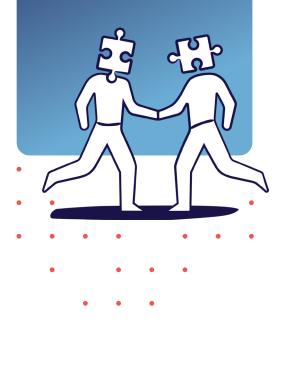


SOLUTION BRIEF

Plixer + Keysight: Up network, application, & security visibility

Joint solution benefits

- Respond quickly to network
 & security events
- Reduce risk with advanced security analytics
- Enrich data context with Keysight's IxFlow exports
- Retain historical forensic data for fast investigation
- Generate flow and IPFIX data
 from anywhere
- Simplify compliance and audit reporting



Plixer Scrutinizer is a security & network intelligence platform that provides the analytics and forensic insight needed to optimize network operations and effectively manage risk. The solution allows you to gain visibility into cloud applications, security events, and network traffic. It delivers actionable data to guide you from the detection of network and security events all the way to root cause analysis and mitigation. Keysight's network visibility solutions complement Scrutinizer by generating enriched flow data (IxFlow) and sending it to Scrutinizer for analysis. Keysight's AppStack features turn packets into insights via deep packet inspection, application classification, geolocation, user device details, and other flow and metadata exports.

Network and security incidents are inevitable. When they occur, Plixer and Keysight are there to help you quickly return to normal and minimize business disruption.

Solution highlights

Networks are among the most complex and the most critical assets within enterprises today. Organizations urgently need complete network visibility that extends past Layer 4 all the way to Layer 7 to secure and optimize their networks.

Keysight's Vision network packet brokers (NPBs) feature AppStack intelligence that combines with Plixer's Scrutinizer to ensure customers enjoy a secure, always-on, and low-latency user experience. AppStack taps into the physical and virtual infrastructure, using deep packet inspection to classify applications, and delivers enriched NetFlow records that equip IT with additional information about geolocation, application names and IDs, devices, browsers, and threats. This enriched IxFlow intelligence is delivered as IPFIX to Scrutinizer, where it is stitched together with thousands of other data elements gathered from all across the network. Data is correlated and visualized, enabling rich reporting that includes details specific to unique IxFlow exports.

THREAT INSIGHTS					Want to block the	se threats? Click <u>here</u>	to learn ho	w.				MAP VIEW FILTER	VIEW	
FILTERS									î	» RAP SHEET		168.144.18	7.112	
THREATS THREAT COUNTRY			TARGET COUNTRY THREAT IP			SRC IP		DST IP						
MALWARE HIJACKED PHISHING BOTNET EXPLOIT	UNITED AUSTRA CANADA ARGENT NIGERIA	IA	UNITED STATES OF AN	107.11 66.33. 173.44 168.14 107.11 190.2. 99.192	9 64.180 208.81 1.60.37 14.247.139 19.64.183 18.70 1.232.211 14.187.112	121 200 229 199 107 179 64 180 4.18 100 37 4.18 100 1 4.18 100 1 4.18 100 55 4.18 100 14 4.18 100 18 4.18 100 18 4.18 100 48 4.18 100 48 4.18 100 32	1 6 1 1 1 1 1 1 1 1 1 1 1 1 1	12: 200 229 199 107 179 64 180 16 33 208 81 173 44 60 37 168 144 247 139 107 179 64 183 190 218 70 199 192 232 211 168 144 187 112 41 138 175 1		FOUND JS/PHI THREAT URL LAST SCAN DATE FILE CHECKSUM	THREATS DETECTED: 4 PHISHING ISH http://khwajaghanibnawazrestaurant.co.za/images/ablegodfo rme/Goldbook/auth/view/document/ 08/27/2018, 8-20PM SH/256 2571/d0a192frd890a4e4b5646e95474eaa8a5d3a306de0f6f83 9b1b778df9b0			
SESSIONS						MATCHING SES	SIONS: 1000	C REFRESH DA	ТА					
FIRST SEEN 🕹	THREAT TYPE	SRC COUNTRY	SRC IP	SRC PORT	DST COUNTRY	DST IP	DST PORT	BYTES						
AUG 28, 2018, 6:3	PHISHING	UNITED STATES	4.18.100.190	58657	CANADA	168.144.187.112	6881	16.8 KB						
AUG 28, 2018, 6:3	PHISHING	UNITED STATES	4.18.100.12	51456	CANADA	168.144.187.112	6881	83 BYTES						
AUG 28, 2018, 6:3	PHISHING	UNITED STATES	4.18.100.55	26857	CANADA	168.144.187.112	6881	83 BYTES						
AUG 28, 2018, 6:3	PHISHING	UNITED STATES	4.18.100.46	18218	CANADA	168.144.187.112	6881	10.9 KB		FOUND JS/PHI	SH			
AUG 28, 2018, 6:3	PHISHING	UNITED STATES	4.18.100.36	42428	CANADA	168.144.187.112	80	5.9 KB		THREAT URL	http://khwajagharibnawazrestaurant.co.za/images/a		blegodfo	
AUG 28, 2018, 6:3	PHISHING	UNITED STATES	4.18.100.165	31159	CANADA	168.144.187.112	63095	132 BYTES			rme/Goldbook/es/auth/view/document/ 08/26/2018, 10:45PM SHA256 - 0498621dcfea0cc0e29f2dce259c391b22edb1dbd1693a3ef9f4			
AUG 28, 2018, 6:3	PHISHING	UNITED STATES	4.18.100.38	44167	CANADA	168.144.187.112	30469	128 BYTES		LAST SCAN DATE FILE CHECKSUM				
AUG 28, 2018, 6:3	PHISHING	UNITED STATES	4.18.100.105	60108	CANADA	168.144.187.112	41828	5.3 KB		FILE CHECKSOM				
AUG 28, 2018, 6:3	PHISHING	UNITED STATES	4.18.100.23	20754	CANADA	168.144.187.112	21034	128 BYTES			6cd8a66621fd		/50501514	
AUG 28, 2018, 6:3	PHISHING	UNITED STATES	4.18.100.32	27773	CANADA	168.144.187.112	23769	219 BYTES						
AUG 28, 2018, 6:3	PHISHING	UNITED STATES	4.18.100.19	51339	CANADA	168.144.187.112	6881	5 KB		in the second second				
AUG 28, 2018, 6:3	PHISHING	UNITED STATES	4.18.100.198	55577	CANADA	168.144.187.112	35250	6.7 KB						
AUG 28, 2018, 6:3	PHISHING	UNITED STATES	4.18.100.56	19384	CANADA	168.144.187.112	53330	16 KB						
AUG 28, 2018, 6:3	PHISHING	UNITED STATES	4.18.100.45	19815	CANADA	168.144.187.112	6881	83 BYTES						
AUG 28, 2018, 6:3	PHISHING	UNITED STATES	4.18.100.139	22497	CANADA	168.144.187.112	11885	17.3 KB		FOUND JS/PHISH				
AUG 28, 2018, 6:3	PHISHING	UNITED STATES	4.18.100.34	8547	CANADA	168.144.187.112	80	17.7 KB						
AUG 28, 2018, 6:3	PHISHING	UNITED STATES	4.18.100.184	2822	CANADA	168.144.187.112	80	5.9 KB		THREAT URL	AT URL http://www.khwajagharibnawazresta		ges/able	
AUG 28, 2018, 6:3	PHISHING	UNITED STATES	4.18.100.12	12778	CANADA	168,144,187,112	65238	570 BYTES	*		godforme/Goldbook/auth/view/document/			

FIG. 1—Keysight's Threat Intelligence detailed view

IxFlow exported data elements

Geographical data	 Client IP Country Code, Country Name, Region Code, Region Name, City Name, Latitude, Longitude, and AS Name Server IP Country Code, Country Name, Region Code, Region Name, City Name, Latitude, Longitude, and AS Name
Application details	 HTTP Hostname, URI, and User Agent Application ID and Name DNS TXT, DNS Host Name, DNS Class Latency
Device information	 Device OS ID and Name Browser ID and Name
SSL visibility	 SSL Connection Type Encryption Cipher Name and Key Length
Threat intelligence	 Threat type (malware, botnet, exploits, hijacked IPs and phishing activity IP address of the threat source or destination host

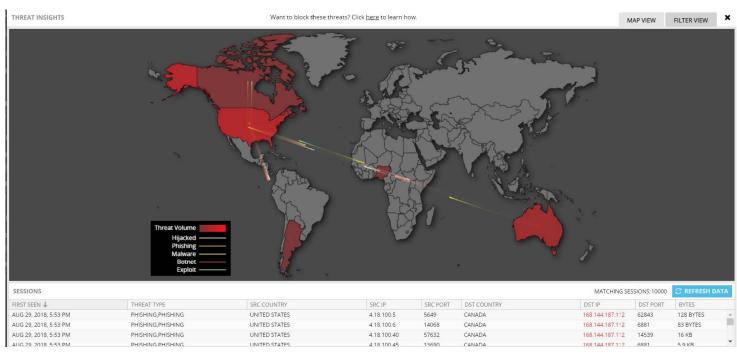


FIG. 2—Keysight's Threat Intelligence map

The combined solution allows administrators to identify the users, device types, operating systems, and applications that generate excessive traffic or security threats. Armed with context-rich data, IT can isolate and remove unwanted behaviors.

Keysight's AppStack

Relying on both static traffic pattern identification and dynamic application discovery, AppStack provides a comprehensive view of the applications running within your network, how much bandwidth they consume, where these applications are running geographically, and which hosts are affected by threats. 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 information that is (optionally) enhanced with application layer data (IxFlow) is exported to Scrutinizer, delivering unique data elements to improve the visibility and context of every flow.

For additional information, visit keysight.com.

Plixer security & network intelligence Platform

Plixer Scrutinizer gathers multi-dimensional telemetry from every corner of the network to actively monitor, visualize, and report on network and security incidents. The system delivers the analytics and forensic insight needed by IT professionals to support fast and efficient incident response.

Scrutinizer stands out by delivering the most scalable solution on the market, offering the fastest reporting, and providing the richest data context available anywhere. It creates a holistic view of the entire enterprise regardless of equipment vendor and leverages the latest flow technologies, such as IxFlow from Keysight, to foster deep visibility and pervasive security into every corner of the network.

Scrutinizer network benefits

- Enrich data context of network traffic
- Increase efficiency and reduce cost
- Monitor network and application performance
- Achieve fast reporting and massive scale

Scrutinizer security benefits

- Reduce attack surface and security risks
- Support faster time-to-resolution
- Deliver contextual forensics
- Run advanced security analytics
- Correlate with Keysight's Threat Intelligence

Scrutinizer uses dozens of security algorithms to uncover odd behavior patterns indicative of malicious activity. Furthermore, role-based access automatically presents the network and security teams with the data they need.

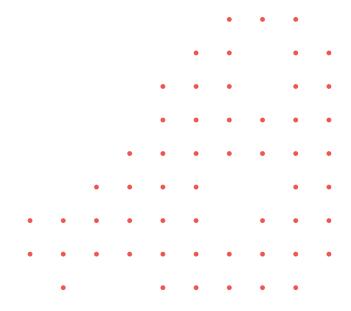
For more information: plixer.com/products/scrutinizer/_

About Plixer

Plixer provides a network and security intelligence platform that supports fast and efficient incident response. The solution allows you to gain visibility into cloud applications, security events, and network traffic. It delivers actionable data to guide you from the detection of network and security events all the way to root-cause analysis and mitigation. Network and security incidents are inevitable. When they occur, Plixer is there to help you quickly return to normal and minimize business disruption. Thousands of organizations rely on Plixer solutions to keep their IT infrastructure running efficiently.

About Keysight

Keysight delivers a powerful combination of innovative solutions and trusted insight to support network and security infrastructures from concept to operation. Whether you are preparing a product for launch, deploying a service or application, or managing performance in operation, we offer an extensive array of solutions in testing, visibility, and security—all in one place. Our solutions are used worldwide to validate network functions, test the integrity of security infrastructures, and deliver an end-to-end view of the network. The result: stronger applications, better performance, increased security resilience, happier customers, and maximum ROI.



[©]Plixer, LLC. All rights reserved. Plixer and Scrutinizer are trademarks of Plixer. All other brand names are trademarks or registered trademarks of their respective companies.

The content in this document is for informational purposes only and is subject to change by Plixer, LLC without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, Plixer, LLC assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Plixer, Plixer, LLC has no obligation to develop or deliver any future release or upgrade or any feature, enhancement, or function. sb-4006.1-0221