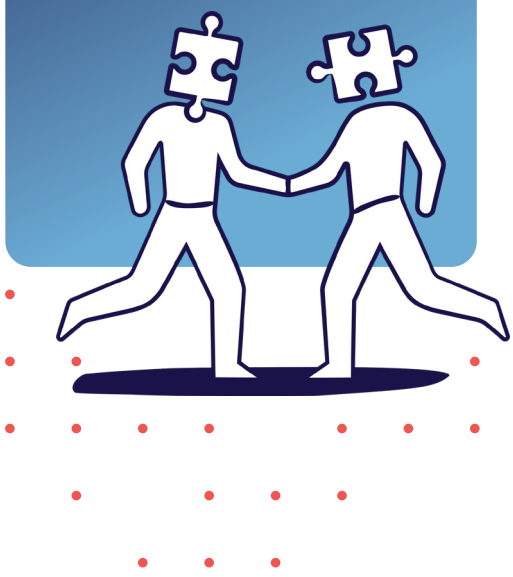
SOLUTION BRIEF

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.

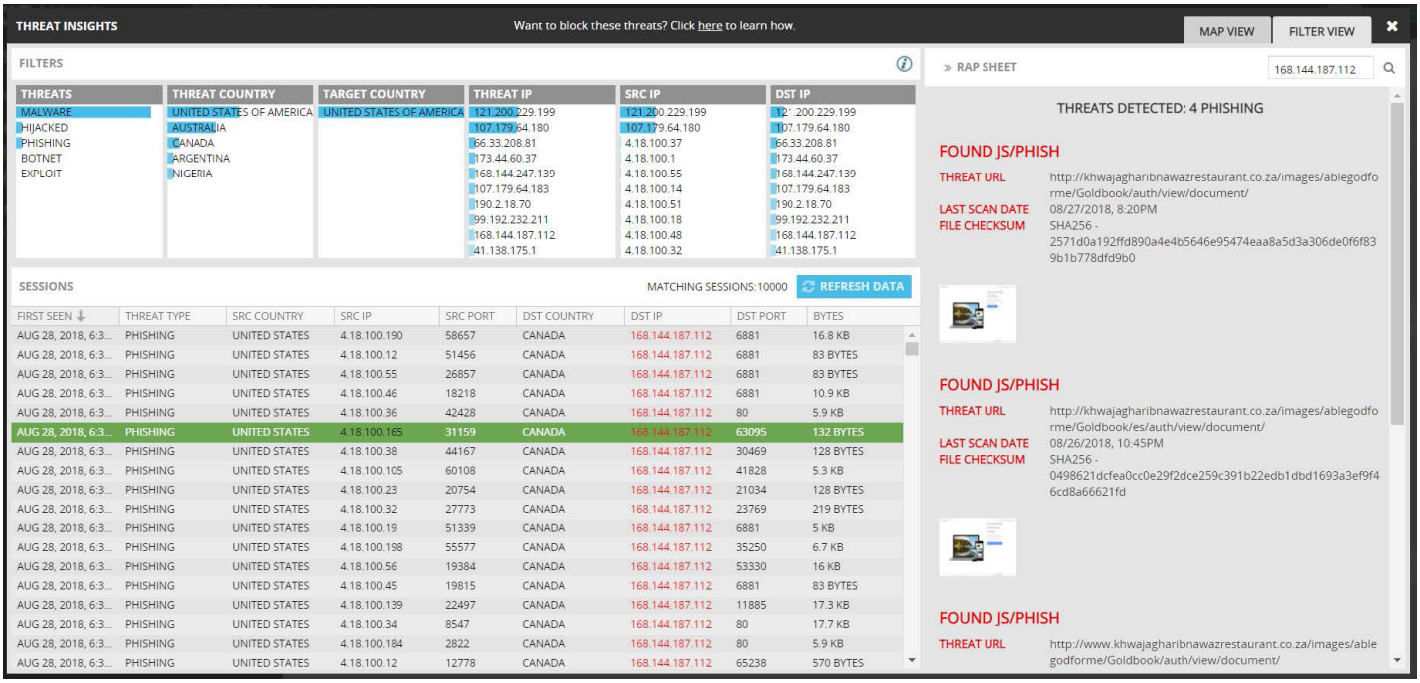


FIG. 1—*Keysight's Threat Intelligence detailed view*

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

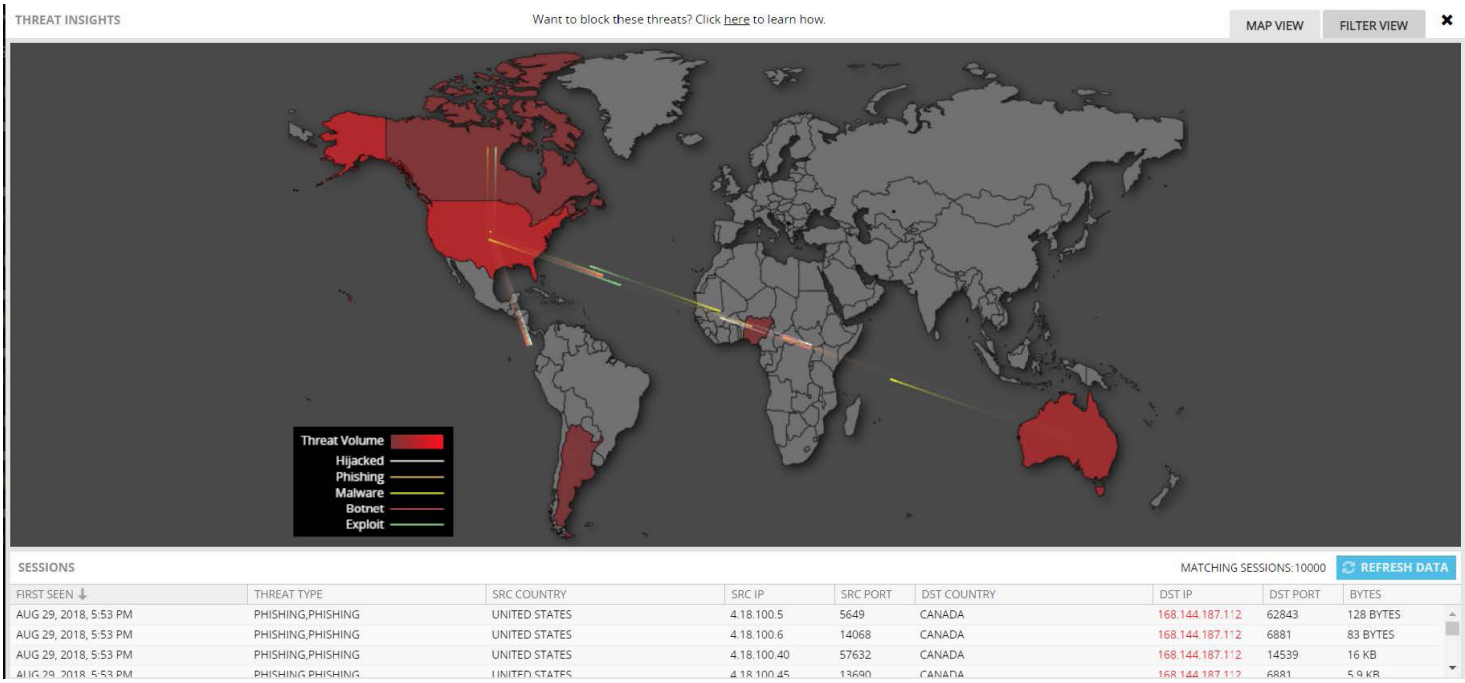


FIG. 2—*Keysight's Threat Intelligence map*

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.

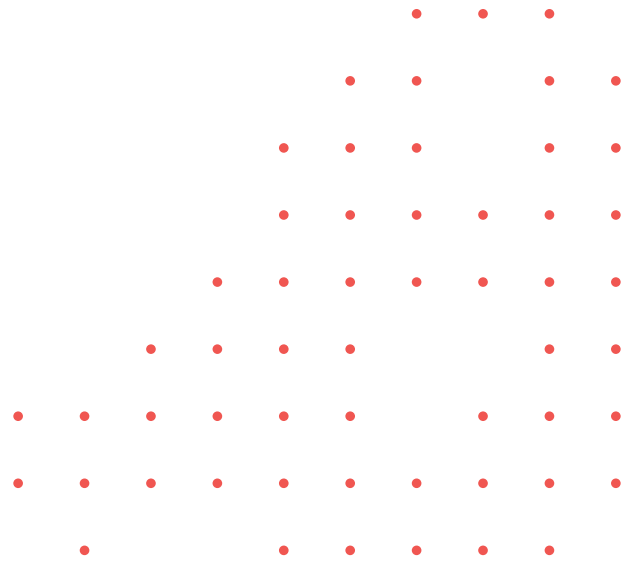
For more information:
plixer.com/products/scrutinizer/

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.



sb-4006.1-0221