DATA SHEET

AppStack

Context-aware, signature based Application Layer Filtering

Problem

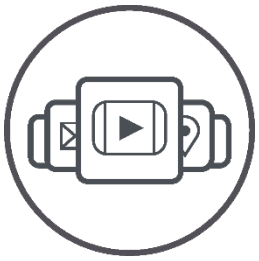
Networks are the most complex and most critical asset to most enterprises today. Organizations urgently need a solution to one of the biggest challenges facing network administrators – complete network visibility that extends past Layer 4 information. For example, many applications today run over HTTP or HTTPS 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 bandwidth they consume, 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, operating system, transport protocol, and other criteria. In addition to packet forwarding, NetFlow/IPFIX information, optionally enhanced with application layer data (IxFlow), can be sent to up to tools, enhancing their capability to report granular user and application data.

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 NetFlow/IPFIX
- Greatly improves monitoring platforms by adding a much richer set of geographical, application and device information
- Application signatures are managed and maintained by Keysight, allowing tools to expand awareness automatically as new applications come online



KEYSIGHT TECHNOLOGIES

Use Cases

Deliverables actionable information

1. Monitor application bandwidth explosions
2. Track application failures
3. Identify suspicious activity
4. Track application usage by geography
5. Understand device impacts and user trend behavior
6. Conduct audits for security, policy and infractions

The AppStack Capabilities from the Dashboard

1. Real-time traffic volume
2. Application distribution, per-application bandwidth
3. **Displays latest dynamic applications**, which are applications not known to AppStack, helping you to quickly zoom into potentially malicious applications
4. **Top Countries** based on **the** largest amount of traffic generated
5. **World view display**, with countries that originate traffic highlighted
6. **Top Devices by OS** displayed by aggregated per-OS traffic, by bytes and sessions, for the last hour
7. **Top Filters:** displays the aggregated per-filter traffic for the last 24 hours
8. **Top Applications** by aggregated per-application traffic, by used bandwidth, bytes, and sessions
9. **Top Browsers:** This view displays a pie chart showing the per-browser traffic percentage for the last hour

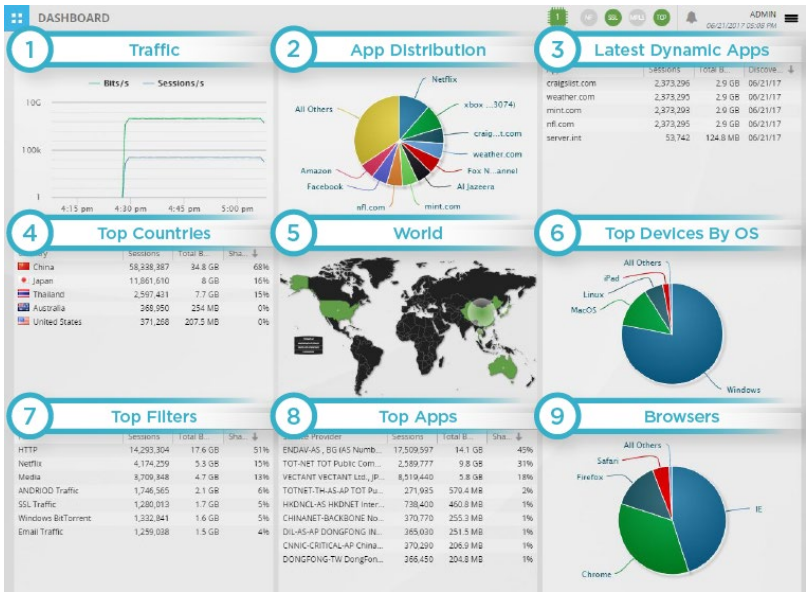


Figure 1. The AppStack dashboard provides comprehensive network traffic information

Each of the nine 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 geos that generate server or client traffic session.

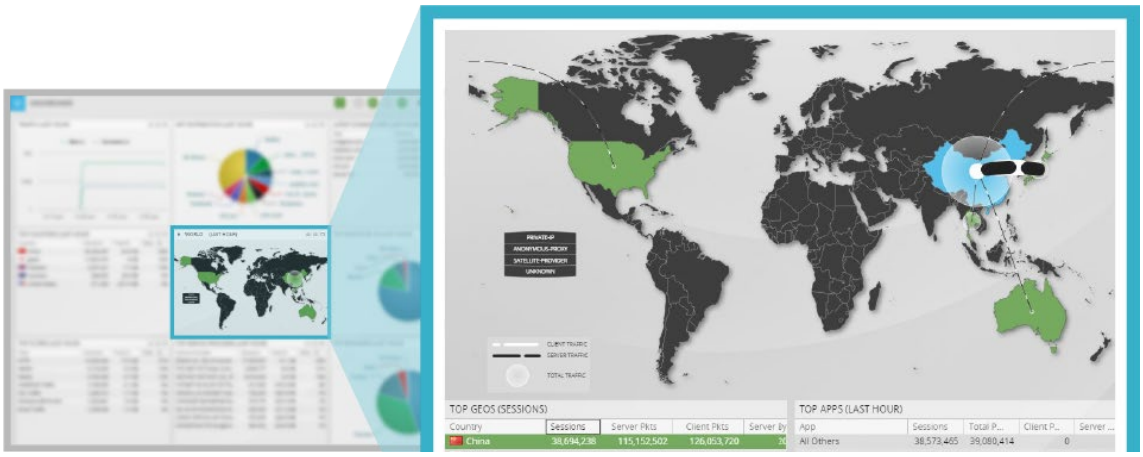


Figure 2. Enlarged world map shows additional information allowing deeper drill down into data flows

Setup Application Filters within a Simple Point-and-click Interface

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

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

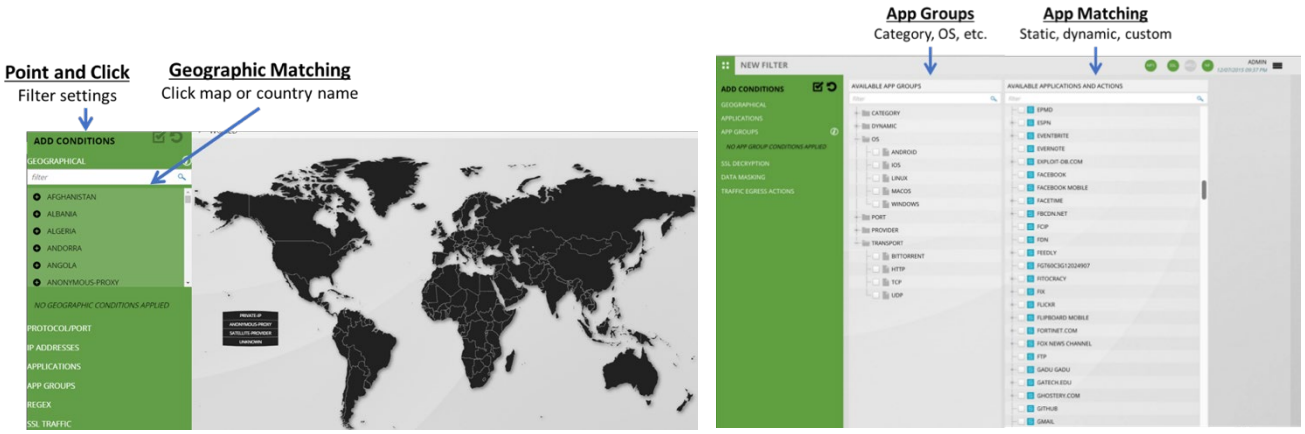


Figure 3. AppStack provides detailed application information, allows filtering by Application Groups, Categories, Provider Type, Transport and more!

For example, you can use the Geographical feature to quickly setup a filter that shows traffic from certain countries.

AppStack allows the combination of any number of filter conditions to devise views important to you and your organization. For example, you could take the same filter and choose to see only specific application data from those countries, for example, just traffic from Android based devices with a simple click of the mouse.

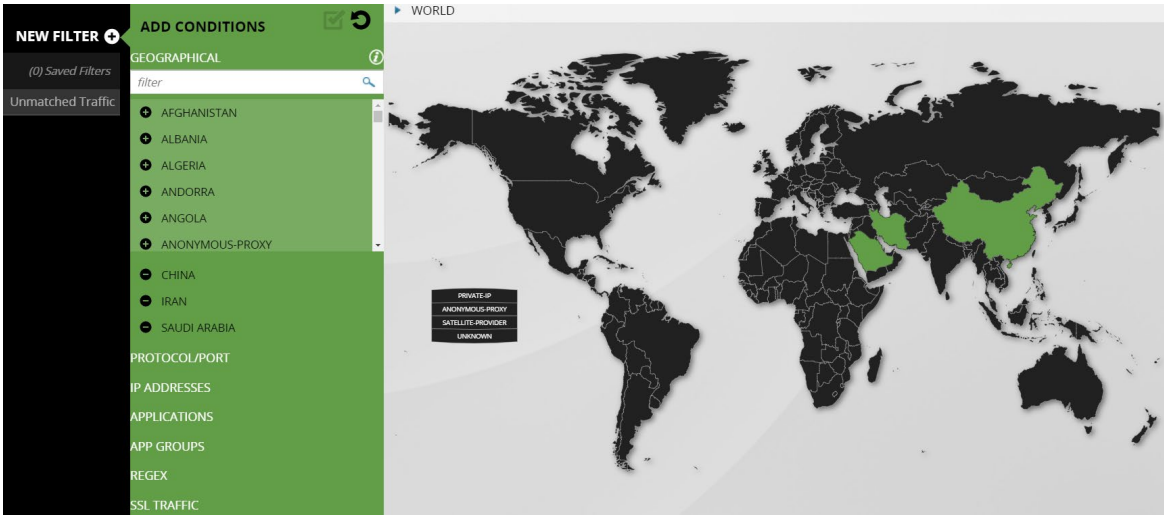


Figure 4. Simple point-and-click interface allows a new filter that identifies all traffic from China, Iran and Saudi Arabia

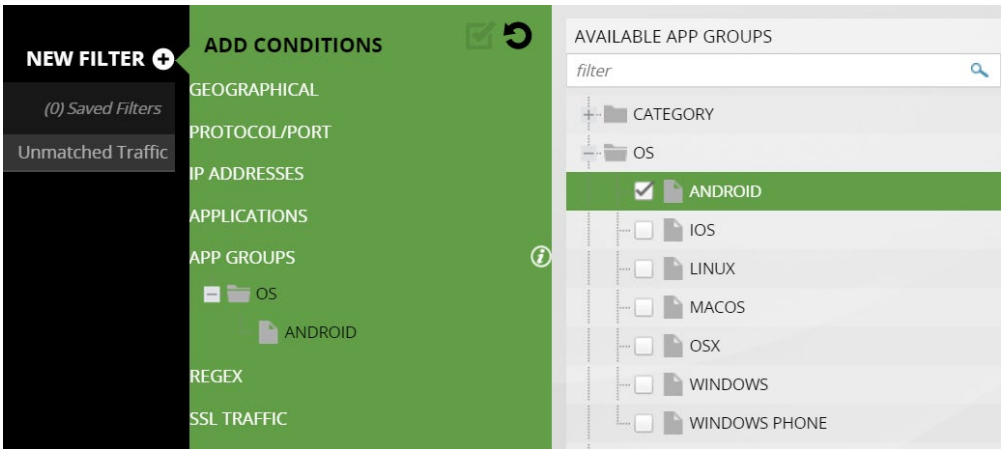


Figure 5. Selecting all Android based traffic

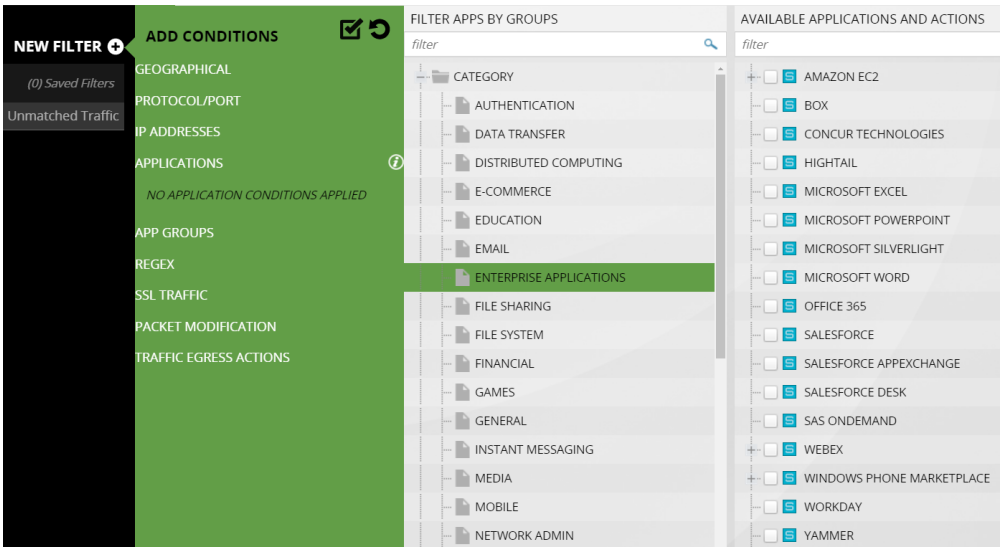


Figure 6. Filtering by Application Group allows quick and easy filtering selection, in this case all enterprise application types

Application Groups Allow Quick Selection of Common Groups of Application Traffic

Instead of specifying several different applications, you can specify an entire Application Group to filter by. For example, instead of selecting individual enterprise applications, for instance all the Microsoft office applications, you can simply select the “Enterprise Applications” which will encompass these plus many more.

Key Features

Feature	Function
 Application Identification	Keysight's AppStack detects applications through signatures: static, dynamic or even customized with a patent pending technology. • Application identification and/or 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, carrier • Ability to detect unknown applications and add mainstream applications by request • Monitor and report top applications' and countries' bandwidth consumption • Database of >1000 applications, that is regularly updated with new applications • No regular expression (RegEx) matching required
 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. • 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 & tagging features • Predefined matches for Taxpayer ID, phone numbers, and common credit cards • Isolate emails from potentially compromised accounts
 IxFlow (NetFlow + meta data)	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, latitude and city name. Application ID or name, device, browser and even SSL/TLS cipher as part of extra information send to tools. • Subscriber-aware reporting provides detail on application and handset (device) type for mobile users • HTTP URL and hostname for web activity tracking • HTTP and DNS metadata for rapid breach detection • Transaction Latency for application performance tracking

	Let Keysight generate the NetFlow/IPFIX without burdening routers and other network devices. • Simultaneous NetFlow generation, SSL/TLS decryption and Application forwarding • Rich NetFlow stats including drop counts when the CPU reaches its peak • High performing mode – can produce NetFlow records for over 300K TCP sessions/second • Supports generation of NetFlow v9 and v10/IPFIX data • Supports up to 10 NetFlow collectors • 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 repeat issue you need to get to the bottom of? Quickly capture those connection 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, browser, device, and more – right your fingertips. • Quickly verify filter configuration by capturing and validating data • Capture up to 10 samples with 100MB sampling window each • Easily download to a laptop/workstation for analysis • Packet capture capability at 30GE line rate
 ATI Subscription	Application and threat intelligence (ATI) subscription provides updates to application signature database, vital for AppStack to stay updated with emerging applications which increases the accuracy of known and unknown 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 & Ordering Information

AppStack is available for Keysight Vision X, Vision ONE, Vision 7300 and CloudLens

	Vison ONE	VIsion X
	Keysight's turnkey network packet broker with AppStack capabilities built-in	Keysight's highest capacity network packet broker
Baseline Platform Requirements	**Chassis (options)** • SYS-V1-48PX-AC • SYS-V116PX8PGAC • SYS-V1-48PX-DC • SYS-V116PX8PGDC	**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  Threat Insight  Out-of-Band SSL/TLS Decryption (SecureStack)  Data Masking Plus (SecureStack)	**Full Subscription – Hardware Activation & Features** • **SUB-V1-SSAS**: Keysight Vision ONE subscription of one-year SecureStack (Oout-of-Band SSL/TLS Decryption) and AppStack license. Includes Out-of-Band SSL/TLS Decryption and all AppStack features, including the ATI Subscription. (993-0113)	**Full 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) **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)

	Vison ONE	VIsion X
	Hardware Activation • **LIC-V1-SSAS-E:** Keysight Vision ONE hardware enablement license for SecureStack (Out-of-Band SSL/TLS Decryption) and AppStack at entry-level performance - QTY (1) (993-0101) • **LIC-V1-SSAS-F:** Keysight Vision ONE hardware enablement license for SecureStack (Out-of-Band SSL/TLS Decryption) and AppStack at full performance - QTY (1) (993-0102) **LIC-V1-SSAS-U:** Keysight Vision ONE hardware enablement upgrade license to enable SecureStack (Out-of-Band SSL/TLS Decryption) and AppStack capabilities (from entry-level to full performance) - QTY (1) Requires additional licenses for features (993-0104)	**Hardware/Dashboard License**
 Application Identification +  Threat Insight	• **SUB-V1-APTL2:** Keysight Vision ONE AppStack one-year subscription license. Includes Application Identification & Filtering, Geolocation & tagging, Application and Threat Intelligence (ATI) data feed - QTY (1) (993-0112)	• **SUB-VX-APTL:** Keysight Vision X, One (1) year subscription; Includes AppStack signature updates and Threat Intelligence feature/updates, QTY (1) per system (993-9612) •
Bundles: System + Licenses	• SYS-V14PX16PGAC • SYSV1FC8PX4P4XAC	

	VIsion 7300	CloudLens
	Keysight's highest capacity network packet broker	Keysight's platform for public, private and hybrid cloud visibility
Baseline Platform Requirements	**Chassis** • SYS7300-STD • SYS7303-STD **Module** • **M7300-SSAS-48PX:** Keysight Vision 7300 family - module to deliver AppStack and SecureStack (SSL/TLS) capabilities - with 48 SFP+ ports (992-0050)	**Virtual Tapping (options)** • 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
 All AppStack Features  Threat Insight  Out-of-Band SSL/TLS Decryption (SecureStack)  Data Masking Plus (SecureStack)	**Full Subscription** • **SUB-7300-SSAS:** Keysight Vision 7300 one-year subscription of SecureStack (Out-of-Band SSL/TLS Decryption) and AppStack license for M7300-SSAS-48PX. Includes SSL Decryption and all AppStack features, including the ATI Subscription. (993-0049) **Perpetual** • **LIC-7300-APPS:** Keysight Vision 7300, AppStack Add-on perpetual license for App Filtering, Netflow, IxFlow, Masking, Regex and Out-of-Band SSL/TLS. QTY (1) per line card (993-0140)	**Subscription (no SSL Decryption)** • **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)

	Vlsion 7300	CloudLens
	Hardware/Dashboard License **LICS-7300-SSAS-F:** Keysight Vision 7300, License for AppStack dashboard at full performance - QTY (1) per line card (993-0141)	
 Application Identification +  Threat Insight	• **SUB-7300-APTL:** Keysight Vision 7300 AppStack, first year subscription license, required per line card. Includes Application signature updates and Threat insight feature and updates. QTY (1) (993-0077)	
 Packet Capture	Hardware: **M7300PCM-48PX** • Keysight Vision 7300 family - Packet Capture Module (PCM) - line card that facilitates packet capture - with 48 SFP+ ports (992-0051)	
Bundles: System + Licenses		

Specifications for M7300-SSAS-48px

General Specifications	
Performance • All ports are bidirectional and fully non-blocking • Full line-rate across all ports with filtering enabled	**Management** • SNMP v1, v2, v3 support • Local, RADIUS, and TACACS+ support (members and groups) • Granular access control features • Event monitoring and logging • Syslog • IT Automation control with web-based API
Physical Specifications	
• 1U high interface card for 19” chassis • Dimensions: 17.5W x 15L x 1.75H (inches) • Weight: 17.0lb (7.7 kg)	• Operating input voltage: -40 to -60VDC • Nominal current: 4.15A @ -53VDC, 220W • Maximum operating input current: 5.5A @ 40VDC, 220W max • Heat/power dissipation for module at 100% traffic load: maximum 220W / 751 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)

Learn more at: www.keysight.com

For more information on Keysight Technologies’ products, applications or services, please contact your local Keysight office. The complete list is available at: www.keysight.com/find/contactus

KEYSIGHT TECHNOLOGIES