VIAVI

VIAVI Solutions

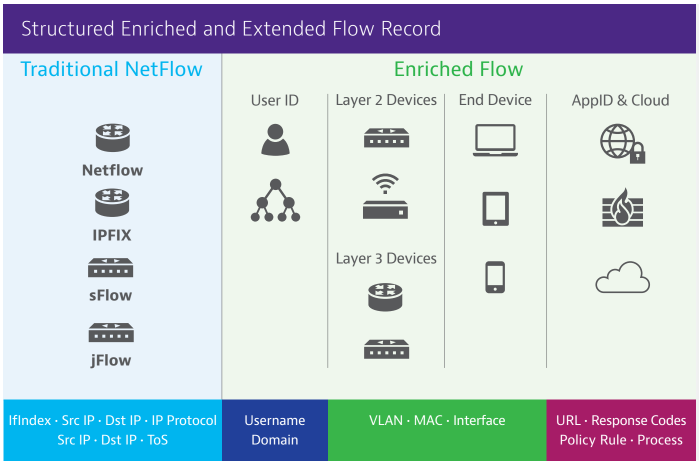
Brochure

Enriched Flow with Observer

Combining Data into Structured Insights

What's Connected and Who's Communicating on Your Network?

Observer reimagines traditional flow to deliver its full potential by intelligently bringing together multiple sources of data into a single enriched flow record. An enriched flow record is a structured piece of data formed from stitching together data from multiple traffic and network infrastructure sources – traditional flow augmented by device information, user identity, application usage and more.



How can Enriched Flow help you?

Enriched Flow can grant you visibility into:

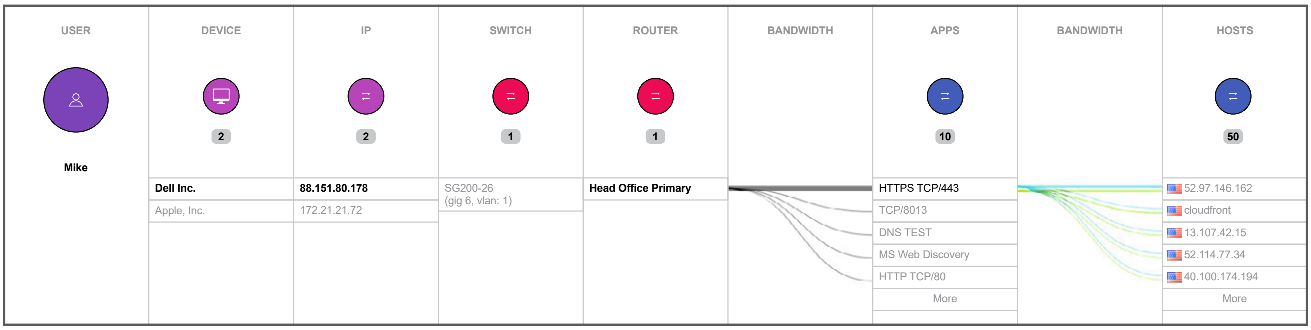
- 3rd Party devices including Packet Brokers, Proxy Servers, Load Balancers, SD-WAN Forwarders, Firewalls, and more
- ARP and CAM tables
- Authentication details from Active Directory and other 3rd party sources
- DNS Responses and Timing
- Cloud sources like VPC Flow Logs

Example fields shown; actual GigaFlow record can contain dozens of unique fields

Navigate User, IP, Device, and Application Usage Relationships in Your Network

By compiling Layer 2 to Layer 3 insights into a single enriched flow record, Observer can produce unique, interactive visualizations that illustrate the relationships between User, IP, MAC, and application usage in the network. These visualizations are a welcome addition to existing traffic insights provided by traditional flow like quality of service marking and traffic volume analysis, which are all available in Observer.

Because the IP Viewer can even provide insights into ports associated with VPN, IT departments can use it to spot compromised accounts that show irregular VPN usage patterns for remote workers.



USER	DEVICE	IP	SWITCH	ROUTER	BANDWIDTH	APPS	BANDWIDTH	HOSTS
	2	2	1	1		10		50
Mike	Dell Inc.	88.151.80.178	SG200-26 (gig 6, vlan: 1)	Head Office Primary		HTTPS TCP/443		52.97.146.162
	Apple, Inc.	172.21.21.72				TCP/8013		cloudfront
						DNS TEST		13.107.42.15
						MS Web Discovery		52.114.77.34
						HTTP TCP/80		40.100.174.194
						More		More

Figure 1: Observer's IP Viewer lets you understand who's communicating and what's connected

Leveraging Enriched Flow in Observer GigaFlow

Security Insights and Incident Response

Threat Identification and Profiling

Leverage automated detection of suspicious and malicious behaviors leveraging multiple techniques including:

IP Blacklisting: Continuously updated pre-configured and custom blacklists.

SYN Forensics: Alerts on suspicious volumes and patterns of SYN-only flow records, often associated with network and port sweeps.

Host and Service Profiling: Notifies and records all details of hosts or services acting in unexpected ways that fall outside of their normal behavior profile. (For example, certain groups of devices, such as ATMs, Point-of-Sale systems, or medical devices, are expected to behave in specific ways. The behavior, access and traffic associated with services like DNS, Web Proxy, or devices containing confidential information should follow predictable patterns.)

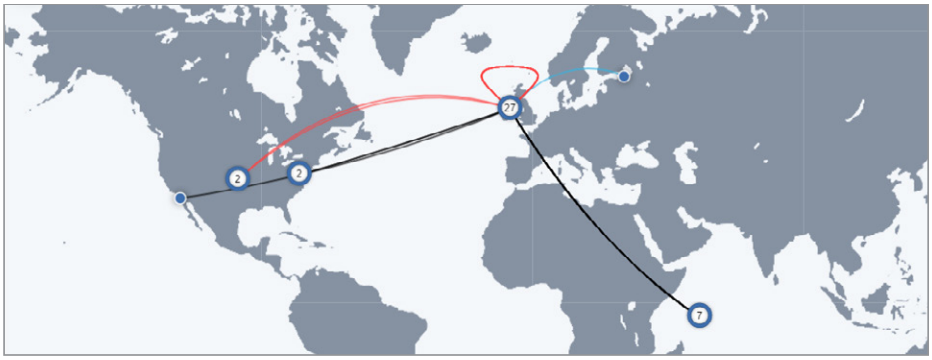


Figure 2: Enriched Flow Provides a Real-Time Threat Map Displaying Identified Threats

Back-in-Time Analysis Using Enriched Flow Records

Enriched flow records dynamically capture all relevant data including timestamp and location continuously for storage over extended periods. This allows IT teams to navigate to a specific event or anomaly in the past to troubleshoot and solve the problem by answering who it impacted, when, where, and how the incident occurred.

Observer Platform Provides A Holistic Solution

When enriched flow from GigaFlow is combined with Observer Apex and Observer GigaStor, the complementary nature of wire data and enriched flow analysis becomes clear.

1. **Wire Data from GigaStor:** Packet-level wire data remains the ultimate source of end-to-end visibility and the best source for accurate measurements of end-user experience and high-fidelity forensic analysis
2. **Enriched Flow from GigaFlow:** By collecting information from the devices that see that data as it traverses the network, additional information about the user, the physical connectivity, traffic classification, prioritization (or blocking), behavioral patterns, and other critical details can be observed.
3. **Analysis and Workflows from Apex:** With data visualizations and stream-lined workflows, Apex pulls together information from GigaStor and GigaFlow for comprehensive views of performance and threat landscapes across your environment. Pin-point problems with patent-pending End-User Experience Scores and real-time Threat Maps for actionable insights that decrease time to know and time to resolution.

By combining wire data and flow based analyses, Observer offers SecOps and NetOps teams with comprehensive visibility into their network, allowing them to manage daily operations, mitigate risk, and solve problems faster than ever before.

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact