

AppStack

Контекстно-зависимый анализ приложений на основе сигнатур

Проблема

Сегодня сети являются самым сложным и наиболее критически важным активом для большинства предприятий. Организациям срочно требуется решение одной из крупнейших проблем, стоящих перед сетевыми администраторами, - обеспечение полной видимости сети, выходящей за рамки информации уровня 4. Например, сегодня многие приложения работают по HTTP или HTTPS в сетевой или облачной инфраструктуре и поэтому могут оставаться незаметными. Вам необходима аналитика приложений, которая предоставляет вашим средствам мониторинга нужную информацию в нужное время.

Решение

Опираясь одновременно на идентификацию статических шаблонов трафика и динамическое обнаружение приложений, AppStack предоставляет комплексное представление о том, какие приложения работают в вашей сети, какую пропускную способность они потребляют и где географически выполняются эти приложения. С помощью AppStack можно определять фильтры трафика для просмотра или перенаправления конкретных шаблонов трафика, которые требуется отслеживать, на основе типа приложения, операционной системы, транспортного протокола и других критериев. Помимо перенаправления пакетов, средствам может передаваться информация NetFlow / IPFIX / JSON, при необходимости дополненная данными уровня приложений (IxFlow), что расширяет их возможности по формированию детализированных отчетов о пользователях и приложениях.

Ключевые особенности

- Улучшение решений обеспечения видимости благодаря высокоточной идентификации приложений
- Простой интерфейс управления «наведи и щелкни» позволяет операторам легко выбирать интересующие типы трафика приложений
- Фильтрация трафика приложений для средств или обогащение предоставляемых средствам данных расширенными NetFlow/IPFIX/JSON
- Значительное улучшение платформ мониторинга за счет добавления гораздо более полного набора географической информации, сведений о приложениях и устройствах
- Сигнатуры приложений управляются и поддерживаются Keysight, что позволяет средствам автоматически расширять осведомленность по мере появления новых приложений

Сценарии использования

1. Предоставление практически значимой информации
2. Мониторинг резкого роста потребления пропускной способности приложениями
3. Отслеживание сбоев приложений
4. Выявление подозрительной активности
5. Отслеживание использования приложений по географическим регионам

Тел: +7 (495) 252-00-96

Email: info-site@akmetron.ru

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

6. Понимание влияния устройств и тенденций поведения пользователей
7. Проведение проверок на предмет безопасности, соблюдения политик и нарушений

Возможности AppStack на панели мониторинга

1. **Объем трафика (Traffic)** в реальном времени
2. **Распределение приложений (Application distribution)**, пропускная способность по каждому приложению
3. **Ведущие страны (Top Countries)** на основе наибольшего объема сформированного трафика
4. **Отображение карты мира (World view display)** с выделением стран, из которых исходит трафик
5. **Последние динамические приложения (Latest dynamic applications)** - приложения, неизвестные AppStack, позволяющие быстро сосредоточиться на потенциально вредоносных приложениях
6. **Ведущие устройства по ОС (Top Devices by OS)** с отображением агрегированного трафика по каждой ОС
7. **Ведущие приложения (Top Applications)** по агрегированному трафику каждого приложения, используемой пропускной способности, байтам и сеансам
8. **Ведущие браузеры (Top Browsers)**: это представление отображает круговую диаграмму с процентным распределением трафика по браузерам за последний час
9. **Ведущие фильтры (Top Filters)**: отображает агрегированный трафик за последние 24 часа

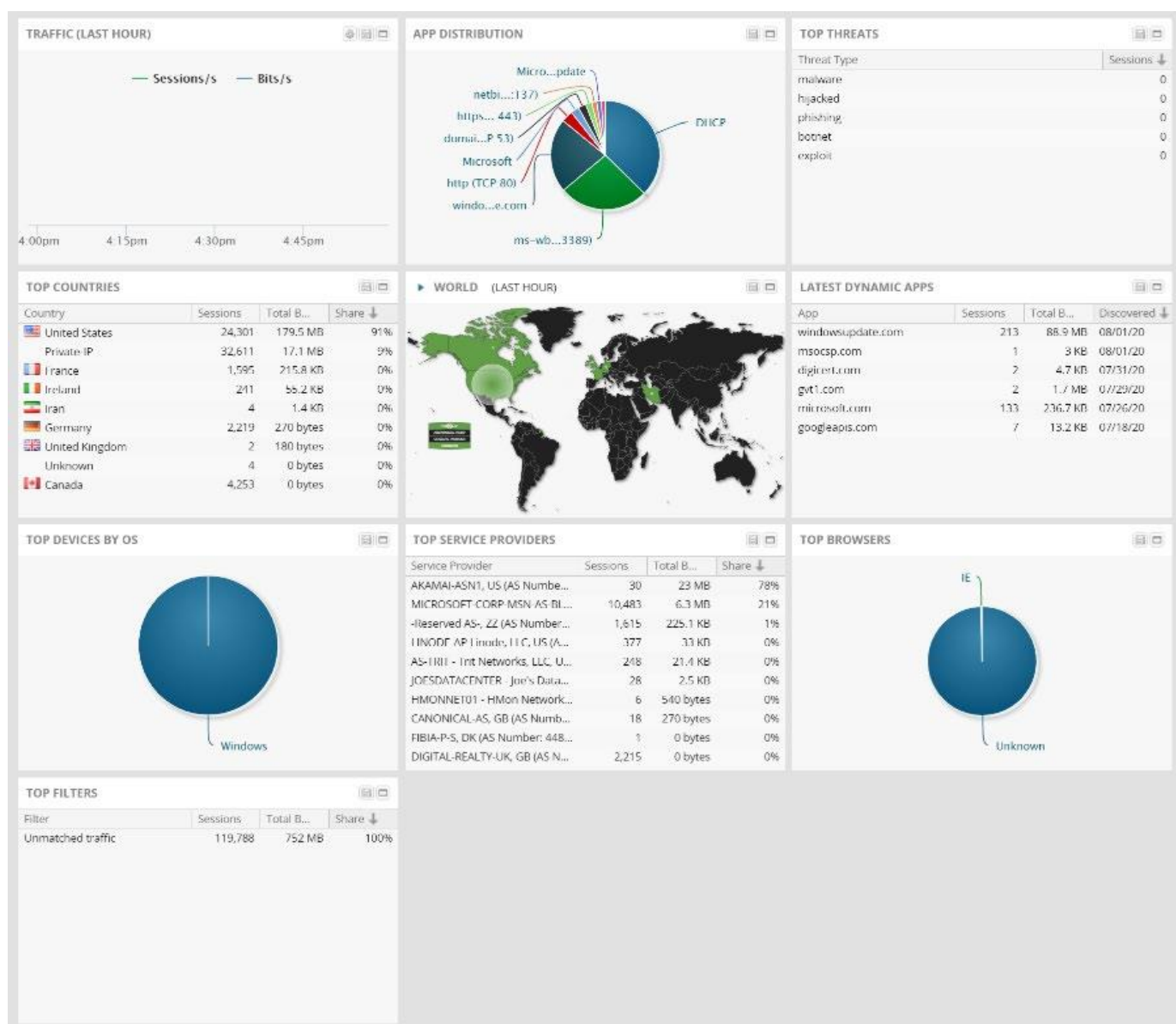


Рисунок 1. Панель мониторинга AppStack предоставляет комплексную информацию о сетевом трафике

Каждое из десяти представлений можно развернуть для отображения дополнительной информации. Например, щелчок по карте мира отображает увеличенную карту мира со списком ведущих географических регионов, формирующих сеансы серверного или клиентского трафика.

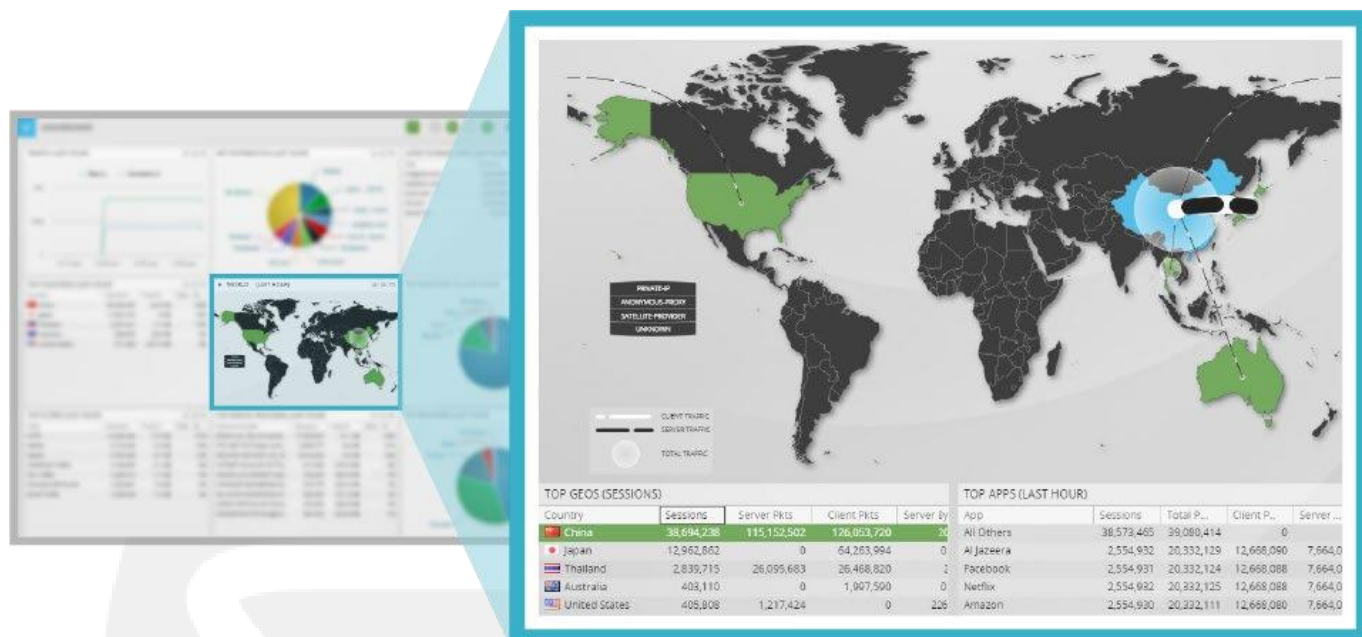


Рисунок 2. Увеличенная карта мира отображает дополнительную информацию, позволяя глубже детализировать потоки данных

Настройка фильтров приложений в простом интерфейсе «наведи и щелкни»

С помощью AppStack можно определять фильтры трафика для просмотра или перенаправления конкретных шаблонов трафика, которые требуется отслеживать, на основе типа приложения, операционной системы, транспортного протокола и других критериев. Фильтры можно объединять для создания детализированных потоков данных, повышающих точность платформ мониторинга:

- Географический признак
- Протокол/порт
- Поддействия приложений
- Группы приложений
- IP-адрес
- Приложение
- Сопоставление с регулярными выражениями
- Трафик SSL/TLS

Point and Click
Filter settings

Geographic Matching
Click map or country name



Рисунок 3. AppStack предоставляет подробную информацию о приложениях и позволяет фильтровать по группам приложений, категориям, типу поставщика, транспорту и другим параметрам!

Например, с помощью функции географической фильтрации можно быстро настроить фильтр, отображающий трафик из определенных стран.

AppStack позволяет объединять любое количество условий фильтрации для создания представлений, важных для вас и вашей организации. Например, можно использовать тот же фильтр и выбрать отображение только определенных данных приложений из этих стран, например только трафика с устройств на базе Android, простым щелчком мыши.



Рисунок 4. Простой интерфейс «наведи и щелкни» позволяет создать новый фильтр, выявляющий весь трафик из Китая, Ирана и Саудовской Аравии

Тел: +7 (495) 252-00-96

Email: info-site@akmetron.ru

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

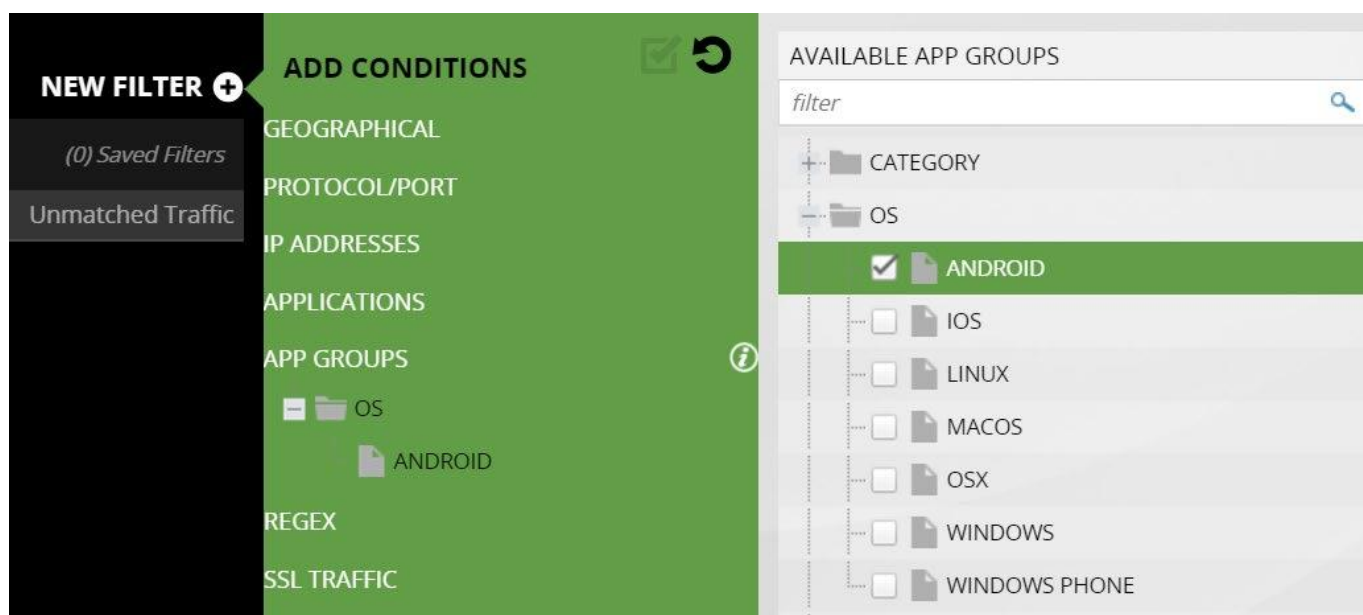


Рисунок 5. Выбор всего трафика устройств на базе Android

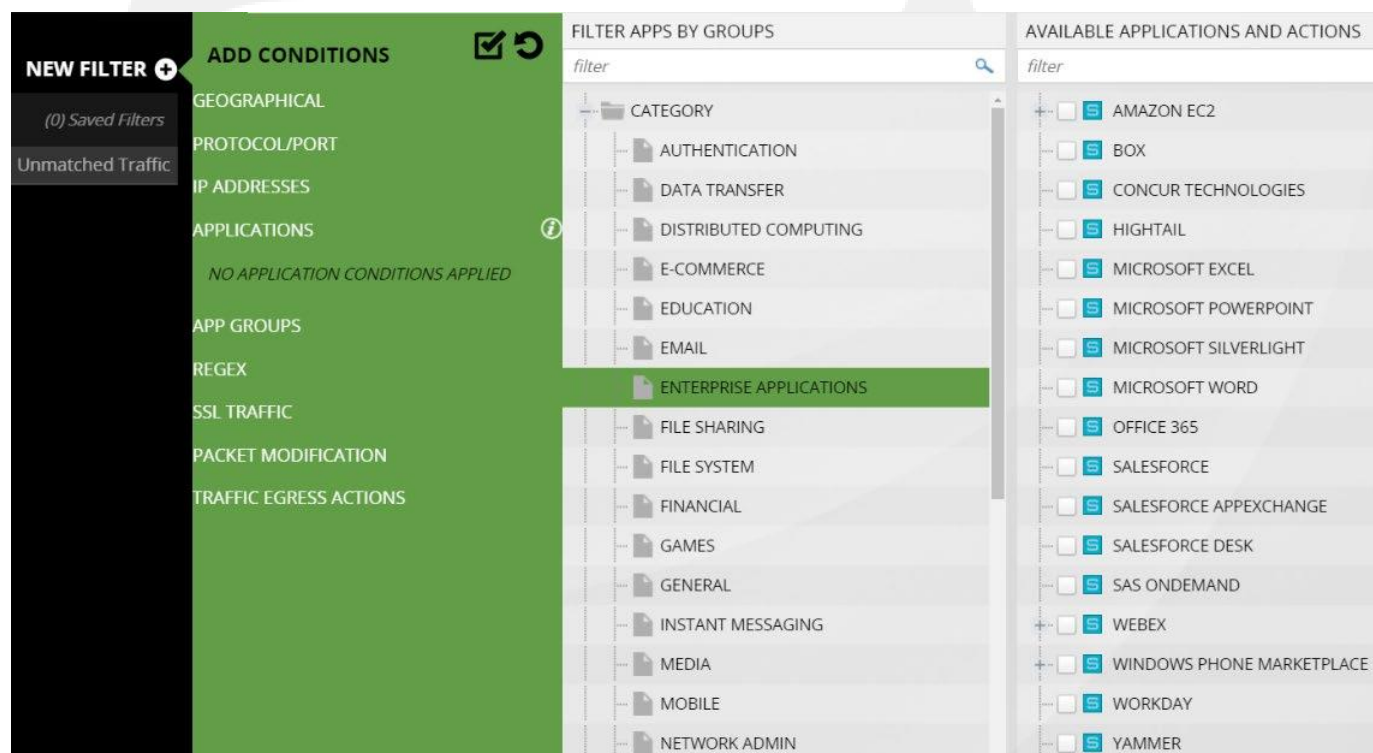


Рисунок 6. Фильтрация по группе приложений обеспечивает быстрый и простой выбор фильтра; в данном случае - всех типов корпоративных приложений

Тел: +7 (495) 252-00-96

Email: info-site@akmetron.ru

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

Группы приложений позволяют быстро выбирать распространенные группы трафика приложений

Вместо указания нескольких различных приложений можно задать для фильтрации целую группу приложений. Например, вместо выбора отдельных корпоративных приложений, в частности всех приложений Microsoft Office, можно просто выбрать «Корпоративные приложения», которые охватывают их и многие другие приложения.

Основные функции

Функция	Назначение
 Идентификация приложений	AppStack компании Keysight обнаруживает приложения по сигнатурам: статическим, динамическим и даже пользовательским с помощью технологии, патентная заявка на которую находится на рассмотрении. • Идентификация и/или фильтрация приложений по сигнатуре, браузеру, ОС, IP-адресу и географическому местоположению с перенаправлением в соответствующие средства безопасности • Быстрое разделение потоков трафика по типу приложения - видео, электронная почта, веб или другое, - устройству, ОС и оператору связи • Возможность обнаруживать неизвестные приложения и добавлять распространенные приложения по запросу • Мониторинг и отчетность по потреблению пропускной способности ведущими приложениями и странами • База данных, содержащая более 1000 приложений и регулярно пополняемая новыми приложениями • Сопоставление с регулярными выражениями (RegEx) не требуется
 Геолокация и маркировка	Разделение трафика по местоположению: предварительно определенные параметры и обнаружение по сигнатурам позволяют фильтровать приложения по географическому признаку, чтобы средства могли выполнять подробный анализ с близкого расстояния. • Перенаправление трафика сеансов приложений по региону, стране, городу, а во многих случаях - по широте/долготе, в соответствующие средства вашего набора • Быстрая настройка фильтров без необходимости ручного написания сценариев • Поддержка пользовательских местоположений, например частных IP-адресов

 Необязательный RegEx	Хотя это и не требуется, для дополнительного контроля и настройки можно применять сопоставление с регулярными выражениями (RegEx). Что еще важнее, его можно использовать совместно со всеми другими интеллектуальными фильтрами, обеспечивая одновременно простоту применения и точность критериев. • Наложение RegEx на действительно интеллектуальные функции фильтрации приложений, геолокации и маркировки • Предварительно определенные совпадения для идентификационного номера налогоплательщика, номеров телефонов и распространенных кредитных карт • Выделение электронных писем из потенциально скомпрометированных учетных записей
 NetFlow	Keysight позволяет обогащать записи NetFlow расширениями, повышающими их ценность. Вы можете определить, какую дополнительную информацию отправлять вашим средствам. • Включение географической информации, например IP-адреса региона, широты и названия города. Идентификатор или название приложения, устройство, браузер и даже шифр SSL/TLS могут входить в дополнительную информацию, отправляемую средствам. • Отчетность с учетом абонента предоставляет сведения о приложении и типе мобильного устройства для пользователей мобильной связи • URL-адрес HTTP и имя хоста для отслеживания веб-активности • Метаданные HTTP и DNS для быстрого обнаружения нарушений безопасности • Задержка транзакций для отслеживания производительности приложений
	Позвольте Keysight формировать NetFlow/IPFIX без нагрузки на маршрутизаторы и другие сетевые устройства. • Одновременное формирование NetFlow, дешифрование SSL/TLS и перенаправление приложений • Расширенная статистика NetFlow, включая счетчики отброшенных пакетов при достижении пиковой загрузки CPU • Высокопроизводительный режим: может формировать записи NetFlow для более чем 300 тыс. сеансов TCP в секунду • Поддержка формирования NetFlow v9 и v10/IPFIX, а также данных JSON • Поддержка до 10 коллекторов NetFlow Эмуляция устройства для разгрузки маршрутизатора с передачей исходных ODID и идентификатора интерфейса устройства

 Захват пакетов	Устраняете неполадки соединений VoIP из офиса в Германии? Возникла повторяющаяся проблема, причину которой необходимо установить? Быстро захватите эти соединения и проанализируйте их. Возможность захвата пакетов позволяет быстро и легко настроить фильтр и получить любой необходимый фрагмент трафика - из конкретной страны, приложения, браузера, устройства и т. д. - прямо у вас под рукой. • Быстрая проверка конфигурации фильтра путем захвата и проверки данных • Захват до 10 выборок с окном выборки 100 МБ для каждой • Простая загрузка на ноутбук/рабочую станцию для анализа • Возможность захвата пакетов на линейной скорости 30GE
 Интеллектуальный анализ приложений	Подписка на интеллектуальный анализ приложений предоставляет обновления базы сигнатур приложений, необходимые для поддержания актуальности AppStack по мере появления новых приложений, что повышает точность определения известных и неизвестных типов приложений. Эта услуга также включает обновления картографических данных геолокации, обеспечивая актуальность названий стран и городов при любых изменениях. Фильтры, использующие группы приложений, будут автоматически расширяться за счет новых приложений, которые по мере появления относятся к этим группам.
 Панель мониторинга в реальном времени	Панель мониторинга AppStack отображает комплексную информацию о сетевом трафике в девяти представлениях, предоставляющих сведения о сетевом трафике в реальном времени. Она содержит девять представлений, предоставляющих сведения о сетевом трафике в реальном времени, такие как объем трафика, пропускная способность, используемая различными приложениями в сети, приложения, создающие наибольший объем трафика, и многое другое.

Дополнительные функции

Функция	Назначение
Режим, соответствующий требованиям FIPS Министерства обороны США	Когда включены политики безопасности уровня Министерства обороны США, AppStack ограничивает пользователя одним сеансом HTTPS, а сеансы, превышающие заданный пользователем период бездействия, аннулируются.

Доступность и информация для заказа

AppStack доступен для Keysight [Vision X](#), [Vision ONE](#), Vision 7300 (снята с производства) и [CloudLens](#).

	Vision ONE	Vision X
Требования к базовой платформе	Готовый сетевой пакетный брокер Keysight со встроенными возможностями AppStack Шасси (варианты) SYS-V1-48PX-AC SYS-V116PX8PGAC-2 SYS-V1-48PX-DC SYS-V116PX8PGDC	Сетевой пакетный брокер Keysight максимальной емкости Шасси SYSVX-BASE-AC SYSVX-BASE-DC Модуль MVX-AM4PC: модуль приложений Keysight Vision X с (4) портами 100G; лицензии на порты и функции продаются отдельно (991-8102)



Все функции AppStack Внеполосное дешифрование SSL/TLS (SecureStack) Data Masking Plus (SecureStack)	Полная подписка - активация аппаратных средств и функции SUB-V1-SSAS: годовая подписка Keysight Vision ONE на SecureStack (внеполосное дешифрование SSL/TLS) и лицензия AppStack. Включает внеполосное дешифрование SSL/TLS и все функции AppStack, в том числе подписку на интеллектуальный анализ приложений. (993-0113) SUB-V1-SSAS-APFL: годовая лицензия подписки AppStack для Keysight Vision ONE. Включает фильтрацию приложений, маскирование и RegEx. Количество (1) на систему (993-0334) SUB-V1-SSAS-NTFL: годовая лицензия подписки AppStack для Keysight Vision ONE на формирование метаданных (993-0335) Бессрочная лицензия LIC-V1-APFL: бессрочная лицензия фильтрации приложений AppStack для Keysight Vision ONE, включающая фильтрацию приложений, маскирование и RegEx. Количество (1) на систему (993-0330) LIC-V1-NTFL2: бессрочная лицензия функции формирования метаданных AppStack для Keysight Vision ONE - количество (1) (993-0331)	Полная подписка SUB-VX-SSAS: годовая подписка Keysight Vision X на функцию AppStack. Лицензируется для одного (1) CPU на модуле MVX-AM4PC; максимум (2) на модуль (993-9613) SUB-VX-SSAS-APFL: годовая лицензия подписки AppStack для Keysight Vision X. Включает фильтрацию приложений, маскирование и RegEx. Один (1) экземпляр CPU (993-0336) SUB-VX-SSAS-NTFL: годовая лицензия подписки AppStack для Keysight Vision X на формирование метаданных. Один (1) экземпляр CPU (993-0337) Бессрочная лицензия LIC-VX-SSAS: бессрочная функция AppStack для Keysight Vision X; лицензируется для одного (1) CPU на модуле MVX-AM4PC; максимум (2) на модуль (993-9611) LIC-VX-SSAS-APFL: бессрочная лицензия AppStack для Keysight Vision X. Включает фильтрацию приложений, маскирование и RegEx. Один (1) экземпляр CPU (993-0032) LIC-VX-SSAS-NTFL: бессрочная лицензия AppStack для Keysight Vision X на формирование метаданных. Один (1) экземпляр CPU (993-0333) LIC-VX-MSMD: поддержка формирования метаданных MobileStack для Keysight Vision X на шасси с модулями MVX-AM4PC; максимум 1 на шасси
--	---	--

	Активация аппаратных средств LIC-V1-SSAS-E: лицензия активации аппаратных средств Keysight Vision ONE для SecureStack (внеполосное дешифрование SSL/TLS) и AppStack с производительностью начального уровня - количество (1) (993-0101) LIC-V1-SSAS-F: лицензия активации аппаратных средств Keysight Vision ONE для SecureStack (внеполосное дешифрование SSL/TLS) и AppStack с полной производительностью - количество (1) (993-0102) LIC-V1-SSAS-U: лицензия обновления активации аппаратных средств Keysight Vision ONE для включения возможностей SecureStack (внеполосное дешифрование SSL/TLS) и AppStack (переход от начальной к полной производительности) - количество (1). Требуется дополнительные лицензии на функции (993-0104)	Лицензия на аппаратные средства/панель мониторинга
 Идентификация приложений	SUB-V1-APTL2: годовая лицензия подписки AppStack для Keysight Vision ONE. Включает идентификацию и фильтрацию приложений, геолокацию и маркировку, поток данных интеллектуального анализа приложений - количество (1) (993-0112)	SUB-VX-APTL: годовая подписка Keysight Vision X; включает обновление сигнатур AppStack, количество (1) на систему (993-9612)
Комплекты: система + лицензии	SYS-V14PX16PGAC SYSV1FC8PX4P4XAC	
	Vision 7300	CloudLens

Требования к базовой платформе	Сетевой пакетный брокер Keysight максимальной емкости Шасси SYS7300-STD SYS7303-STD Модуль M7300-SSAS-48PX: модуль семейства Keysight Vision 7300 для предоставления возможностей AppStack и SecureStack (SSL/TLS) - с 48 портами SFP+ (992-0050)	Платформа Keysight для обеспечения видимости общедоступного, частного и гибридного облака Виртуальное подключение к трафику (варианты) LIC-CL-VTAP-10 LIC-CL-VTAP-50 LIC-CL-VTAP-100 LIC-CLVTAP-250 LIC-CL-VTAP-1000 SUB-CL-VTAP-1000 SUB-CL-VTAP-CSMP SUB-CL-VTAP-AG100 SUB-CL-VTAP-AG250 SUB-CL-VTAP-AG1000
 Все функции AppStack  Внеполосное дешифрование SSL/TLS (SecureStack)  Data Masking Plus (SecureStack)	Полная подписка SUB-7300-SSAS: годовая подписка Keysight Vision 7300 на SecureStack (внеполосное дешифрование SSL/TLS) и лицензия AppStack для M7300-SSAS-48PX. Включает дешифрование SSL и все функции AppStack, в том числе подписку на интеллектуальный анализ приложений. (993-0049) Бессрочная лицензия LIC-7300-APPS: бессрочная дополнительная лицензия AppStack для Keysight Vision 7300 на фильтрацию приложений, NetFlow, IxFlow, маскирование, RegEx и внеполосное дешифрование SSL/TLS. Количество (1) на линейную плату (993-0140) Лицензия на аппаратные средства/панель мониторинга	Подписка (без дешифрования SSL) SUB-CL-AS-1-F: Keysight CloudLens Private с AppStack. Полный пакет функций, подписка на первый год, 1 экземпляр (954-4064) 909-5021: подписка Keysight на продление SUB-CL-AS-1-F. Виртуальная обработка пакетов CloudLens Private с функциями AppStack (909-5021) Бессрочная лицензия LIC-CL-AS-1-F: Keysight CloudLens Private с AppStack. Полный пакет функций, бессрочная лицензия, 1 экземпляр (954-4065)

	LICS-7300-SSAS-F: лицензия Keysight Vision 7300 на панель мониторинга AppStack с полной производительностью - количество (1) на линейную плату (993-0141)	
 Идентификация приложений	SUB-7300-APTL: лицензия подписки AppStack для Keysight Vision 7300 на первый год, требуемая для каждой линейной платы. Включает обновления сигнатур приложений. Количество (1) (993-0077)	
 Захват пакетов	Аппаратные средства M7300PCM-48PX: модуль захвата пакетов (Packet Capture Module, PCM) семейства Keysight Vision 7300 - линейная плата, обеспечивающая захват пакетов, - с 48 портами SFP+ (992-0051)	

Технические характеристики M7300-SSAS-48px

Общие характеристики

Производительность	Управление
• Все порты являются двунаправленными и полностью не блокирующими • Полная линейная скорость на всех портах при включенной фильтрации	• Поддержка SNMP v1, v2, v3 • Поддержка локальной аутентификации, RADIUS и TACACS+ (участники и группы) • Функции детального управления доступом • Мониторинг и регистрация событий • Syslog • Управление автоматизацией ИТ через веб-API

Физические характеристики

Механические параметры	Электропитание и тепловыделение
- Интерфейсная плата высотой 1U для 19-дюймового шасси - Размеры: 17,5 (Ш) x 15 (Д) x 1,75 (В) дюйма - Масса: 17,0 фунта (7,7 кг)	- Рабочее входное напряжение: от -40 до -60 В пост. тока - Номинальный ток: 4,15 А при -53 В пост. тока, 220 Вт - Максимальный рабочий входной ток: 5,5 А при 40 В пост. тока, макс. 220 Вт - Тепловыделение/рассеивание мощности модуля при 100% нагрузке трафиком: максимум 220 Вт / 751 БТЕ/ч

Условия эксплуатации

Температура	Влажность
- Рабочая: от 5 °C до 40 °C - Кратковременно*: от -5 °C до 55 °C (*не более 96 часов подряд) - Кратковременно* при отказе вентилятора: от -5 °C до 40 °C (*не более 96 часов подряд)	- Рабочая: от 5% до 85% (без конденсации) - Кратковременно*: от 5% до 90% (без конденсации) (*не более 96 часов)

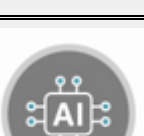
Найдите свою платформу

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](#)