AppStack

Context-Aware, Signature-Based Application Intelligence

Problem

Networks are the most complex and critical asset to enterprises today. Organizations urgently need a solution to one of the biggest challenges facing network administrators – complete network visibility that extends past Layer 4 information. For example, many applications today run over TLS or QUIC encrypted connections within network or cloud infrastructures and thus can be obscured. You need application intelligence that serves your monitoring tools the right information at the right time.

Solution

Relying on both static traffic pattern identification and dynamic application discovery, AppStack provides a comprehensive view of which applications are running within your network, what their users and KPIs are and where these applications are running geographically. Using AppStack, you can define traffic filters to view or forward specific traffic patterns that you want to monitor, based on application type and other Layer 2-7 criteria. In addition to packet forwarding, flow-based and AI-ready metadata, enhanced with application layer and subscriber-aware data (IxFlow), can be sent to tools, enhancing their capability to report granular and consolidated user and application data for fixed and mobile networks.

Highlights

- Improves visibility solutions through highly accurate application identification
- Simple point-and-click management interface allows operators to simply select application traffic types of interest
- Filter application traffic to tools or enhance data provided to tools with enhanced metadata
- Greatly improves monitoring platforms by adding a much richer set of geographical, application, KPI and device information
- Application signatures are managed and maintained by Keysight, allowing tools to expand awareness automatically as new applications come online
- In conjunction with MobileStack, improves service provider network monitoring and AI/ML engine analysis with enhanced subscriber aware metadata

KEYSIGHT

Use Cases

1. Deliver actionable information
2. Monitor application bandwidth explosion
3. Track application Key Performance Indicators
4. Identify suspicious activity
5. Track application usage by geography, subscriber or radio network
6. Understand device impacts and user trend behavior
7. Conduct audits for security, policy and compliance
8. Deliver application aware metadata to application monitoring solutions
9. Provide AI-ready metadata to AI/ML analysis and model training

The AppStack Capabilities from the Dashboard

1. **Traffic** volume in real time
2. **Application distribution**, per-application bandwidth
3. **Top Countries** based on the largest amount of traffic generated
4. **World view display**, with countries that originate traffic highlighted
5. **Latest dynamic applications**, which are applications learned by AppStack based on identifiable traffic patterns
6. **Top devices by OS** displayed by aggregated per-OS traffic
7. **Top service providers** by aggregated per-AS number, by used bytes and sessions
8. **Top browsers:** This view displays a pie chart showing the per-browser traffic percentage for the last hour
9. **Top filters:** Displays the aggregated traffic per filter for the last 24 hours



Figure 1. The AppStack dashboard provides comprehensive network traffic information

Each of the 9 views can be expanded to show additional information, for instance, clicking the world view shows an enlarged world map, with a list of the top geographies that generate server or client traffic sessions.

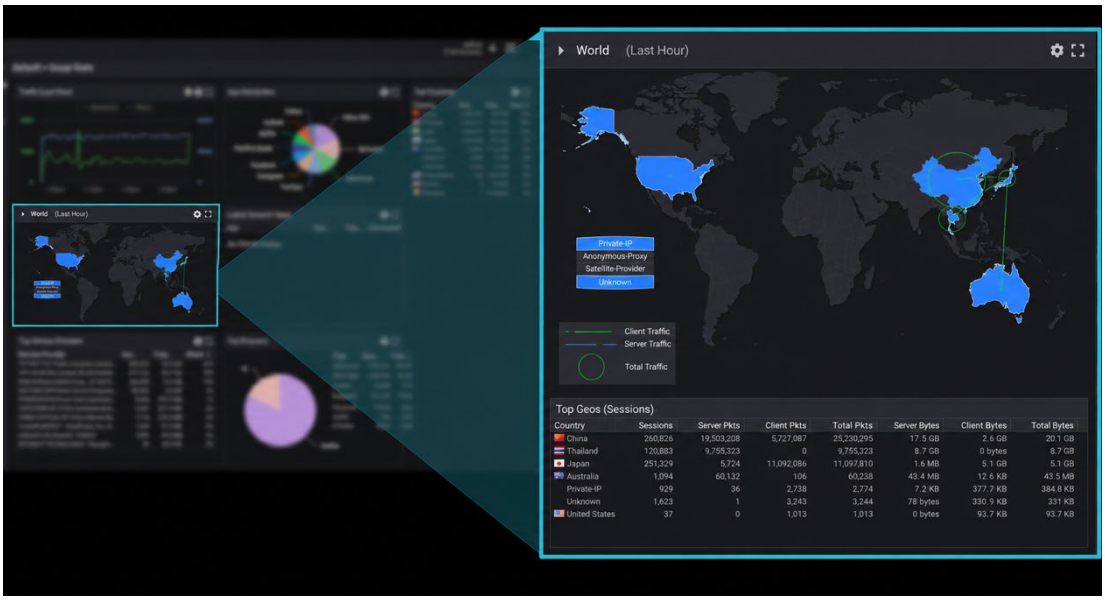


Figure 2. Enlarged world map shows additional information allowing deeper drill down into data flows

Set Up Application Filters Within a Simple Point-and-Click Interface

Using AppStack, you can define traffic filters to view or forward specific traffic patterns that you want to monitor, based on application details, RegEx and other criteria. Filters can be combined to create detailed data flows that improve monitoring platform accuracy:

- Geographical
- Protocol/Port
- Application
- Application Groups
- SSL/TLS Traffic
- VLAN
- IP Address
- Application Sub-actions
- Regular Expression Matching

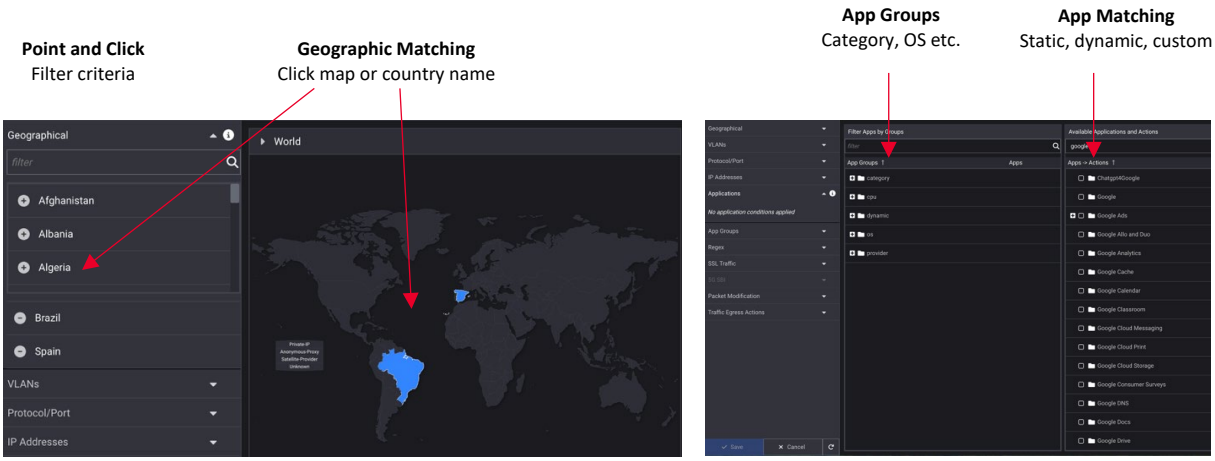


Figure 3. AppStack provides detailed flow intelligence, allowing filtering by country, application and more

AppStack allows the combination of any number of filter conditions.

AppStack is a session-oriented engine, therefore when it matches a packet, it filters the entire TCP, UDP or SCTP connection containing that packet. With optional buffering, all the packets in the connection before the match occurred can also be filtered.

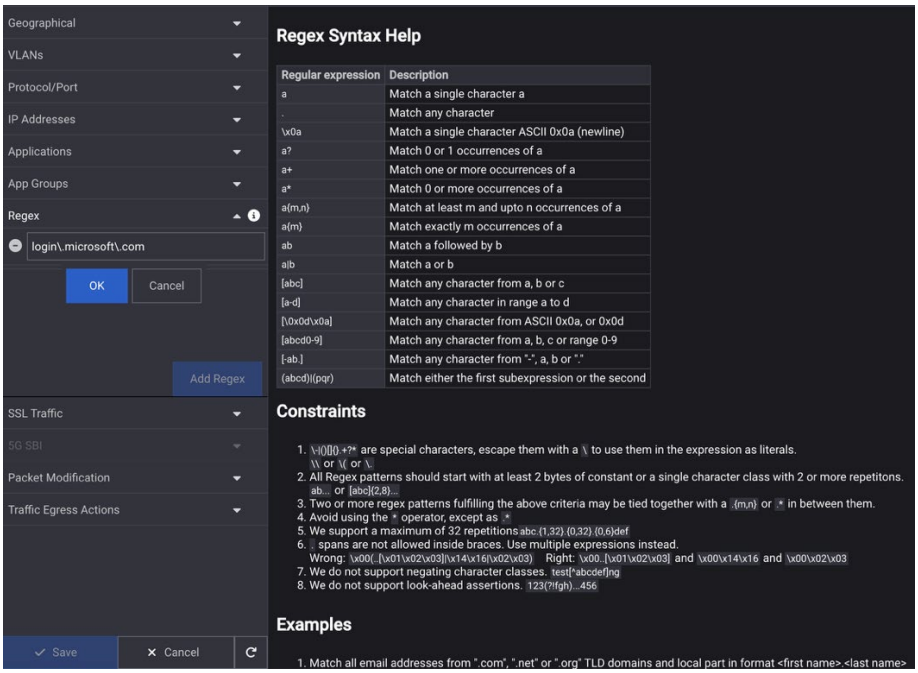


Figure 4. Filtering by Regular Expressions (RegEx) allows session-aware matching of entire connections containing specified keywords, phrases or expressions

Empower AI-enabled Analytics Tools with Application and Subscriber-aware Metadata

AppStack transforms raw network telemetry into **AI-ready, application- and subscriber-aware metadata** that is purpose-built for advanced analytics platforms and machine-learning pipelines.

AppStack generates **granular metadata exports**, allowing analytics tools to access per-flow attributes and protocol fields when fine-grained inspection or forensic analysis is required.

AppStack can optionally **aggregate and enrich** flow-level data across L4–L7, consolidating millions of individual connections into compact, high-signal records keyed by meaningful entities such as application name, client or server IP, and mobile subscriber identifiers like IMSI. This *smart data* approach dramatically reduces noise and data volume while preserving behavioral context, enabling AI systems to reason about patterns, distributions, and anomalies rather than isolated flows. Integrated aggregation profiles, statistical summaries, and temporal KPIs allow external analytics engines—such as NetFlow consumers and AI-driven observability tools—to ingest metadata that is already contextualized, normalized, and optimized for fast inference and explainability. As a result, AppStack empowers AI-enabled analytics tools to deliver deeper insights into application performance, subscriber behavior, and network health with lower processing cost and higher analytical value.

Granular Metadata
Standard NetFlow and enriched IxFlow fields

Aggregated Metadata
Field information consolidated per key

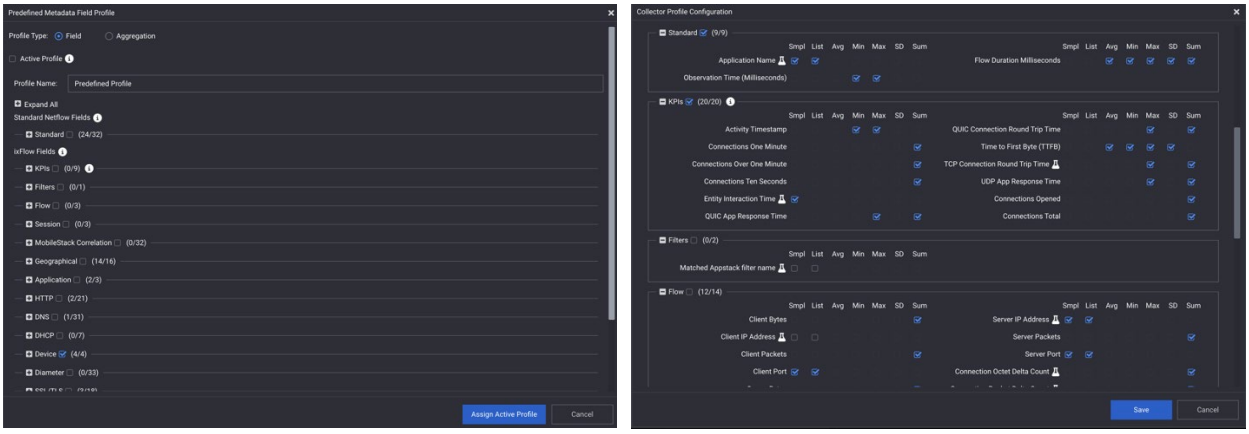


Figure 5. Metadata can be generated granularly per flow or aggregated per essential entities (keys) such as IMSI, Server Name Indication or others.

Key Features

Feature	Function
 Application Identification	Keysight's patented technology detects applications through signatures: static, dynamic or customized. • Application identification and/or filtering based on signature elements for HTTPS (TLS, SSL), QUIC, HTTP, DNS, IP address and more • Monitor and report top applications' and countries' bandwidth consumption • Database of >2400 static applications, that is regularly updated • Up to 2000 additional applications learned dynamically, helping identify unknown services or potentially unwanted connections • Custom signatures to detect and filter non-mainstream, proprietary, in-house or experimental applications
 Geolocation and Tagging	Separate traffic by location – IP geolocation allows for traffic filtering based on geography so tools can zoom in for close-range visibility. • 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
 Optional RegEx	Though not required, regular expression matching (RegEx) can be used for additional control and customization. More importantly, it can be used in conjunction with all the other smart filters to offer both ease of use and preciseness of criteria. • Layer RegEx over the truly intelligent application filtering, geolocation and tagging features • Predefined matches for Taxpayer ID, phone numbers, and common credit cards • Isolate emails from potentially compromised accounts
 Data Masking Plus (SecureStack)	Protect sensitive user data by dynamically masking selected fields, such as IP address, credit card and Social Security Numbers, while preserving protocol integrity. • Enables secure sharing of traffic data for analytics, without exposing confidential information. • Predefined payload masks for major credit cards
 IxFlow	Keysight allows you to enrich NetFlow records with value-add extensions. You can determine what additional information to send to your tools. • Include geographical information such as region IP, lat./long. and city name. • Application ID or name, device, browser and SSL/TLS JA3/JA4 fingerprint as part of extra information sent to metadata collectors. • Subscriber-aware reporting provides detail on application, KPI, network-based location, GTP tunnel information and handset (device) type for mobile users • HTTP URL and hostname for cleartext web activity tracking • HTTP and DNS metadata for rapid breach detection • HTTPS and QUIC header metadata for encrypted application intelligence
 Metadata	Let Keysight generate the metadata without burdening routers and other network devices. • Simultaneous metadata generation, RegEx/Data Masking+ and Application forwarding • Rich metadata stats per collector • High performing mode – can produce NetFlow records for over 300K TCP sessions/second • Supports generation of NetFlow v9 and v10 (IPFIX), JSON, AVRO and HTTP data

	• Supports up to 10 metadata collectors per AppStack instance • Device emulation for router offload, while reporting original device's ODID and Interface ID
 Packet Capture	Troubleshooting VoIP connections from your office in Germany? Have a repeated issue you need to get to the bottom of? Quickly capture those connections and analyze. With the Packet Capture capability, it is quick and easy to setup a filter and get any slice of traffic you need – from a specific country, application, device, and more – right at your fingertips. • Quickly verify filter configuration by capturing and validating data • Capture up to 10 samples with 2GB sampling window each • Easily download to a laptop/workstation for analysis • Packet capture capability at 30Gbps rate (Vision ONE) or 50Gbps (Vision 400 / Vision X instance)
 Application Intelligence	Application intelligence subscription provides updates to application signature database, vital for AppStack to stay updated with emerging applications which increases the accuracy of known and new application types. This service also includes updates to Geolocation map data, ensuring country and city name data are updated with any changes. Filters that utilize Application Groups will automatically expand to new applications that fall into those groups as they come online.
 Real-time Dashboard	The AppStack Dashboard displays comprehensive network traffic information within nine views that provide real-time network traffic information. It contains nine views that provide real-time network traffic information, such as traffic volume, bandwidth used by the different applications running on the network, the applications that generate most traffic, and more.

Additional Features

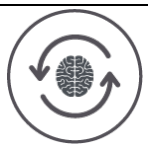
FIPS DOD Compliant Mode	When the DoD-level security policies are enabled, AppStack restricts a user to a single https session and sessions that exceed a user defined inactivity period are invalidated.

Availability and Ordering Information

AppStack is available for Keysight Vision ONE, Vision X, Vision 400 and CloudLens

	Vision ONE	Vision X
	Keysight's turnkey network packet broker	Keysight's highest processing capacity network packet broker
Baseline Platform Requirements	**Chassis** • SYS-V1-48PX-AC • SYS-V1-48PX-DC **Module** • **MV1-VAM**: Keysight Vision ONE Visibility Application Module, for use in Vision ONE Network Packet Broker (992-0142)	**Chassis** • SYSVX-BASE-AC • SYSVX-BASE-DC **Module** • **MVX-AM4PC:** Keysight Vision X, App Module (4) port 100G module; Port and feature licenses sold separately (991-8102)
 All AppStack Features	**Perpetual** • **LIC-V1-APPS2:** Keysight Vision ONE, AppStack perpetual license for App Filtering, NetFlow, IxFlow, Masking and Regex; Licensed for the Vision ONE Visibility Application Module (993-9618)	**Subscription** • **SUB-VX-SSAS:** Keysight Vision X, One (1) year AppStack feature subscription. Licensed for one (1) CPU on MVX-AM4PC module; Max (2) per module (993-9613) • **SUB-VX-SSAS-APFL:** Keysight Vision X AppStack one year subscription license. Includes App Filtering, Masking and Regex. One (1) CPU instance (993-0336) • **SUB-VX-SSAS-NTFL:** Keysight Vision X AppStack one year subscription license for MetaData generation. One (1) CPU instance (993-0337) **Perpetual** • **LIC-VX-SSAS:** Keysight Vision X, AppStack perpetual feature; Licensed for one (1) CPU on MVX-AM4PC module; Max (2) per module (993-9611) • **LIC-VX-SSAS-APFL:** Keysight Vision X AppStack perpetual license. Includes App Filtering, Masking and Regex. One (1) CPU instance (993-0032) • **LIC-VX-SSAS-NTFL:** Keysight Vision X AppStack perpetual license for MetaData generation. One (1) CPU instance (993-0333) • **LIC-VX-MSMD**: Keysight Vision X, MobileStack Metadata Generation support per chassis on MVX-AM4PC modules; Max 1 per chassis; requires MobileStack correlation license

	Vision ONE	Vision X
 Application Updates	• **SUB-V1-APTL2:** Keysight Vision ONE AppStack Application Intelligence updates, one year subscription license. Includes application signature updates. QTY (1) per system (993-0123)	• **SUB-VX-APTL:** Keysight Vision X, One (1) year subscription; Includes AppStack signature update, QTY (1) per system (993-9612)
Bundles: System + Licenses	• SYS-V116PX8PGAC • SYS-V116PX8PGDC • SYS-V14PX16PGAC-2 • SYSV1FC8PX4P4XAC	

	Vision 400	CloudLens
	Keysight's all-in-one 400G network packet broker with AppStack capabilities built-in	Keysight's platform for public, private and hybrid cloud visibility
Baseline Platform Requirements	**Chassis** • SYS-V400-BASE-AC • SYS-V400-BASE-DC	
 All AppStack Features	**Subscription** • **SUB-V400-AS-SSAS:** Keysight Vision 400 one year subscription for fully featured AppStack with 50Gbps throughput. Supported from NVOS 6.4.1 and AppStack 4.9. (993-0363) • **SUB-V400-AS-APFL**: Keysight Vision 400 one year subscription for AppStack Application Filtering feature with 50Gbps throughput. Supported from NVOS 6.4.1 and AppStack 4.9. (993-0311) • **SUB-V400-AS-NTFL**: Keysight Vision 400 one year subscription for AppStack Meta Data generation feature with 50Gbps throughput. Supported from NVOS 6.4.1 and AppStack 4.9. (993-0314) **Perpetual** • **LIC-V400-AS-SSAS**: Keysight Vision 400 AppStack perpetual feature; Fully featured AppStack with 50Gbps throughput. Supported from NVOS 6.4.1 and AppStack 4.9. (993-0362) • **LIC-V400-AS-APFL**: Keysight Vision 400 AppStack Application Filtering perpetual feature with 50Gbps throughput. Supported from NVOS 6.4.1 and AppStack 4.9. (993-0303) • **LIC-V400-AS-NTFL**: Keysight Vision 400 AppStack Meta Data generation perpetual feature with 50Gbps throughput. Supported from NVOS 6.4.1 and AppStack 4.9. (993-0305)	**Subscription** • **SUB-CL-AS-1-F:** Keysight CloudLens Private with AppStack. Full Feature pack, first year subscription, 1 instance (954-4064) • **909-5021:** Keysight renewal subscription for SUB-CL-AS-1-F. CloudLens private virtual packet processing with AppStack features (909-5021) **Perpetual** • **LIC-CL-AS-1-F:** Keysight CloudLens Private with AppStack. Full Feature pack, perpetual license, 1 instance (954-4065)
 Application Updates	• **SUB-V400-AS-APTL:** Keysight Vision 400 one year subscription for AppStack signature updates per device. Supported from NVOS 6.4.1 and AppStack 4.9.(993-0312)	

Specifications for MVX-AM4PC

General Specifications

Performance

- All ports are bidirectional and fully non-blocking
- Full line-rate across all ports with filtering enabled

Multi-Speed Support (per module)

- 4 x 100G QSFP28 front panel packet broker ports
- Speeds supported
  - 1 x 100G
  - 2 x 50G
  - 1 x 40G
  - 4 x 25G
  - 4 x 10G

Physical Specifications

Card Size and Weight

- Height= 1.75"
- Width= 9"
- Depth= 19.5"
- Weight= 9.47lb

Power (for Vision X)

AC Power

- Quad hot swappable AC power supplies
- Input AC Voltage: 90 – 240 VAC RMS
- Maximum power, each power supply
  - 100 VAC input – 1260W
  - 110-120 VAC input – 1400W
  - 200-240 VAC input – 1500W
- Maximum heat/power dissipation for system: 3500W / 11942 BTU/hour

DC Power

- Quad hot swappable DC power supplies
- Operating input voltage: -40 to -72 VCD
- Maximum power, each power supply: 1500W
- Maximum heat/power dissipation for system: 3500W / 11942 BTU/hour

Operating Specifications

Temperature

- Operating: 5 °C to 40 °C
- Short-term*: -5 °C to 55 °C
  (*not to exceed 96 consecutive hours)
- Short-term* with fan failure: -5 °C to 40 °C
  (*not to exceed 96 consecutive hours)

Humidity

- Operating: 5% to 85%, (non-condensing)
- Short-term*: 5% to 90% (non-condensing)
  (*not to exceed 96 hours)

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, 2024 - 2026, Published in USA, June 26, 2026, 3124-1039.EN