OVERVIEW

Enterprises are adopting private cloud solutions to leverage the flexibility and power of virtualized environments with the increased control of owning the physical infrastructure. However, the limited view of virtualized network traffic creates network visibility blindspots for virtual or physical datacenter monitoring tools.

Ixia CloudLens™ Private allows for a complete cloud based visibility solution for virtual network traffic; includes mirroring, filtering and forwarding traffic between virtual machines and virtual packet processing to aggregate, filter and deduplicate traffic all within a private cloud environment without the need of a physical packet broker.

CloudLens Private has two main components, a tapping capability which gathers, filters and forwards virtual machine traffic, and a virtual packet processing capability which aggregates, filters, deduplicates and forwards traffic to both virtual and physical datacenter tools.

HIGHLIGHTS

- Tap Virtual Machine network traffic.
- Optionally filter traffic at virtual tap, or within a virtual packet broker.
- Virtual packet processing and aggregation in your private cloud without the need for physical packet brokers.
- Aggregate, deduplicate, originate and terminate tunnels without the need for physical hardware.
# PRODUCT FEATURES

<table>
<thead>
<tr>
<th>Feature</th>
<th>Benefit</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Capture Virtual Machine Traffic</strong></td>
<td>Removed visibility blindspots by providing total visibility into all inter-VM 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, and blade server mid-plane traffic through virtual tapping, filtering and traffic forwarding.</td>
</tr>
<tr>
<td><strong>Tap Filtering</strong></td>
<td>Integrated filtering reduces vSwitch and LAN bandwidth consumption by filtering at vTap, providing a multi-layer L2-L4 filtering engine allowing for filtering based on IP address, sub-net, protocols, port numbers, and individual VMs.</td>
</tr>
<tr>
<td><strong>Virtual Packet Processing</strong></td>
<td>Reduces the need for physical packet brokers by allowing for aggregation, filtering, and deduplication within a private cloud.</td>
</tr>
<tr>
<td><strong>Application Filtering</strong></td>
<td>Allows for Ixia’s signature based Application Threat Intelligences (ATI) filtering capabilities within a CloudLens virtual packet broker, providing private cloud based application-level filtering and enhanced NetFlow generation via Ixia best-in-class deep packet inspection (DPI). Also includes the CloudLens Application and Threat Intelligence Dashboard which includes easy-to-use graphical displays of application, OS and device type characteristics.</td>
</tr>
<tr>
<td><strong>Support for vMotion</strong></td>
<td>Guarantees the integrity of visibility as virtual machines are automatically moved due to the dynamic nature of private cloud resourcing.</td>
</tr>
<tr>
<td><strong>Hypervisor agnostic</strong></td>
<td>Supports the most popular private cloud hypervisors including VMware ESXi, Microsoft Hyper-V, KVM, and OpenStack KVM. Integrates with OpenStack orchestration and management to offer multi-tenancy and Tap-as-a-Service (TaaS) support.</td>
</tr>
<tr>
<td><strong>vSwitch agnostic</strong></td>
<td>CloudLens Private is vSwitch agnostic, supporting VMware vSS, vDS, and third-party virtual switches. Supports vSS (virtual standard switch), vDS (virtual distributed switch), and third-party virtual switches for a switch-agnostic solution.</td>
</tr>
<tr>
<td><strong>No Agents Required</strong></td>
<td>Does not require any services or agents to be installed the virtual machine.</td>
</tr>
<tr>
<td><strong>Tool Agnostic</strong></td>
<td>Sends traffic to any existing end-point appliance, physical or virtual tool.</td>
</tr>
</tbody>
</table>
The Private Cloud Monitoring Challenge

Enterprises have been utilizing tap solutions for network traffic access for many years. Traffic capture, analysis, replay, and logging are now part of every well-managed network environment. In recent years, the significant shift to virtualization is yielding great efficiency benefits. However, today’s virtualization-based deployments create challenges for network security, compliance, and performance monitoring. This is because Inter-VM traffic is optimized to speed up connections and minimize network use on the physical core network switches. Such optimization can make traffic invisible to physical tools unable to extend easily into the virtual environments. Costly new virtualization-specific tools plus training can affect the economic benefits and cost-savings of virtualizing. Currently, many tools suffer from limited throughput, hypervisor incompatibility, and excessive resource utilization.

Next-generation data centers use virtualization technology to deploy private/public cloud environments on a single physical server or across a clustered group of servers, local and remote. Traditional taps cannot see the traffic between VMs that reside on the same hypervisor (east-west traffic), nor can they “follow” VMs as they are migrated from one host to another.

Visibility is further reduced by the complexity of blade servers that have each blade running multiple VMs on a hypervisor. Traffic running on blade servers shares a common backplane and creates a network blind spot, since the physical network and its attached tools are unable to see traffic above the virtual switch layer or the blade chassis network modules.

Cloudlens Private Virtual Tapping

CloudLens™ Private utilizes a virtual tapping service which monitors all inter-VM traffic and forward packets to any end-point tool of choice, whether virtual, physical, or a physical network packet broker, to achieve full visibility and verification across networks.

- Enables complete visibility of east-west, inter-VM, and blade server mid-plane traffic through virtual tapping, filtering and traffic forwarding
- Offers a solution with full access to network packets passing between VMs on hypervisor stack
- Provides multi-layer L2-L4 filtering engine
- Sends traffic to any existing end-point appliance, physical or virtual (tool agnostic)
- Follows VMs for continuous visibility throughout migration (VM-level monitoring)
- Supports vMotion and DRS
- Enables proactive monitoring and security of virtual data centers
- Allows retention of system resources by eliminating any need to install agents or services on the VM or application layer
- Allows control of multiple Phantom instances (included software component) for centralized management

Cloudlens™ Private Virtual Packet Processing

In addition to tapping capabilities, CloudLens™ Private supports packet processing within a private cloud environment allowing virtual network traffic aggregation, filtering, deduplication, netflow generation, and access to Ixia’s application intelligence capabilities without the need of a physical packet broker.
Ixia’s CloudLens virtual packet processing resides on a dedicated virtual machine and is an intermediate component in the virtual visibility architecture that “sits” between virtual taps and performance and monitoring tools to

- Terminate the GRE and VLAN tunnels
- Aggregate network packets
- Filter and deduplicate traffic
- Duplicate and forward traffic

Such processing typically requires a physical network packet broker appliance. With CloudLens™, these features are available as a virtual appliance, offering flexibility and simple deployment in dynamic virtual environments.

There are two virtual packet processing products available, CloudLens™ with Packetstack which offers packet manipulation capabilities like header stripping and packet trimming, or CloudLens™ with AppStack which offers Ixia’s best-of-class application and geolocation filtering, Netflow and IxFlow generation, and data masking.

**CloudLens™ Private Virtual Packet Processing with AppStack**

Ixia’s CloudLens AppStack, or Application and Threat Intelligence Processing for virtual environments Processor has patent-pending ability to dynamically detect new and unknown applications. It also provides granular application behavior, user geo-location, mobile device identifier, and browser information. It delivers real-time application data to monitoring tools so that IT professionals to:

- Identify unknown network applications
- Mitigate network security threats from suspicious applications and locations
- Spot trends in application usage to predict and forestall congestion
• Exclude noncritical applications (such as Netflix) when forwarding to an intrusion detection system (IDS) or other tools, optimizing tool processing and delaying the need to upgrade or purchase new gear

To expose hidden attacks, the CloudLens Appstack includes metadata generation which can be exported as enhanced NetFlow, as well as data masking capabilities, useful for compliance requirements, which can automatically overwrite sensitive information such as credit card, taxpayer ID, and phone numbers via a point-and-click user interface.

<table>
<thead>
<tr>
<th>CloudLens TM</th>
<th>Virtual Tapping (vTap)</th>
<th>Virtual Packet Processing – Standard</th>
<th>Virtual Packet Processing – Advanced</th>
<th>Virtual Packet Processing with AppStack</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>NetStack</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>L2-L3 Filtering (Eth Type, VLAN, IP)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>L2-L4 Filtering (Eth type, VLAN, IP, Ports, IP Protocol)</td>
<td>Yes</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td># Virtual Network Interface Supported</td>
<td>Not applicable</td>
<td>2</td>
<td>6</td>
<td>7</td>
</tr>
<tr>
<td>Max # of Filtering Rules</td>
<td>Unlimited</td>
<td>20</td>
<td>9999</td>
<td>9999</td>
</tr>
<tr>
<td><strong>PacketStack</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Aggregation</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Replication</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes (1 GRE Tunnel)</td>
</tr>
<tr>
<td>Load Balancing</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>Deduplication</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Header Stripping</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>Yes (GRE &amp; ERSPAN)</td>
</tr>
<tr>
<td>Packet Trimming</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
<td>-</td>
</tr>
<tr>
<td>Data Masking</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Yes</td>
</tr>
<tr>
<td>Feature</td>
<td>GRE, L2GRE, ERSPAN</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>--------------------</td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>Tunnel Termination</td>
<td></td>
<td>-</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>AppStack</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Application Filtering</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Real-Time Application Dashboard</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Application Identification based on signature</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Data Masking Credit Card and Social Security numbers</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Geolocation &amp; Tagging</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Netflow &amp; IxFlow</td>
<td></td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>Available Part Numbers</td>
<td></td>
<td>PT-10vTAP-P</td>
<td>LIC-CL-1vPB-1BP</td>
<td>LIC-CL-1vPB-1AP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PT-50vTAP-P</td>
<td>SUB-LIC-CL-1vPB-1BP</td>
<td>SUB-LIC-CL-1vPB-1AP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PT-100vTAP-P</td>
<td>SUB-LIC-CL-1vPB-1BP</td>
<td>SUB-LIC-CL-1vPB-1AP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PT-250vTAP-P</td>
<td>SUB-LIC-CL-1vPB-1BP</td>
<td>SUB-LIC-CL-1vPB-1AP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PT-1000vTAP-P</td>
<td>SUB-LIC-CL-1vPB-1BP</td>
<td>SUB-LIC-CL-1vPB-1AP</td>
</tr>
<tr>
<td></td>
<td></td>
<td>SUB-LIC-PT-1000vTAP</td>
<td>SUB-LIC-CL-1vPB-1BP</td>
<td>SUB-LIC-CL-1vPB-1AP</td>
</tr>
</tbody>
</table>
Aggregation, Replication, Deduplication and Filtering

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™ private, 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™ Private with PacketStack is 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.

Application Filtering

Easily exclude YouTube and Netflix traffic from security inspection - reducing bandwidth to your tools. Ixia’s AppStack detects applications through signatures: static, dynamic or even customized with a patent pending technology. With Ixia doing the heavy lifting of figuring out application signature and maintaining a database, you or your team don’t have to become RegEx experts or track changing applications. Ixia regularly updates its application database, tracking leading and new applications, as well as developing signatures for unknown applications.

- Application identification and filtering based on signature, browser, OS, IP address, and geolocation and forwarding to the right security tools
- Quickly separate traffic flow by application type – video, email, web or other – device, OS, browser, carrier, BGP AS#
- Ability to detect unknown applications and add mainstream applications by request
- Monitor and report top applications’ and countries’ bandwidth consumption
NetFlow / IxFlow Generation & Real Time AppStack Dashboard

To expose hidden attacks, CloudLens with AppStack capabilities can generate metadata which can be exported as enhanced NetFlow, as well as data masking capabilities, useful for compliance requirements, which can automatically overwrite sensitive information such as credit card, taxpayer ID, and phone numbers via a point-and-click user interface.

CloudLens Private AppStack feature set provides application-level visibility such as application filtering, deep packet inspection (DPI) and enhanced Netflow generation.

The CloudLens AppStack Dashboard (figure below) 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.

The AppStack is easily managed from a web UI. A web-based RESTful interface is also supported.

While the Dashboard provides extremely useful information on one screen, CloudLens AppStack is build to provide 3rd party applications (IPS, IDS, Netflow collectors) the right information at the right time.

Private cloud implementations can leverage CloudLens AppStack for deep packet analysis of the virtual traffic sent from virtual taps or directly captured from the virtual switch. CloudLens AppStack can leverage CloudLens PacketStack, but the latter is not required.

In addition to SDDC data center East West traffic inspection, CloudLens AppStack is the candidate of choice for remote branch office implementations, where limited available technical resources make troubleshooting difficult. In this use case, CloudLens AppStack can send Netflow metadata to the central data center for processing by monitoring and analyzing tools.

GeoLocation & 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, check out ThreatARMOR. It uses the same information feed and geolocation database as Ixia’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.

**SPECIFICATIONS**

<table>
<thead>
<tr>
<th>TAPPING SPECIFICATIONS</th>
<th>VMware</th>
<th>ESXi 5.0 &amp; 5.1</th>
<th>ESXi 5.5</th>
<th>ESXi 6.0</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi - vSwitch (Kernel Module)</td>
<td>Yes</td>
<td>Yes¹</td>
<td>No</td>
<td></td>
</tr>
<tr>
<td>ESXi - vDS</td>
<td>Yes</td>
<td>Yes²</td>
<td>Yes²</td>
<td></td>
</tr>
<tr>
<td>ESXi - vSS</td>
<td>No</td>
<td>Yes²</td>
<td>Yes²</td>
<td></td>
</tr>
<tr>
<td>Microsoft Hyper-V</td>
<td>Windows 2012 and 2012 R2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KVM</td>
<td>v.2.01 and above with Open vSwitch (OVS) 2.0 and above²</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpenStack KVM</td>
<td>Liberty with KVM OVS (see above)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OpenStack Tap-as-a-Service (TaaS)</td>
<td>Liberty, Mitaka with v2 authentication (Keystone)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Network Connectivity</td>
<td>Phantom Management Server VM must be accessible via HTTP to access Web UI</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>TCP port 22, 80, 443, and 5989 must be open between Phantom Management Server VM and VMware vCenter server</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Disk Storage</td>
<td>Phantom Manager: 4 GB - vTap Service (SVM): 2-4GB – TaaS SVM: 5GB</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CPU</td>
<td>Phantom Manager: 2 vCPU - vTap Service (SVM): 1-2 Vcpu</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### DATA SHEET

<table>
<thead>
<tr>
<th>Memory</th>
<th>Phantom Manager: 8GB (recommended) – vTap Service (SVM): 512MB to 3GB (Hyper-V), 3GB (ESXi) – Taas: 1GB - KVM (integrated with OVS, no additional resource)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Browser</td>
<td>Google Chrome, Internet Explorer, and Firefox</td>
</tr>
</tbody>
</table>

1 For upgrading existing customer or special cases
2 vCenter required (No standalone ESXi)
3 Standalone Hyper-V Hosts (No SCVMM)

### STANDARD & ADVANCED PACKET PROCESSING SPECIFICATIONS

<table>
<thead>
<tr>
<th>Supported Hypervisors</th>
<th>VMware ESXi 5.5</th>
</tr>
</thead>
</table>
| CPU                   | • Haswell or later processor, e.g.: E5-26xx  
• 1 dedicated CPU per IO port +1 CPU for management functions |
| Disk Storage          | 8GB – Thin provisioning |
| Memory                | 16GB |
| Network Connectivity  | 6 predefined interfaces (customizable after installation) |

### PACKET PROCESSING WITH APPSTACK SPECIFICATIONS

<table>
<thead>
<tr>
<th>Supported Hypervisors</th>
<th>VMware ESXi 5.5</th>
</tr>
</thead>
</table>
| CPU                   | • Intel x86-64 - Westmere or newer processor  
• 6 vCPUs |
| Disk Storage          | 30GB – Thin provisioning |
| Memory                | 8GB |
| Network Connectivity  | 3 predefined interfaces |
### Ordering Information: Packet Processing – Basic

**PT-10vTAP-P**
954-4056. Phantom vTap 10 pack Perpetual license
This 10 licenses pack includes 10 Phantom 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 Phantom Service Manager.

**PT-50vTAP-P**
954-4059. Phantom vTap 50 pack Perpetual license
This 50 licenses pack includes 50 Phantom vTap licenses.

**PT-100vTAP-P**
954-4057. Phantom vTap 100 pack Perpetual license
This 100 licenses pack includes 100 Phantom vTap licenses.

**PT-250vTAP-P**
954-4061. Phantom vTap 250 pack Perpetual license
This 250 licenses pack includes 250 Phantom vTap licenses.

**PT-1000vTAP-P**
954-4058. Phantom vTap 1000 pack Perpetual license
This 1000 licenses pack includes 1000 Phantom vTap licenses.

**SUB-LIC-PT-1000VTAP**
954-4085. Phantom vTap 1000 pack license - 1 Year subscription
This license pack includes the right to use 1000 Phantom vTap agent VMs, valid for 1 year.
This license covers the 1st year subscription. Renewals will use SUB-LIC-PT-1000vTAP-EXTN (909-5020).

**SUB-LIC-PT-1000VTAP-EXTN**
909-5020. Subscription Renewal for 954-4085 (Phantom vTap 1000 pack license)
Subscription renewal for Phantom vTap 1000 pack - 1 Year extension.
REQUIRES pre-existing purchase and valid subscription of SUB-LIC-PT-1000vTAP (954-4085), 1st year subscription license.

### Ordering Information: Packet Processing – Basic

**LIC-CL-1vPB-1BP**
Virtual Packet Broker - Basic pack. 1 instance, Perpetual license (954-4062)
The Basic Pack includes:

- 2 virtual interfaces (Multiple GRE tunnels termination)
- 20 rules
- L2-3 Filtering (Eth type, VLAN, IP)

**SUB-LIC-CL-1vPB-1BP**

Virtual Packet Broker - Basic Pack. 1 instance, 1 year subscription

The Basic Pack yearly subscription license includes:

- 2 virtual interfaces (Multiple GRE tunnels termination)
- 20 rules
- L2-3 Filtering (Eth type, VLAN, IP)

Unlimited software updates for one year from date of purchase
Access to Customer Web Portal and Technical Support during normal business hours

**SUB-LIC-CL-1vPB-1BP-EXTN**

Virtual Packet Broker - Basic pack. 1 instance, 1 year extension (909-5017)

1-year service extension for the subscription license

### Ordering Information: Packet Processing – Advanced

**LIC-CL-1vPB-1AP**

Virtual Packet Broker. Advanced pack, 1 instance, Perpetual license (954-4063)

The Advanced Pack includes:

- 6 virtual interfaces - 12 GRE originating tunnels
- Up to 9999 rules
- Header stripping
- L2-4 filtering (Ports, IP Protocol)
- Load balancing

**SUB-LIC-CL-1vPB-1AP**

Virtual Packet Broker. Advanced pack, 1 instance, 1 year subscription (954-4083)

The Advanced Pack yearly subscription license includes:

- 6 virtual interfaces - 12 GRE originating tunnels
- Up to 9999 rules
- Header stripping
• L2-4 filtering (Ports, IP Protocol)
• Load balancing

Unlimited software updates for one year from date of purchase
Access to Customer Web Portal and Technical Support during normal business hours

**SUB-LIC-CL-1vPB-1AP-EXTN**
Virtual Packet Broker - Advanced pack. 1 instance, 1-year extension (909-5016)
1-year service extension for the subscription license

### Ordering Information: Packet Processing – with AppStack

**SUB-LIC-CL-VATI-1FP**
CloudLens Private AppStack. Full Feature pack, 1 virtual instance, 1 year subscription (954-4064).
This pack includes:

• Netflow generation
• Application Intelligence (App filtering, Geo-location)
• Data masking
• Software updates for one (1) year
• Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours.

**SUB-LIC-CL-VATI-1FP-RENEWAL**
Subscription Renewal for 954-4064 (CloudLens Private AppStack Full Feature pack for one (1) virtual instance). REQUIRES pre-existing purchase of SUB-LIC-CL-vATI-1FP (954-4064)
This includes:

• The right to use CloudLens Private AppStack Full Pack for one (1) year
• Software updates for one (1) year
• Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours.

**LIC-CL-VATI-1FP**
CloudLens Private AppStack. Full Feature pack, 1 virtual instance - Permanent license (954-4065). This pack includes:

• Netflow generation
• App Intelligence (App filtering, Geo-location)
• Data masking
• Software updates for one (1) year
• Access to Customer Web Portal and Technical Support for one (1) year, during normal business hours.

IXIA WORLDWIDE HEADQUARTERS
26601 AGOURA RD.
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