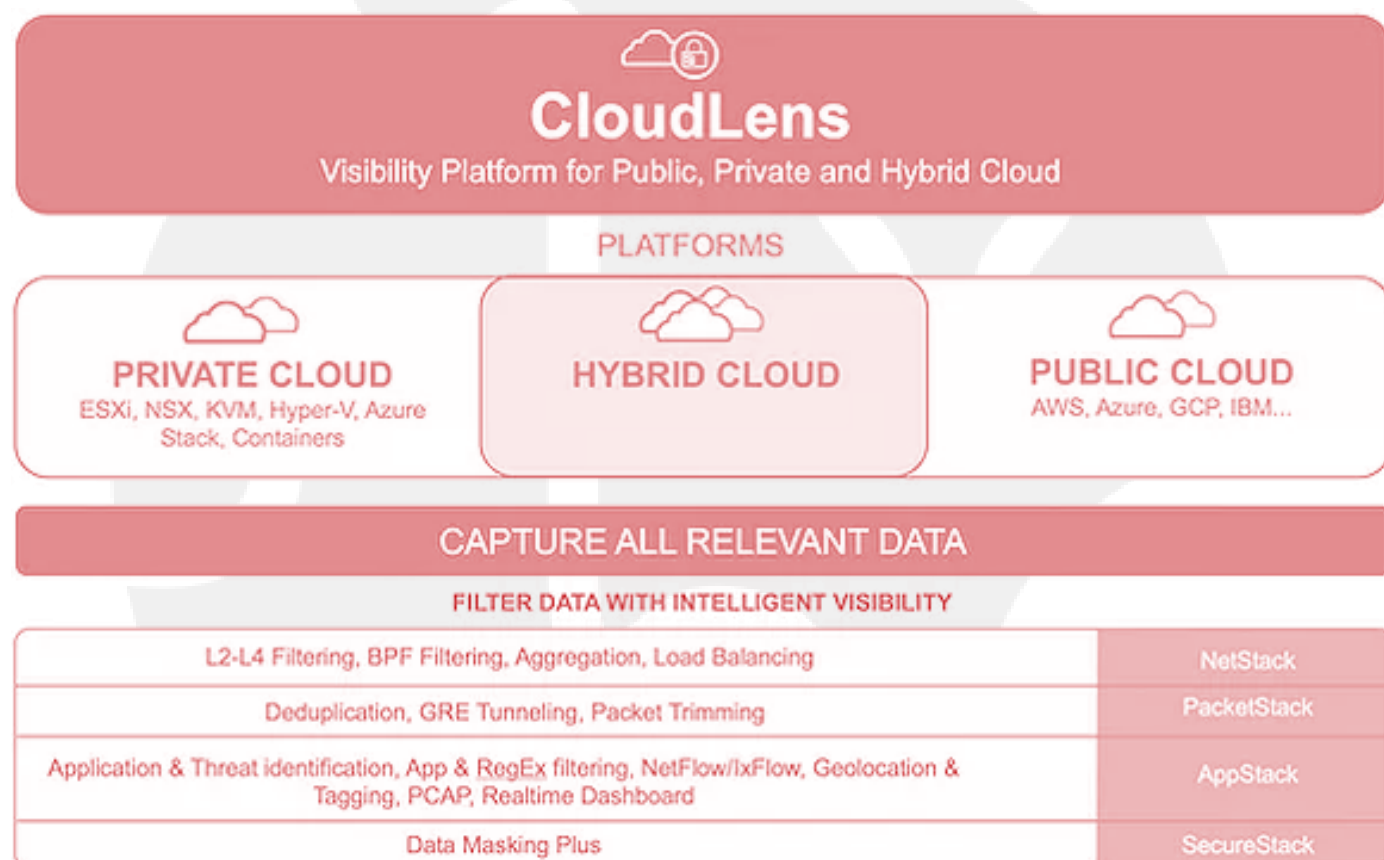


CloudLens

Видимость публичного, частного и гибридного облака

Обеспечение видимости для защиты и мониторинга облачных сред

Организации переносят рабочие нагрузки в облако, поскольку оно обеспечивает масштабируемость, гибкость и адаптивность. Этим организациям необходима видимость, чтобы соблюдать политики безопасности, соответствия требованиям и мониторинга в публичном, частном и гибридном облаке.



Тел: +7 (495) 252-00-96

Email: info-site@akmetron.ru

Адрес: Москва, ул. Рабочая, д.93 стр.2, под. 2.

Основные особенности

- Захват и передача полных пакетов и/или NetFlow из виртуальной машины (VM), контейнеров или сетевого трафика между Pod средствами либо физическим и/или виртуальным пакетным брокерам для агрегирования, расширенной фильтрации и дедупликации.
- Виртуальная обработка и агрегирование пакетов в облаке, для которых традиционно используются физические пакетные брокеры.
- Агрегирование и дедупликация пакетных данных; формирование и терминация туннелей без необходимости в физическом оборудовании.
- Виртуальная обработка пакетов с возможностями AppStack использует расширенную аналитику приложений Keysight с обнаружением приложений на основе сигнатур, геолокацией, NetFlow и IxFlow (расширенным NetFlow).
- Интерфейс управления, который можно развернуть в любом облаке для более эффективного контроля и безопасности.
- Поддержка нескольких платформ, независимость от поставщика облачных услуг и платформы.
- Автоматическое эластичное масштабирование по требованию с помощью облачных экземпляров.
- Работа в облачном масштабе (тысячи экземпляров). Автоматическое эластичное масштабирование по требованию с помощью облачных экземпляров.
- Простой в использовании интерфейс с перетаскиванием и компоновкой от сети к средствам.

Задача обеспечения видимости облака

Все сети неизбежно подвергаются все более сложным и продвинутым рискам и угрозам безопасности. Ключевой задачей является как можно более быстрое выявление рисков и угроз и принятие эффективных мер. Цель архитектуры полной видимости — предоставить доступ ко всем данным, пересекающим ваши сети, чтобы можно было.

Каждое решение сетевой видимости включает два основных аспекта:

1. захват всего сетевого трафика; и агрегирование, фильтрация, дедупликация и изменение собранного сетевого трафика до его передачи средствам производительности, мониторинга и безопасности.

Для сбора сетевого трафика традиционно наилучшим способом захвата всего трафика в сетевом канале является использование сетевого ответвителя (network tap). Ответвители предоставляют непрерывный неразрушающий доступ к сети и обладают следующими характеристиками:

- получают весь трафик в сетевом канале;
- требуют минимальной настройки или не требуют ее вовсе и могут быть установлены в любое время;
- не имеют IP-адреса и поэтому не уязвимы для удаленного доступа злоумышленника;
- не вносят задержку и не изменяют содержимое данных.

Для агрегирования, фильтрации, дедупликации и изменения сетевого трафика традиционно применяется физический сетевой пакетный брокер (Network Packet Broker, NPB). NPB используются для обработки пакетов и передачи выбранных пакетов конкретным средствам в соответствии с тем, для мониторинга и анализа чего предназначены эти средства. NPB агрегируют необработанный или отфильтрованный трафик из нескольких точек мониторинга в сети и фильтруют и дедуплицируют пакеты, чтобы средства получали только релевантный трафик. Это снижает перегрузку данными, минимизирует ложные срабатывания и позволяет обрабатывать трафик с меньшим количеством устройств мониторинга.

Однако в современных виртуализованных развертываниях оба этих аспекта представляют сложность:

1. сбор виртуализованного сетевого трафика между виртуальными рабочими нагрузками или трафика восток–запад (между ВМ или между контейнерами/Pod), недоступного традиционному физическому ответвителю;
2. обеспечение масштабирования решения видимости в соответствии с динамическим характером частного и публичного облака. Если трафик виртуализованной сети необходимо обрабатывать физическим сетевым пакетным брокером, добавление новых ресурсов требует ручного вмешательства, а сложность возрастает.

CloudLens решает обе проблемы с помощью двух основных компонентов: функции виртуального ответвления (vTap), которая собирает, фильтрует и направляет трафик виртуальных рабочих нагрузок, и функции виртуальной обработки пакетов, которая агрегирует, фильтрует, дедуплицирует и направляет трафик как виртуальным, так и физическим средствам центра обработки данных. Кроме того, CloudLens может динамически обнаруживать конкретные приложения и угрозы, а не только типы или категории приложений, фильтруя и направляя сетевой трафик в реальном времени соответствующим средствам для дальнейшего анализа безопасности, производительности или криминалистического анализа.

Решение CloudLens

Keysight CloudLens™ предоставляет комплексное облачное решение видимости трафика виртуальной сети. С CloudLens можно зеркалировать данные, фильтровать и направлять трафик между виртуальными машинами, **контейнерами или Pod Kubernetes и средствами. Решение включает две основные возможности. Во-первых**, возможность виртуально создавать ответвление (vTap), то есть захватывать, фильтровать и направлять копию сетевого трафика непосредственно средствам или сетевому пакетному брокеру. Во-вторых, оно может работать как виртуализованный сетевой пакетный брокер, обеспечивая агрегирование, фильтрацию и дедупликацию трафика виртуальной сети целиком в облаке.

CloudLens vTap

CloudLens предоставляет службу vTap, которая контролирует весь трафик между виртуальными рабочими нагрузками и направляет пакеты любому выбранному конечному устройству — виртуальным или физическим средствам безопасности, мониторинга или аналитики, а также физическим сетевым пакетным брокерам — для достижения полной видимости и проверки во всех сетях.

Захват виртуального трафика

Устранение слепых зон видимости за счет полного обзора всего трафика между VM и/или между Pod, захвата интересующего трафика и его направления физическим или виртуальным пакетным брокерам либо непосредственно средствам мониторинга.

- обеспечивает полную видимость трафика восток–запад, между VM и между Pod посредством виртуального ответвления, фильтрации и перенаправления трафика;
- предоставляет решение с полным доступом к сетевым пакетам, проходящим между VM в стеках гипервизоров;
- передает трафик любому существующему конечному устройству — физическому или виртуальному (не зависит от средства);
- следует за VM для непрерывной видимости на протяжении миграции (мониторинг на уровне VM);
- поддерживает vMotion и DRS;
- соответствует требованиям SLA и нормативным требованиям (SOX, PCI, HIPAA);
- обеспечивает упреждающий мониторинг и безопасность виртуальных центров обработки данных.

Фильтрация ответвления

Встроенная фильтрация снижает потребление пропускной способности vSwitch, vNet, VPC и LAN за счет фильтрации в точке vTap (источнике) и предоставляет многоуровневый механизм фильтрации L2–L4 по IP-адресу, подсети, протоколам, номерам портов и/или отдельным рабочим нагрузкам.

CloudLens vTap — среды на базе гипервизоров

Мониторинг трафика восток–запад в среде гипервизора типа 2 (VMware ESXi, Microsoft Hyper-V, KVM) обычно выполняется на уровне виртуального коммутатора. В таких средах администратор располагает необходимыми разрешениями для развертывания vTap на контролируемых узлах и использования возможностей зеркалирования vSwitch для получения копии сетевого трафика.

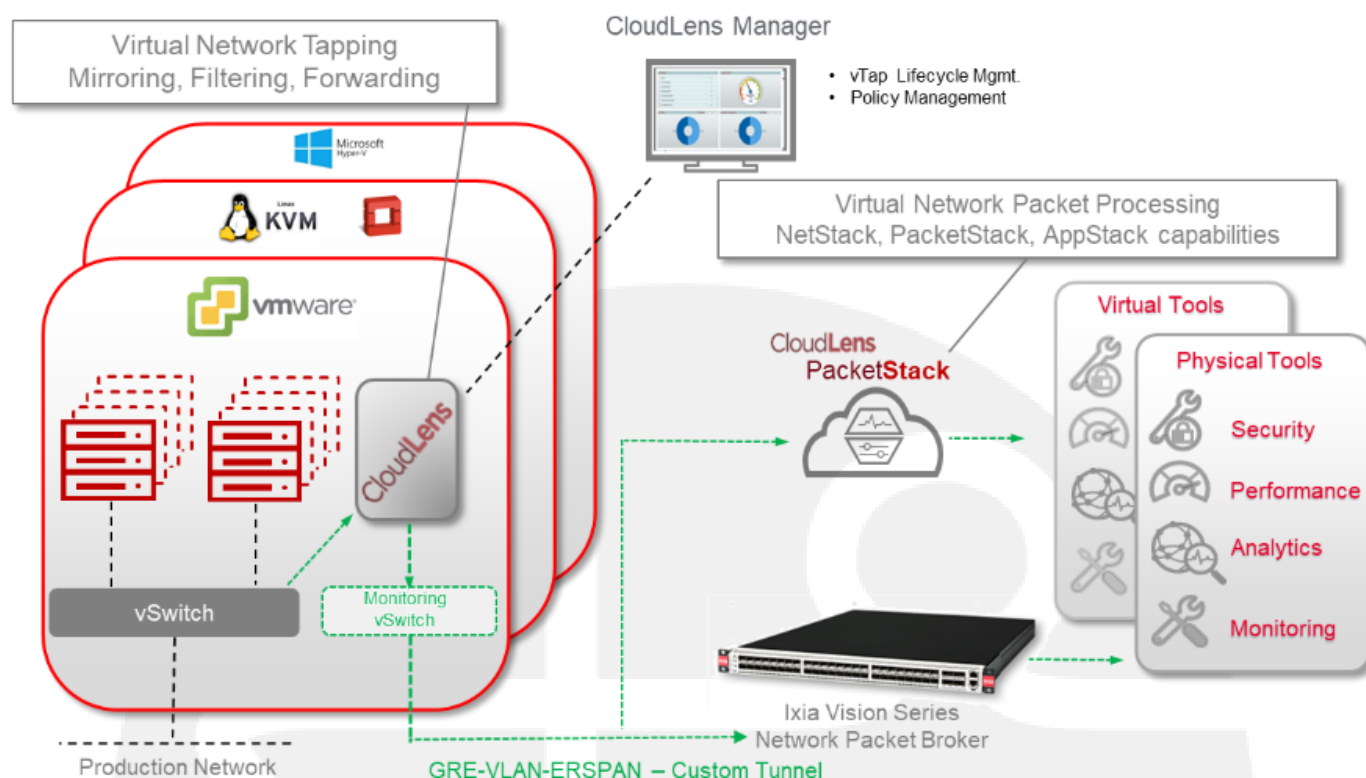


Рисунок 1. Виртуальное ответвление частной облачной сети

CloudLens vTap — развертывания на базе сенсоров

Для виртуальных сред, в которых администратор не имеет доступа к базовому гипервизору и виртуальным коммутаторам, например AWS, Azure, GCP и другим, Keysight представила виртуальный ответвитель в виде Sensor, доступный для Windows и Linux.

Такая реализация, при которой CloudLens Sensor vTap работает в контролируемой рабочей нагрузке, обеспечивает решение, не зависящее от гипервизора.

Управление сенсорами выполняется посредством CloudLens Manager, который может работать практически в любой виртуальной или контейнеризованной среде и может быть развернут в средах с жесткими требованиями безопасности.

CloudLens Sensor vTap можно использовать в контейнеризованных средах (то есть Kubernetes), когда требуется контролировать трафик между Pod. В этом случае сенсоры устанавливаются в качестве дополнительного контейнера (sidecar) в контейнерных Pod Kubernetes.

Экосистема виртуального ответвления включает следующие компоненты:

- CloudLens Manager, развертываемый как виртуальное устройство или в кластере Kubernetes, обеспечивает управление захватом и фильтрацией, а также мониторинг.

Тел: +7 (495) 252-00-96

Email: info-site@akmetron.ru

Адрес: Москва, ул. Рабочая, д.93 стр.2, под. 2.

- CloudLens Sensor vTap, установленные в контролируемых виртуальных рабочих нагрузках, например в AWS, Azure и GCP, являются источниками зеркалируемого трафика. Сенсоры предоставляют варианты фильтрации BPF и направляют ответвленный трафик по туннелю GRE, VxLAN или зашифрованному туннелю в точки агрегирования. Сенсоры могут передавать трафик через любой интерфейс, доступный в виртуальной рабочей нагрузке.

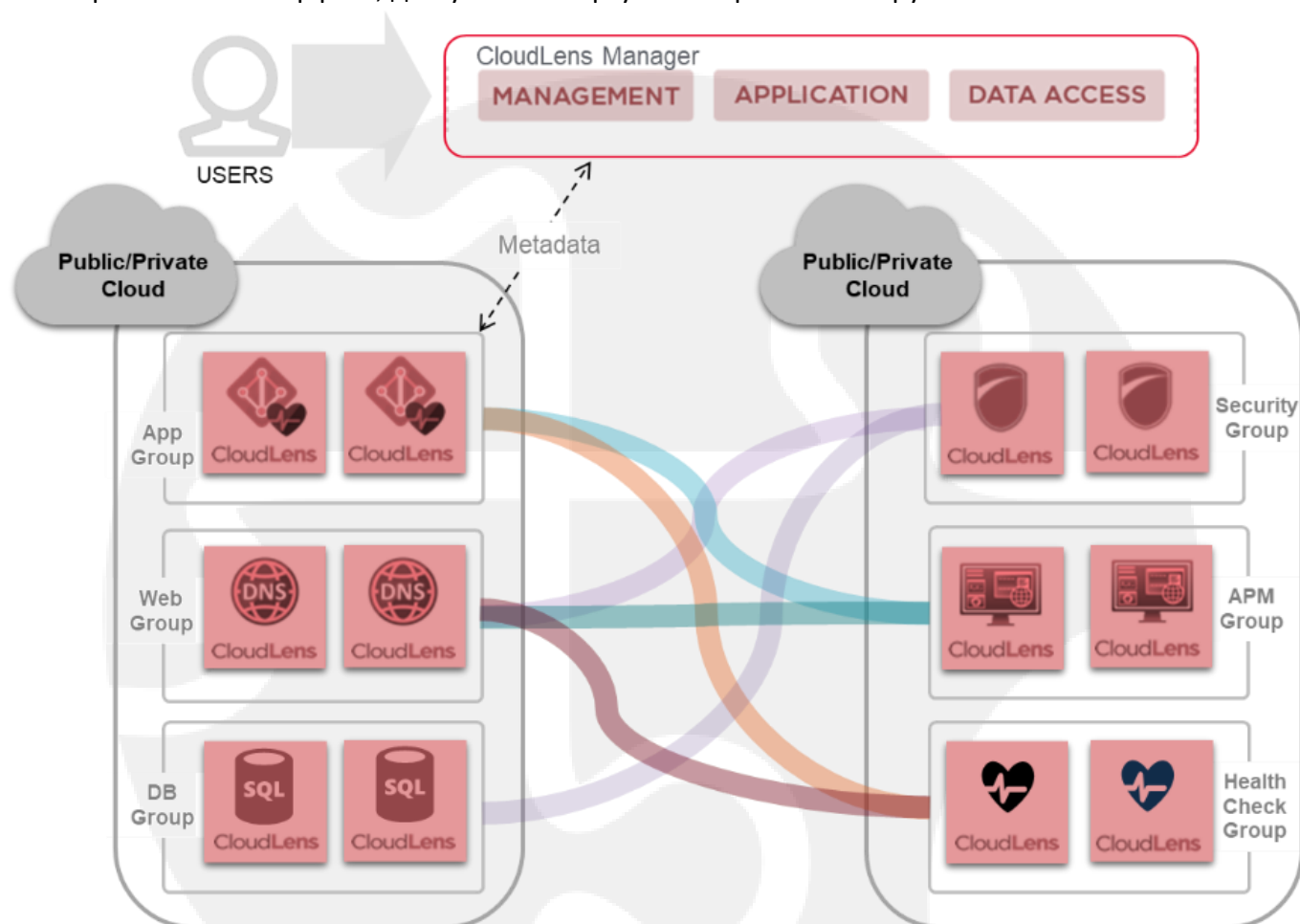


Рисунок 2. Sensor vTap на уровне приложения

CloudLens vTap для VMware NSX

Keysight CloudLens — сертифицированное VMware решение, которое предлагает специальную интеграцию CloudLens vTap для виртуального ответвления сред NSX for vSphere и NSX Data Center (NSX-T).

В NSX Data Center CloudLens использует механизм цепочки служб NSX для вставки CloudLens в качестве службы сетевой интроспекции; затем служба интегрируется с группами и политиками безопасности NSX и становится частью архитектуры NSX. Чтобы упростить задачи администратора, жизненный цикл развертывания управляется из NSX Manager. Сетевой администратор может выбрать развертывание виртуальной машины службы виртуальных ответвителей CloudLens (SVM) на узел или на кластер узлов.

Тел: +7 (495) 252-00-96

Email: info-site@akmetron.ru

Адрес: Москва, ул. Рабочая, д.93 стр.2, под. 2.

Функция «Копирование пакетов» (Copy Packet) зеркалирует трафик восток–запад выбранных ВМ в CloudLens vTap (захват трафика основан на группах и политиках безопасности NSX).

Служба CloudLens предоставляет возможности фильтрации L2–L4, а также может формировать метаданные в формате NetFlow (V9 и V10). Зеркалированный трафик может направляться либо непосредственно средству мониторинга, либо агрегатору/сетевому пакетному брокеру (NPB — виртуальному или физическому) для дополнительной обработки. Такая интеграция позволяет VMware NSX использовать глобальное решение видимости Keysight и его расширенные возможности обработки пакетов, идентификации и фильтрации приложений (репликация, дедупликация, идентификация и фильтрация приложений).

Технические характеристики CloudLens vTap

В следующей таблице приведены технические характеристики vTap v5.5 и vTap v6.2.1.

Технические характеристики Network vTap — v5.5

VMware	ESXi 5.0 и 5.1	ESXi 5.5	ESXi 6.0–7.0
ESXi — vDS	ДА	ДА ¹	ДА ¹
ESXi — vSS	НЕТ	ДА ¹	ДА ¹
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 и выше с Open vSwitch (OVS с DPDK или без него), 2.5 и выше		
OpenStack KVM	Mitaka и более новые версии (Keystone v3) с KVM OVS (см. выше)		
Сетевое подключение	ВМ сервера управления должна быть доступна по HTTP/HTTPS для доступа к веб-интерфейсу (сведения о конкретной платформе см. в руководстве пользователя)		
Дисковое пространство	Manager: 4 GB — служба vTap (SVM): 2–4 GB — NSX: см. руководство пользователя		
CPU	Manager: 2 vCPU — служба vTap (SVM): 1–2 vCPU, NSX: см. руководство пользователя		
Память	Manager: 8 GB (рекомендуется) — служба vTap (SVM): от 512 MB до 3 GB (Hyper-V), 3 GB (ESXi) — KVM (интегрируется с OVS, дополнительные ресурсы не требуются), NSX: см. руководство пользователя		
Веб-браузер	Google Chrome, Internet Explorer и Firefox		

Технические характеристики Sensor vTap — v6.2.1	
Sensor vTap	Развертывается в рабочих нагрузках заказчика (ВМ или кластер Kubernetes). Для развертывания требуется containerd (как правило, Docker или Kubernetes, но может работать и с другими системами).
Сенсоры CloudLens	Windows 10, Windows Server 2012–2019, большинство ОС на базе Linux с Docker
SVM на базе сенсора	Nutanix AHV 5.0+
Сетевое подключение	ВМ сервера управления должна быть доступна по HTTP/HTTPS для доступа к веб-интерфейсу (сведения о конкретной платформе см. в руководстве пользователя)
Дисковое пространство	Manager: 100 GB — Sensor vTap: 1 GB
CPU	Manager: 4 vCPU — Sensor vTap: 1 vCPU
Память	Manager: 16 GB — Sensor vTap: 256 MB
Веб-браузер	Google Chrome, Internet Explorer и Firefox

CloudLens vPacketStack (vPB)

В дополнение к возможностям ответвления CloudLens поддерживает обработку пакетов в среде частного или публичного облака, обеспечивая агрегирование, фильтрацию и дедупликацию трафика виртуальной сети, формирование NetFlow и доступ к возможностям аналитики приложений Keysight без необходимости в физическом пакетном брокере.

Виртуальная обработка пакетов CloudLens от Keysight осуществляется выделенной виртуальной машиной, которая является промежуточным компонентом архитектуры виртуальной видимости и «находится» между точками vTap и средствами производительности и мониторинга, для которых она может выполнять следующие действия:

- терминировать/удалять GRE, VxLAN, Geneve и VLAN;
- агрегировать сетевые пакеты;
- повторно собирать сетевые пакеты;
- фильтровать и дедуплицировать трафик;
- дублировать и направлять трафик;
- выполнять балансировку нагрузки.

Для такой обработки традиционно требовалось физическое устройство сетевого пакетного брокера. С CloudLens эти функции доступны в облачном формате, обеспечивая гибкость и простое развертывание в динамических виртуальных средах.

Доступны несколько вариантов виртуальной обработки пакетов: CloudLens Virtual Packet Processing Standard или Advanced, которые предоставляют такие возможности изменения пакетов, как удаление заголовков и усечение пакетов, либо CloudLens с AppStack, предлагающий лучшие в своем классе функции Keysight для фильтрации приложений и геолокации, формирования NetFlow и IxFlow и маскирования данных (дополнительные сведения см. ниже в таблице функций CloudLens).

Примечание. CloudLens Virtual Packet Processing размещается в экземпляре, отдельном от CloudLens Virtual Packet Processing с AppStack.

Агрегирование, репликация, дедупликация и фильтрация с помощью виртуальной обработки пакетов

Агрегирование, репликация, фильтрация и дедупликация данных в частном или публичном облаке обеспечивают более результативное и эффективное использование пропускной способности сети. Традиционно весь сетевой трафик виртуальной видимости должен был покидать частное или публичное облако для агрегирования и очистки перед направлением средствам мониторинга. С CloudLens™ агрегирование может выполняться в частном или публичном облаке, где данные затем дополнительно дедуплицируются и фильтруются, что обеспечивает намного более эффективное использование емкости как виртуальной, так и физической сети.

Балансировка нагрузки

CloudLens vPB можно развернуть как ВМ пакетной брокеризации (или обработки), которая балансирует нагрузку выбранного трафика виртуальной сети по виртуальным средствам, например виртуальным устройствам оптимизации WAN. Она работает аналогично физическому сетевому пакетному брокеру. Любая рабочая нагрузка, не выбранная для оптимизации, направляется в обход систем оптимизации WAN. Остальная рабочая нагрузка направляется средствами оптимизации. После оптимизации трафик возвращается ВМ обработки пакетов, которая направляет его по исходному пути.

CloudLens vAppStack (vATIP)

Keysight CloudLens™ с AppStack включает обработку аналитики приложений для виртуальных сред и находящиеся на стадии патентования возможности выбора приложений и групп приложений простым указанием и щелчком, а также динамического обнаружения новых и даже неизвестных приложений. Кроме того, решение предоставляет подробные сведения о поведении приложений, геолокации пользователей, идентификаторах мобильных устройств и браузерах.

Сбор данных трафика виртуальной сети

В реализациях частного облака можно использовать обработку пакетов CloudLens™ с AppStack для анализа виртуального трафика, поступающего от возможностей ответвления CloudLens™.

Фильтрация приложений

CloudLens vAppStack может сопоставлять сотни сигнатур приложений для индивидуальной идентификации приложений. Это также означает, что можно определять типы и сегменты/группы приложений, например Netflix и Hulu, Microsoft Outlook и Hotmail, Facebook или Snapchat, SAP и Oracle. После сопоставления приложения CloudLens применяет к этому трафику фильтры и правила, что позволяет ИТ-организациям значительно повысить эффективность последующих средств. Например, поскольку передача потокового мультимедийного трафика системам обнаружения вторжений (IDS) практически бесполезна, возможности AppStack позволяют организации ограничить поступление трафика этих приложений на конкретные средства мониторинга и сетевые устройства, снижая требуемую ими пропускную способность.

AppStack компании Keysight обнаруживает приложения по статическим, динамическим и даже настраиваемым сигнатурам с использованием технологии, находящейся на стадии патентования. Поскольку сложную работу по определению сигнатур приложений и ведению базы данных выполняет Keysight, вам и вашей команде не нужно становиться экспертами по RegEx или отслеживать изменения приложений.

Keysight регулярно обновляет базу данных приложений, отслеживает ведущие и новые приложения, а также вручную анализирует неизвестные приложения, чтобы разрабатывать сигнатуры приложений, если они не опубликованы.

В рамках функции идентификации сигнатур приложений возможности AppStack позволяют выявлять и помечать неизвестные приложения. Затем к такому трафику можно применять правила и фильтры для его оценки и дальнейших действий. Эта возможность дополнительно укрепляет инфраструктуру безопасности и может указывать на наличие вредоносного ПО, нежелательных передач или даже перехваченных данных.

Панель обработки пакетов CloudLens™ с AppStack содержит простые в использовании графические представления и предоставляет обзор карты сетевого трафика. Администратор может быстро увидеть, откуда поступает трафик, какие приложения и страны были наиболее активны за определенный период времени, а также какие операционные системы и устройства активны в сети.

Хотя панель предоставляет исключительно полезную информацию на одном экране, CloudLens™ создан для передачи сторонним приложениям — IPS, IDS и коллекторам NetFlow — нужной информации в нужное время.

Панель приложений отображает следующие поля:

1. Трафик (Traffic): объем трафика в реальном времени.
2. Распределение приложений (App Distribution): пропускная способность по приложениям.
3. Сведения об основных угрозах (Top Threats information): сводные данные о количестве угроз в сети, отсортированные по категории угроз — вредоносное ПО, фишинг, перехваченный IP-адрес, ботнет, эксплойты IoT.
4. Последние динамические приложения (Latest Dynamic Apps): последние динамически обнаруженные приложения и сформированный ими трафик в байтах и сеансах.
5. Основные страны (Top Countries): страны, сформировавшие наибольший объем трафика.
6. Мир (World): карта мира, на которой выделены страны-источники трафика.

7. Основные устройства по ОС (Top Devices by OS): агрегированный по ОС трафик в байтах и сеансах за последний час.
8. Основные фильтры (Top Filters): агрегированный по фильтрам трафик за последние 24 часа.
9. Основные приложения (Top Apps): агрегированный по приложениям трафик по используемой пропускной способности, байтам и сеансам.
10. Основные браузеры (Top Browsers): процент трафика по браузерам за последний час.

Формирование NetFlow / IxFlow

Для выявления скрытых атак CloudLens™ с возможностями AppStack может формировать метаданные, экспортируемые как расширенный NetFlow. Кроме того, решение позволяет обогащать записи NetFlow более чем ста дополнительными расширениями. Можно определить, какие дополнительные сведения передавать средствам.

- включение географических сведений, таких как IP-регион, широта и название города. В состав дополнительных сведений, передаваемых средствам, могут входить идентификатор или название приложения, устройство и даже тип браузера;
- отчетность с учетом абонента предоставляет подробные сведения о приложении и типе мобильного телефона (устройства) мобильного пользователя;
- URL и имя узла HTTP для отслеживания веб-активности;
- метаданные HTTP и DNS для быстрого обнаружения нарушений;
- задержка транзакций (Transaction Latency) для отслеживания производительности приложений;
- сведения об угрозах;
- сведения TLS/SSL.

Геолокация и добавление тегов

Разделение трафика по местоположению: предварительно заданные параметры и обнаружение сигнатур позволяют фильтровать приложения по географическому признаку, чтобы средства могли сосредоточиться на детальной видимости. Можно быстро устранить проблему приложения на определенном удаленном объекте, точно указав местоположение и приложение, например проблемы VoIP в офисе в Великобритании. Чтобы блокировать трафик из определенных местоположений, используйте Keysight ATI Research Center: это позволяет блокировать весь трафик в недоверенные страны и из них, значительно сокращая поверхность атаки.

- направление трафика сеансов приложений подходящим средствам в вашем портфеле по региону, стране, городу и во многих случаях по широте и долготе;
- быстрая настройка фильтров без ручного написания сценариев;
- поддержка настраиваемых местоположений, например частных IP-адресов.

Data Masking Plus для номеров кредитных карт и социального страхования

Обеспечивайте соответствие стандарту безопасности данных индустрии платежных карт (Payment Card Industry Data Security Standard, PCI-DSS), HIPAA и другим нормативным требованиям с помощью предварительно заданных шаблонов данных. Поскольку по сети передаются персональные данные, безопасность имеет ключевое значение для защиты ваших потребителей и вашей организации.

- предварительно заданные шаблоны маскирования, включая номера основных кредитных карт, номера социального страхования (SSN) и адреса электронной почты;
- сокращение числа ложных срабатываний благодаря встроенной проверке номеров кредитных карт по алгоритму Луна;
- дополнительное использование стандартного маскирования данных на уровне пакетов с задаваемым пользователем смещением и любым количеством байтов.

Требования к продукту CloudLens

Требования CloudLens vTAP — v6.2.1	
Поддерживаемые среды	AWS, Azure, GCP, VMware, KVM, OpenStack, Nutanix, Kubernetes
СРУ	4 vCPU
Дисковое пространство	100 GB
Память	16 GB
Сетевое подключение	1 интерфейс
Лицензии	SUB-CL-STD, SUB-CL-ENT, SUB-CL-LEN, SUB-CL-ADD-50, SUB-CL-STD2ENT
Требования CloudLens vTap — v5.5	
Поддерживаемые среды	VMware vDS/vSS, VMware NSX/NSX-T, OpenStack, KVM, Hyper-V
СРУ	2 vCPU
Дисковое пространство	20 GB
Память	8 GB
Сетевое подключение	1 интерфейс
Лицензии	LIC-CL-VTAP-10, LIC-CL-VTAP-50, LIC-CL-VTAP-100, LIC-CL-VTAP-250, LIC-CL-VTAP-1000, LIC-CL-VTAP-NSX
Требования CloudLens vPacketStack (vPB) — v2.3	
Поддерживаемые среды	VMware, OpenStack, KVM (дополнительные сведения см. в руководстве пользователя)
СРУ	4 vCPU — процессор Haswell или более новый
Дисковое пространство	8 GB
Память	16 GB

Сетевое подключение	6 предварительно заданных интерфейсов (можно настроить после установки)
Лицензии	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	
Поддерживаемые среды	VMware, OpenStack, KVM (дополнительные сведения см. в руководстве пользователя)
СРУ	6 vCPU — процессор Westmere или более новый
Дисковое пространство	30 GB
Память	16 GB
Сетевое подключение	3 интерфейса
Лицензии	SUB-CL-AS-1-F, LIC-CL-AS-1-F

Функции продукта CloudLens

CloudLens	vTap (v6.2.1)	vTap (v5.5)	vPacketStack (v2.3 Standard)	vPacketStack (v2.3 Advanced)	vAppStack (vATIP v4.3)
Число поддерживаемых виртуальных сетевых интерфейсов	Неприменимо	Неприменимо	2	6	8
Максимальное число правил фильтрации	Не ограничено	Не ограничено	20	2000	100
Фильтрация L2–L3 (тип Eth, VLAN, IP)	Да (BPF)	Да	Да	Да	Да (IP)
Фильтрация L2–L4 (тип Eth, VLAN, IP, порты, протокол IP)	Да (BPF)	Да	–	Да	Да (IP, протокол IP)
Зеркалирование/перенаправление	Да	Да	–	–	–

Тел: +7 (495) 252-00-96

Email: info-site@akmetron.ru

Адрес: Москва, ул. Рабочая, д.93 стр.2, под. 2.

Агрегирование	–	–	Да	Да	Да
Репликация	–	–	Да	Да	Да (1 туннель GRE)
Балансировка нагрузки	–	–	–	Да	–
Дедупликация	–	–	–	Да	Да
Удаление заголовков	–	–	–	Да MPLS, FabricPath, VXLAN, PPPoE, GRE, ERSPAN, GTP, Geneve	Да GRE и ERSPAN
Усечение пакетов	–	–	–	Да	–
Маскирование данных	–	–	–	–	Да
Формирование туннелей	Да (GRE, ERSPAN, VLAN, VxLAN, Encrypted)	Да (GRE, ERSPAN, VLAN, VxLAN)	Да (GRE, ERSPAN, VxLAN)	Да (GRE, ERSPAN, VxLAN)	Да (только GRE)
Терминация туннелей	–	–	Да (GRE, ERSPAN, VxLAN)	Да (GRE, Geneve, ERSPAN, VxLAN)	Да (только GRE)
GRE, ERSPAN, VxLAN, ZT					
Фильтрация приложений	–	–	–	–	Да
Панель приложений в реальном времени	–	–	–	–	Да
Data Masking Plus	–	–	–	–	Да
Геолокация и добавление тегов	–	–	–	–	Да

NetFlow	Да	Да (NSX)	–	–	Да
IxFlow (расширенный NetFlow)	–	–	–	–	Да
Доступные партномера (подробности см. в разделе заказа)	См. «Лицензии» в таблице технических характеристик и разделе заказа	См. «Лицензии» в таблице технических характеристик и разделе заказа	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

Лицензирование продукта CloudLens

Продукт	Лицензия	Описание
vTap v6.0+	SUB-CL-STD	Ixia CloudLens Standard Edition — подписка на один (1) год; пакет включает 50 кредитов. Этот SKU действителен только для CloudLens 6.0 и более новых версий. Включена поддержка Standard.
vTap v6.0+	SUB-CL-ENT	Ixia CloudLens Enterprise Edition — подписка на один (1) год; включает 150 кредитов. Этот SKU предназначен для CloudLens 6.0 и более новых версий. Включена поддержка Standard.
vTap v6.0+	SUB-CL-LEN	Ixia CloudLens Large Enterprise and Reseller/MSP Edition — подписка на один (1) год; пакет включает 500 кредитов. Кредиты распределяются по отдельности. Для каждого активного Sensor vTap требуется 1 кредит. Этот SKU действителен только для CloudLens 6.0 и более новых версий. Включена поддержка Standard для покупателя.
vTap v6.0+	SUB-CL-ADD-50	Дополнительный пакет Ixia CloudLens включает 50 кредитов и действителен в течение одного (1) года. Используйте этот SKU, чтобы добавить 50 кредитов к редакциям CloudLens Standard или Enterprise. Требуется лицензия SUB-CL-ENT, SUB-CL-LEN или SUB-CL-STD.

Тел: +7 (495) 252-00-96

Email: info-site@akmetron.ru

Адрес: Москва, ул. Рабочая, д.93 стр.2, под. 2.

vTap v6.0+	SUB-CL-STD2ENT	Обновление Ixia CloudLens с Standard Edition до Enterprise Edition. Эта лицензия активирует дополнительные функции CloudLens Enterprise Edition и включает 100 дополнительных кредитов. При добавлении SUB-CL-STD2ENT к SUB-CL-STD заказчик получает полную функциональность CloudLens Enterprise Edition (SUB-CL-ENT) до конца срока действия.
vTap v5.5	LIC-CL-VTAP-10	Пакет Ixia из 10 лицензий включает 10 лицензий CloudLens vTap. Лицензия распространяется на число установленных служебных ВМ, или SVM (1 лицензия на SVM), и на один узел для собственных установок KVM OVS. Дополнительная плата за CloudLens Manager не взимается. Применяется ко всем VMware ESXi, Microsoft Hyper-V, KVM и OpenStack KVM. Также включает обновления ПО в течение одного (1) года, доступ к веб-порталу заказчика и техническую поддержку в течение одного (1) года в обычные рабочие часы с ответом по мере возможности.
vTap v5.5	LIC-CL-VTAP-50	Пакет Ixia из 50 лицензий включает 50 лицензий CloudLens vTap. Лицензия распространяется на число установленных служебных ВМ, или SVM (1 лицензия на SVM), и на один узел для собственных установок KVM OVS. Дополнительная плата за CloudLens Manager не взимается. Применяется ко всем VMware ESXi, Microsoft Hyper-V, KVM и OpenStack KVM. Также включает обновления ПО в течение одного (1) года, доступ к веб-порталу заказчика и техническую поддержку в течение одного (1) года в обычные рабочие часы с ответом по мере возможности.
vTap v5.5	LIC-CL-VTAP-100	Пакет Ixia из 100 лицензий включает 100 лицензий CloudLens vTap. Лицензия распространяется на число установленных служебных ВМ, или SVM (1 лицензия на SVM), и на один узел для собственных установок KVM OVS. Дополнительная плата за CloudLens Manager не взимается. Применяется ко всем VMware ESXi, Microsoft Hyper-V, KVM и OpenStack KVM. Также включает обновления ПО в течение одного (1) года, доступ к веб-порталу заказчика и техническую поддержку в течение одного (1) года в обычные рабочие часы с ответом по мере возможности.

Тел: +7 (495) 252-00-96

Email: info-site@akmetron.ru

Адрес: Москва, ул. Рабочая, д.93 стр.2, под. 2.

vTap v5.5	LIC-CL-VTAP-250	Пакет Ixia из 250 лицензий включает 250 лицензий CloudLens vTap. Лицензия распространяется на число установленных служебных ВМ, или SVM (1 лицензия на SVM), и на один узел для собственных установок KVM OVS. Дополнительная плата за CloudLens Manager не взимается. Применяется ко всем VMware ESXi, Microsoft Hyper-V, KVM и OpenStack KVM. Также включает обновления ПО в течение одного (1) года, доступ к веб-порталу заказчика и техническую поддержку в течение одного (1) года в обычные рабочие часы с ответом по мере возможности.
vTap v5.5	LIC-CL-VTAP-1000	Пакет Ixia из 1000 лицензий включает 1000 лицензий CloudLens vTap. Лицензия распространяется на число установленных служебных ВМ, или SVM (1 лицензия на SVM), и на один узел для собственных установок KVM OVS. Дополнительная плата за CloudLens Manager не взимается. Применяется ко всем VMware ESXi, Microsoft Hyper-V, KVM и OpenStack KVM. Также включает обновления ПО в течение одного (1) года, доступ к веб-порталу заказчика и техническую поддержку в течение одного (1) года в обычные рабочие часы с ответом по мере возможности.
vTap v5.5	LIC-CL-VTAP-NSX	Для развертывания CloudLens vTap в средах VMware NSX требуется дополнение Ixia CloudLens vTap для интеграции с VMware NSX. Это дополнение действительно для одного (1) NSX Manager. Оно включает 3 vTap (служебные ВМ — SVM). На каждый узел ESXi под управлением NSX требуется одна (1) SVM. Для дополнительных SVM закажите пакеты лицензий CloudLens SVM vTap.
vpB 2.3	LIC-CL-VPP-STD-1	Виртуальная обработка пакетов Ixia CloudLens с PacketStack — Standard, бессрочная лицензия, 1 экземпляр. Включает: 2 виртуальных интерфейса; NetStack: фильтрация L2–L3 (тип Eth, VLAN, IP), 20 правил; PacketStack: множественная терминция и формирование туннелей GRE. Также включает обновления ПО в течение одного (1) года, доступ к веб-порталу заказчика и техническую поддержку в течение одного (1) года в обычные рабочие часы с ответом по мере возможности.

Тел: +7 (495) 252-00-96

Email: info-site@akmetron.ru

Адрес: Москва, ул. Рабочая, д.93 стр.2, под. 2.

vpB 2.3	SUB-CL-VPP-STD-1	Виртуальная обработка пакетов Ixia CloudLens с PacketStack — Standard, 1 экземпляр. Включает: 2 виртуальных интерфейса; NetStack: фильтрация L2–L3 (тип Eth, VLAN, IP), 20 правил; PacketStack: множественная терминция и формирование туннелей GRE. Также включает обновления ПО в течение одного (1) года, доступ к веб-порталу заказчика и техническую поддержку в течение одного (1) года в обычные рабочие часы с ответом по мере возможности. Годовая лицензия. Может продаваться на несколько лет.
vpB 2.3	LIC-CL-VPP-AD-1	Виртуальная обработка пакетов Ixia CloudLens с PacketStack — Advanced, бессрочная лицензия, 1 экземпляр. Включает: 6 виртуальных интерфейсов; NetStack: агрегирование, репликация, фильтрация L2–L4 (тип Eth, VLAN, IP, порты, протокол IP), до 9999 правил, балансировка нагрузки; PacketStack: дедупликация, 12 исходящих туннелей GRE, удаление заголовков. Также включает обновления ПО в течение одного (1) года, доступ к веб-порталу заказчика и техническую поддержку в течение одного (1) года в обычные рабочие часы с ответом по мере возможности.
vpB 2.3	SUB-CL-VPP-AD-1	Виртуальная обработка пакетов Ixia CloudLens с PacketStack — Advanced, 1 экземпляр. Включает: 6 виртуальных интерфейсов; NetStack: агрегирование, репликация, фильтрация L2–L4 (тип Eth, VLAN, IP, порты, протокол IP), до 3000 правил, балансировка нагрузки; PacketStack: дедупликация, 12 исходящих туннелей GRE, удаление заголовков. Также включает обновления ПО в течение одного (1) года, доступ к веб-порталу заказчика и техническую поддержку в течение одного (1) года в обычные рабочие часы с ответом по мере возможности. Годовая лицензия. Может продаваться на несколько лет.

vAppStack (vATIP)	LIC-CL-AS-1-F	Виртуальная обработка пакетов Ixia CloudLens Private с AppStack. Полный пакет функций, 1 экземпляр, бессрочная лицензия. Включенные функции: PacketStack — терминация GRE, дедупликация; AppStack — формирование NetFlow, фильтрация приложений, геолокация и добавление тегов, маскирование данных, формирование IxFlow; SecureStack — Threat Insights. Также включает обновления ПО в течение одного (1) года, доступ к веб-порталу заказчика и техническую поддержку в течение одного (1) года в обычные рабочие часы с ответом по мере возможности.
vAppStack (vATIP)	SUB-CL-AS-1-F	Виртуальная обработка пакетов Ixia CloudLens Private с AppStack. Полный пакет функций, 1 экземпляр. Включенные функции: PacketStack — терминация GRE, дедупликация; AppStack — формирование NetFlow, фильтрация приложений, геолокация и добавление тегов, маскирование данных, формирование IxFlow; SecureStack — Threat Insights. Также включает обновления ПО в течение одного (1) года, доступ к веб-порталу заказчика и техническую поддержку в течение одного (1) года в обычные рабочие часы с ответом по мере возможности. Годовая лицензия. Может продаваться на несколько лет.

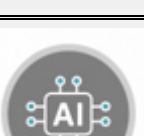
Найдите свою платформу

Стеки		
NetStack		Надёжная фильтрация, агрегация, репликация и многое другое... Узнать больше: NetStack Software Suite Keysight
PacketStack		Интеллектуальная фильтрация, модификация и транспортировка пакетов Узнать больше: PacketStack Software Suite Keysight
PacketStack +		Расширенная обработка пакетов на полной линейной скорости Узнать больше: PacketStack+ Software Suite Keysight

Тел: +7 (495) 252-00-96

Email: info-site@akmetron.ru

Адрес: Москва, ул. Рабочая, д.93 стр.2, под. 2.

Стеки		
AppStack		Контекстно-зависимая фильтрация уровня приложений на основе сигнатур Узнать больше: AppStack Software Suite Keysight
SecureStack		Оптимизированная обработка защищённого трафика Узнать больше: SecureStack Software Suite Keysight
MobileStack		Интеллектуальная видимость, адаптированная для усовершенствованного пакетного ядра мобильного оператора Узнать больше: MobileStack Software Suite Keysight
TradeStack		Управление данными рыночных потоков Узнать больше: TradeStack Software Suite Keysight
AIStack		Управление данными приложений ИИ Узнать больше: AIStack Software Suite Keysight

[Узнайте больше о решениях Keysight Visibility](#)