Controlled hypervisor environments

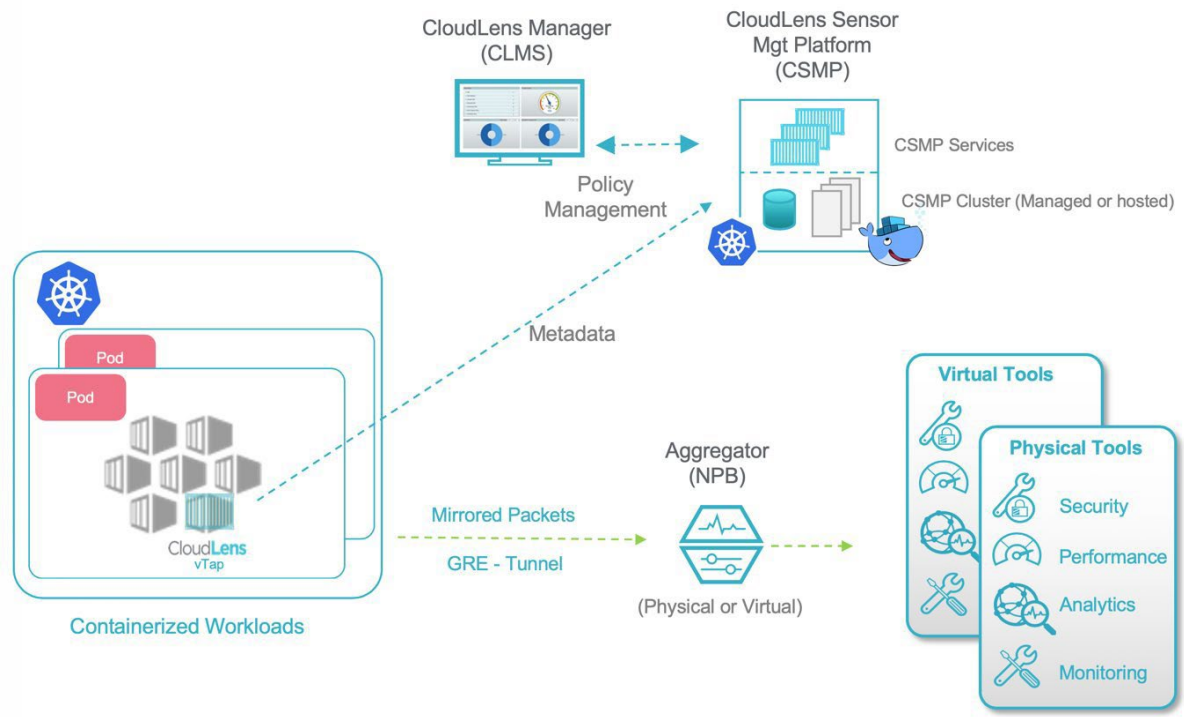


Figure 2. Private Cloud Monitoring – Containerized Workloads or Private Clouds with limited access to hypervisor resources

Product features

Feature	Benefit
Capture VM Traffic (vTap)	Removes blind spots by providing total visibility into all inter-VM traffic. Allows capturing and forwarding traffic of interest to physical or virtual packet brokers, or directly to datacenter monitoring tools.
Cloud Sensor vTap (No hypervisor access required)	Cloud Sensors allows organizations to copy the traffic using Keysight's sensor-based solution from Virtual Machine sitting on any Cloud Platform such as Azure Stack, as well as inter-pod traffic in Kubernetes containerized environments.
Traffic mirroring in SDN environments (NSX, Nutanix)	It enables complete visibility of all traffic incoming and outgoing from a particular virtual workload.
Tap filtering	CloudLens allows optional integrated filtering where data is tapped, which reduces bandwidth consumption. This provides a multi-layer L2-L4 filtering engine that can filter based on IP address, sub-net, protocols, port numbers, and individual VMs
Support for VMware vMotion	Guarantees the integrity of visibility as virtual machines are automatically moved due to the dynamic nature of private cloud resourcing.

Feature	Benefit
Hypervisor Agnostic	Supports the most private cloud hypervisors including VMware ESXi, Microsoft Hyper-V, KVM, and OpenStack KVM. Integrates with VMware NSX for vSphere and NSX Data Center, as well as OpenStack orchestration and management. The use of Cloud Sensors extends monitoring to any Cloud Based environment where vSwitch based monitoring or access is not possible (Microsoft Azure Stack for example) (See Specifications section for details below)
vSwitch Agnostic	CloudLens Self-Hosted is vSwitch agnostic, supporting VMware vSS, vDS, and Open vSwitch (OVS).
Tool Agnostic	(See specifications section for details below)
Virtual Packet Processing	Sends traffic to any existing end-point appliance, physical or virtual tool.
AppStack features	Provides the ability to use Keysight's signature-based application (Layer 7) filtering capabilities. This include the following: • Application filtering using a database of application signatures • Geolocation • Application and Device identification • NetFlow and IxFlow generation • Data masking • Threat Information The vAppStack dashboards provide easy to read information about applications, OS, device type characteristics, as well as threat information.

The private cloud monitoring 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 make informed decisions about how to best protect your business and its data, and ultimately deliver an excellent customer experience.

There are two main aspects to every network visibility solution:

1. Capturing all network traffic, and
2. 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 of these 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 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 Self-Hosted addresses both of these 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.

CloudLens Virtual Tapping (vTap)

CloudLens Self-Hosted 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 Machine Traffic

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

- Enables complete visibility of east-west, inter-VM, inter-Pod through virtual tapping, filtering and traffic forwarding
- Offers a solution with full access to network packets passing between VMs on hypervisor stack
- 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 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, sub-net, protocols, port numbers, and individual VMs.

CloudLens Virtual Taps for Hypervisor 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.

CloudLens Virtual Taps for Containerized Environments and Environments with Limited Hypervisor Access

For private cloud virtual environments where the administrator does not have access to the underlying hypervisor and virtual switches, like the Microsoft private cloud solution Azure Stack, Keysight has introduced a new type of virtual tap in the form of a Cloud Sensor, available for Windows and Linux.

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

The management of the sensors is done via CloudLens Manager, and the CloudLens Sensor Management Platform (CSMP), these services run on premise, do not require Internet access and can be deployed in security tight environments.

The CloudLens Sensors can be used in containerized environments, when there is a need to monitor inter-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, provide capture policies management, and monitoring.
- The CloudLens Sensor Management Platform (CSMP), a cluster of CloudLens services (management services and database) manages and stores the sensors metadata information. The CSMP is managed through CloudLens Manager and it can be deployed on customer workloads (VMs or in a Kubernetes cluster).
- CloudLens vTap sensors, installed in the virtual workloads to monitor, Azure Stack virtual instances for example, are the sources of the traffic to mirror. The sensors offer L2 to L4 filtering options and forward the tapped traffic via GRE tunnel to aggregation points. The sensors can send traffic over any interface available in the virtual workload.

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 tools 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, DPI, application identification and filtering…)

CloudLens Self-Hosted Virtual Packet Processing

In addition to tapping capabilities, CloudLens Self-Hosted supports packet processing within a private cloud environment allowing virtual network traffic aggregation, filtering, deduplication, NetFlow generation, and access to Keysight's application filtering 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 the GRE and VLAN tunnels
- Aggregate network packets
- Filter and deduplicate traffic
- Duplicate and forward traffic

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 Standard or Advanced Virtual Packet Processing must reside in a separate virtual machine 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 cloud allows more effective and efficient use of network bandwidth. Traditionally, all virtual visibility network traffic would be required to leave the private cloud in order to be aggregated and sanitized before forwarded to monitoring tools. With CloudLens™ Self-Hosted, aggregation can occur in the private 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™ Self-Hosted can be deployed as an inline 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 Self-Hosted Virtual Packet Processing with AppStack

Keysight's CloudLens™ with AppStack includes Application 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 deep packet analysis of the virtual traffic sent from CloudLens™ tapping capabilities.

Application Filtering

CloudLens vAppStack has the ability to identify specific hundreds of application signatures, not just application types, and can identify and segment Netflix and Hulu, Microsoft Outlook and Hotmail, Facebook or Snapchat, SAP and Oracle, to name just a few. Once identified, it 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 streaming media 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. Easily exclude YouTube and Netflix traffic from security inspection - reducing bandwidth to your tools.

Keysight's AppStack detects applications through 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, tracking leading and new applications, as well as developing signatures for unknown applications.

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.

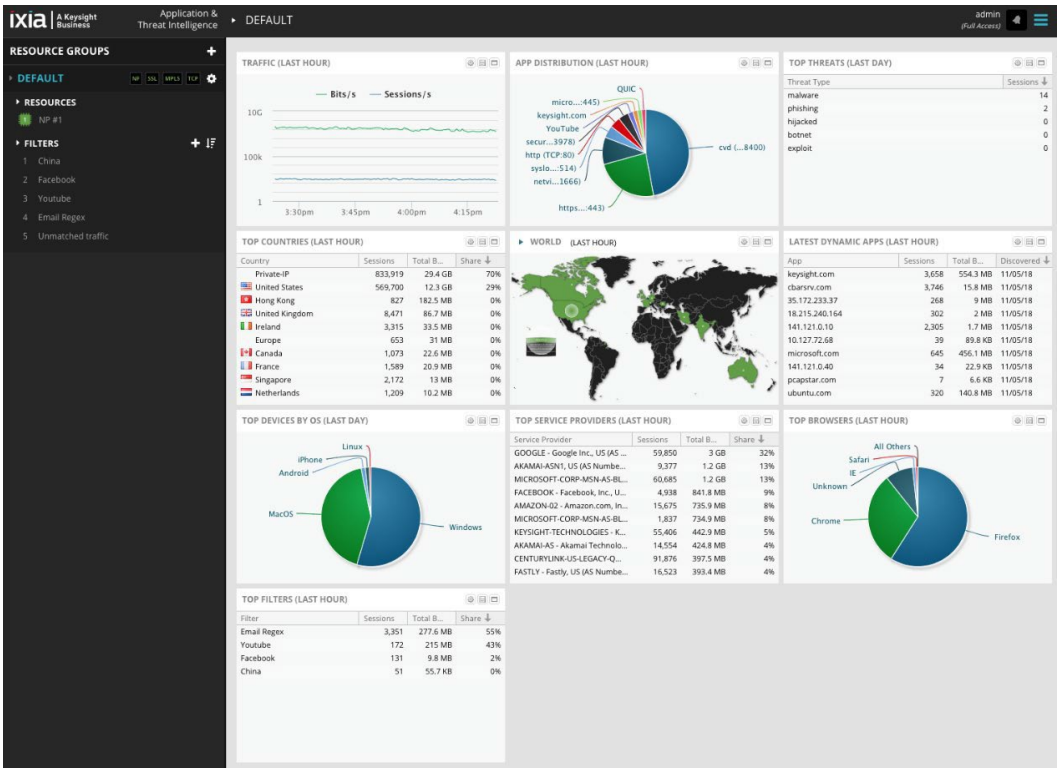


Figure 3. CloudLens with AppStack Real Time Application Dashboard

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 to provide 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 the generated 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 ID or 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

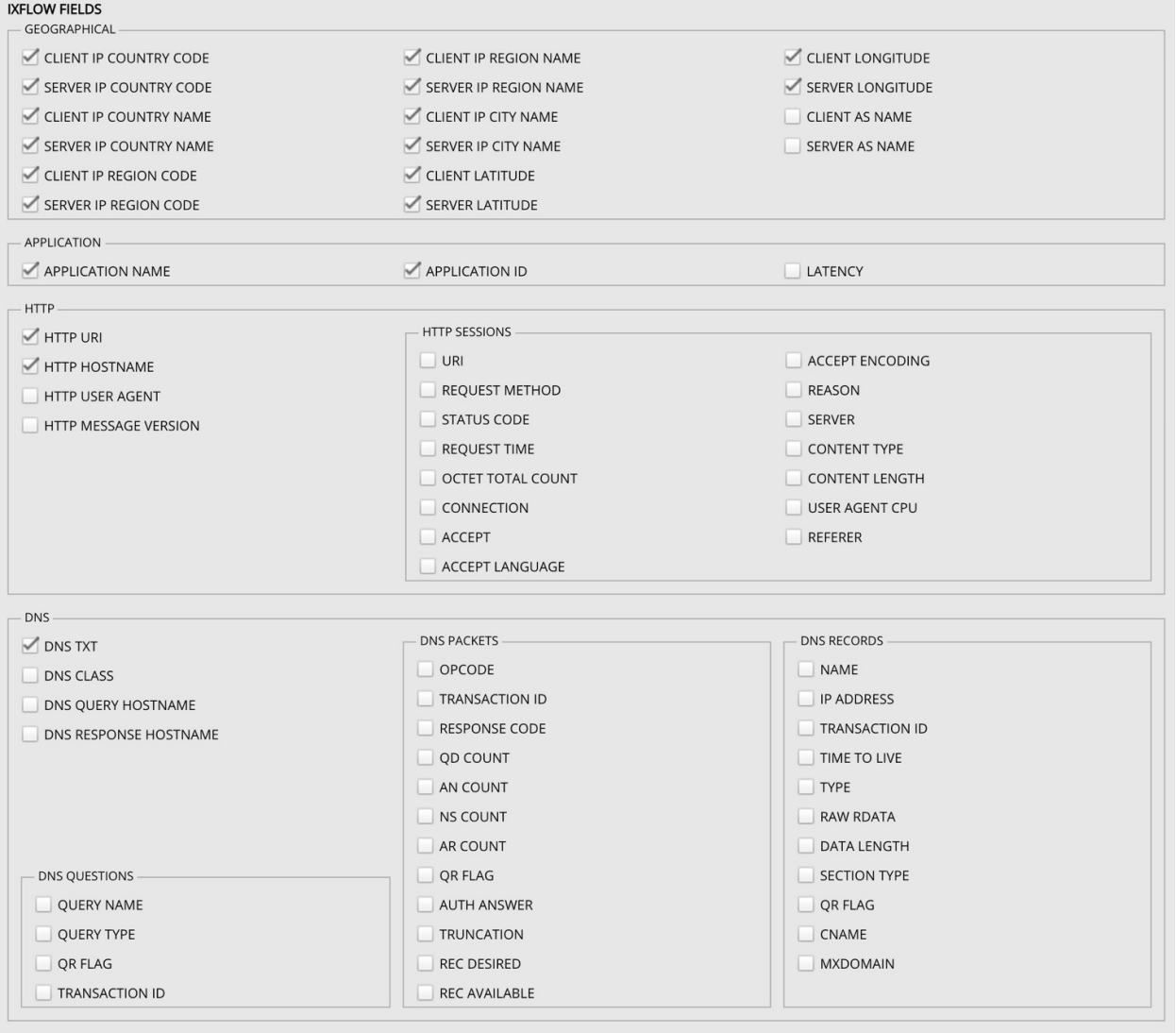


Figure 4. IxFlow fields definition page



Figure 5. IxFlow fields definition page - continued

Geo-Location & 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 the information feed and geolocation database as 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

	Virtual Tapping (vTap)	Virtual packet processing – standard	Virtual packet processing – advanced	Virtual packet processing with AppStack
# Virtual Network Interfaces supported	Not applicable	2	6	8
Max # of filtering rules	Unlimited	20	2000	100
NetStack				
L2-L3 filtering	Yes	Yes	Yes	Yes
(Eth type, VLAN, IP)	(IP)			
L2-L4 filtering	Yes	-	Yes	Yes
Replication	-	Yes	Yes	Yes (1 GRE tunnel)
Load balancing	-	-	Yes	-
Deduplication	-	-	Yes	Yes
Header stripping	-	-	Yes MPLS, FabricPath, VXLAN, PPPoE, GRE, ERSPAN, GTP	Yes GRE & ERSPAN
Packet trimming	-	-	Yes	-
Data masking	-	-	-	Yes
Tunnel origination GRE, ERSPAN	Yes	Yes	Yes	Yes (GRE)
Tunnel termination GRE, ERSPAN	-	Yes	Yes	Yes (GRE)
vAppStack				
Application filtering	-	-	-	Yes
Real-time application dashboard	-	-	-	Yes
Data masking plus	-	-	-	Yes
Geolocation & tagging	-	-	-	Yes
NetFlow	Yes (NSX)	-	-	Yes
IxFlow (enhanced NetFlow)	-	-	-	Yes
Available part numbers (See ordering section for more details)	See “Licenses” in specification table and ordering	LIC-CL-VPP-STD-1 SUB-CL-VPP- STD-1 909-5017	LIC-CL-VPP-AD-1 SUB-CL-VPP-AD-1 909-5016	SUB-CL-AS-1-F 909-5021 SUB-CL-AS-1-F

Table 1. CloudLens™ self-hosted feature breakdown

Specifications

Tapping specifications – V5.1

VMware	ESXi 5.0 & 5.1	ESXi 5.5	ESXi 6.0, 6.5 & 6.7
ESXi - vDS	Yes	Yes [1]	Yes [1]
ESXi - vSS	No	Yes [1]	Yes [1]
NSX for vSphere	6.3, 6.4		
NSX data center (NSX-T)	2.5, 3.0		
Nutanix	AHV (AOS 5.11, 5.15)		
Microsoft Hyper-V	Windows Server 2012, 2012 R2, and 2016		
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)		
Cloud sensor management platform	Deployed on customer workloads (VMs or Kubernetes cluster)		
CloudLens sensors	RedHat, Ubuntu, CentOS, Windows 10, Windows Server 2012 R2 and 2016		
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 CSMP, NSX: Refer to User Guide		
Memory	Manager: 8GB (recommended) – vTap Service (SVM): 512 MB to 3 GB (Hyper-V), 3GB (ESXi) - KVM (integrated with OVS, no additional resource) CSMP, NSX: Refer to User Guide		
Web browser	Google Chrome, Internet Explorer, and Firefox		
Licenses	LIC-CL-VTAP-10		
	LIC-CL-VTAP-50		
	LIC-CL-VTAP-100		
	LIC-CL-VTAP-250		
	LIC-CL-VTAP-1000		
	SUB-CL-VTAP-1000		
	LIC-CL-VTAP-CSMP	SUB-CL-VTAP-CSMP	
	LIC-CL-VTAP-AG100	SUB-CL-VTAP-AG100	
	LIC-CL-VTAP-AG250	SUB-CL-VTAP-AG250	
	LIC-CL-VTAP-AG1000	SUB-CL-VTAP-AG1000	
	LIC-CL-VTAP-NSX		

Standard & advanced packet processing specifications – V1.3

Supported Hypervisors	VMware ESXi 5.5 & 6.0
CPU	Haswell or later processor, e.g.: E5-26xx 4 vCPU
Disk storage	8GB – Thin provisioning
Memory	16GB
Network connectivity	6 predefined interfaces (customizable after installation)
Standard licenses	LIC-CL-VPP-STD-1 SUB-CL-VPP-STD- 909-5017
Advanced licenses	LIC-CL-VPP-AD-1 SUB-CL-VPP-AD-1 909-5016

Packet processing with AppStack specifications – V3.1

Supported Hypervisors	VMware ESXi 6.0, 6.5 & 6.7
CPU	Intel x86-64 - Westmere or newer processor 6 vCPUs
Disk storage	30 GB – Thin provisioning
Memory	16 GB
Network connectivity	3 predefined interfaces
Licenses	SUB-CL-AS-1-F, LIC-CL-AS-1-F 909-5021

1. vCenter required (No standalone ESXi)

Ordering Information: Virtual Tapping

LIC-CL-VTAP-10

Keysight CloudLens vTap 10 License Pack - Perpetual license
This 10 licenses pack includes 10 CloudLens vTap licenses.

LIC-CL-VTAP-50

Keysight CloudLens vTap 50 License Pack - Perpetual license
This 50 licenses pack includes 50 CloudLens vTap licenses.

LIC-CL-VTAP-100

Keysight CloudLens vTap 100 License Pack - Perpetual license
This 100 licenses pack includes 100 CloudLens vTap licenses.

LIC-CL-VTAP-250

Keysight CloudLens vTap 250 License Pack - Perpetual license
This 250 licenses pack includes 250 CloudLens vTap licenses.

LIC-CL-VTAP-1000

Keysight CloudLens vTap 1000 License Pack - Perpetual license
This 1000 licenses pack includes 1000 CloudLens vTap licenses.

LIC-CL-VTAP-NSX

KEYSIGHT CloudLens vTap Add-on for VMware NSX integration - Perpetual license
This add-on includes 3 vTaps (service VMs - SVM). One (1) SVM is required per ESXi host managed by NSX. For additional SVMs, order additional vTap License packs.

SUB-CL-VTAP-1000

Keysight CloudLens vTap 1000 License Pack - 1 Year subscription
This license pack includes the right to use 1000 CloudLens vTap SVMs, valid for 1 year.
This license covers the 1st year subscription. Renewals will use 909-5020

909-5020

Subscription Renewal for SUB-CL-VTAP-1000 (vTap 1000 pack license) Subscription renewal for vTap 1000 pack - 1 Year extension.

REQUIRES pre-existing purchase and valid subscription of SUB-CL-VTAP-1000, 1st year subscription license.

LIC-CL-VTAP-CSMP

CloudLens vTap 1000 Virtual Sensors Pack - Perpetual License

SUB-CL-VTAP-CSMP

Keysight CloudLens vTap Add-on for CloudLens Sensor Management Platform – 1-year subscription

LIC-CL-VTAP-AG50

CloudLens vTap 50 Virtual Sensors Pack – Perpetual License

LIC-CL-VTAP-AG100

CloudLens vTap 100 Virtual Sensors Pack – Perpetual License

SUB-CL-VTAP-AG100

CloudLens vTap 100 Virtual Sensors Pack – 1-year subscription

LIC-CL-VTAP-AG250

CloudLens vTap 250 Virtual Sensors Pack – Perpetual License

SUB-CL-VTAP-AG250

CloudLens vTap 250 Virtual Sensors Pack – 1-year subscription

LIC-CL-VTAP-AG1000

CloudLens vTap 1000 Virtual Sensors Pack – Perpetual License

SUB-CL-VTAP-AG1000

CloudLens vTap 1000 Virtual Sensors Pack – 1-year subscription

Ordering Information: Packet Processing – Basic

LIC-CL-VPP-STD-1

Keysight CloudLens Self-Hosted Virtual Packet Processing with PacketStack (AFM) - 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

SUB-CL-VPP-STD-1

Keysight CloudLens Self-Hosted Virtual Packet Processing with PacketStack (AFM) - 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

909-5017

Subscription Renewal for SUB-CL-VPP-STD-1 CloudLens Self-Hosted Virtual Packet Processing - Standard, 1 instance).

Ordering Information: Packet Processing - Advanced

LIC-CL-VPP-AD-1

Keysight CloudLens Self-Hosted Virtual Packet Processing with PacketStack (AFM) - Advanced, perpetual license, 1 instance.

Includes: 6 virtual interfaces- NetStack: Aggregation, Replication - L2-4 filtering (Eth type, VLAN, IP, Ports, IP Protocol), Up to 2000 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."

SUB-CL-VPP-AD-1

Keysight CloudLens Self-Hosted Virtual Packet Processing with PacketStack (AFM) - Advanced, perpetual license, 1 instance.

Includes: 6 virtual interfaces- NetStack: Aggregation, Replication - L2-4 filtering (Eth type, VLAN, IP, Ports, IP Protocol), Up to 2000 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.

909-5016

Subscription Renewal for SUB-CL-VPP-AD-1 (CloudLens Self-Hosted Virtual Packet Processing - Advanced, 1 instance.

Ordering Information: Packet Processing – with AppStack

LIC-CL-AS-1-F

Keysight CloudLens Self-Hosted virtual packet processing with AppStack (ATIP). 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.

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.

SUB-CL-AS-1-F

Keysight CloudLens Self-Hosted with AppStack (ATIP). Full Feature pack, first year subscription, 1 instance.

Features included: PacketStack: GRE Termination, Deduplication - AppStack: NetFlow generation - Application Filtering, Geolocation and tagging, Data masking, IxFlow generation.

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.

909-5021

Subscription renewal for SUB-CL-AS-1-F (CloudLens Self-Hosted virtual packet processing with AppStack). Must have purchased SUB-CL-AS-1-F in year 1 to be able to renew.

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.

KEYSIGHT

This information is subject to change without notice. © Keysight Technologies, 2018 – 2023, Published in USA, June 6, 2023, 7019-0132.EN