VIAVI Solutions

Brochure

# VIAVI Observer
## GigaFlow

Network, user, and infrastructure enriched
flow visibility for NetOps and SecOps

## IT Operational Clarity

Among all the change within IT, the one constant has been IP technology. While reliable and scalable, this reliance has consequences:

1. IT teams know less about how IT infrastructure connects and functions

2. There are no open standards defining the who, what, where, and how users and devices are communicating

The result: IT often struggles to keep on top of user experience and performance issues.

It's getting worse. Today's hybrid IT environment is increasingly difficult to manage. The growing number and variety of devices, whether related to IoT deployments, cloud migrations, or users at the network edge, are becoming unmanageable. IT teams are losing control.

Observer GigaFlow intelligently combines numerous metrics, resolving these challenges by quantifying the health of every network interface, independent of location or ownership. This delivers enhanced end-user experience insight with enriched, high-fidelity network data for forensic analysis.

The network and infrastructure has much to tell you about what is connected and who is talking. GigaFlow enables you to hear it clearly.
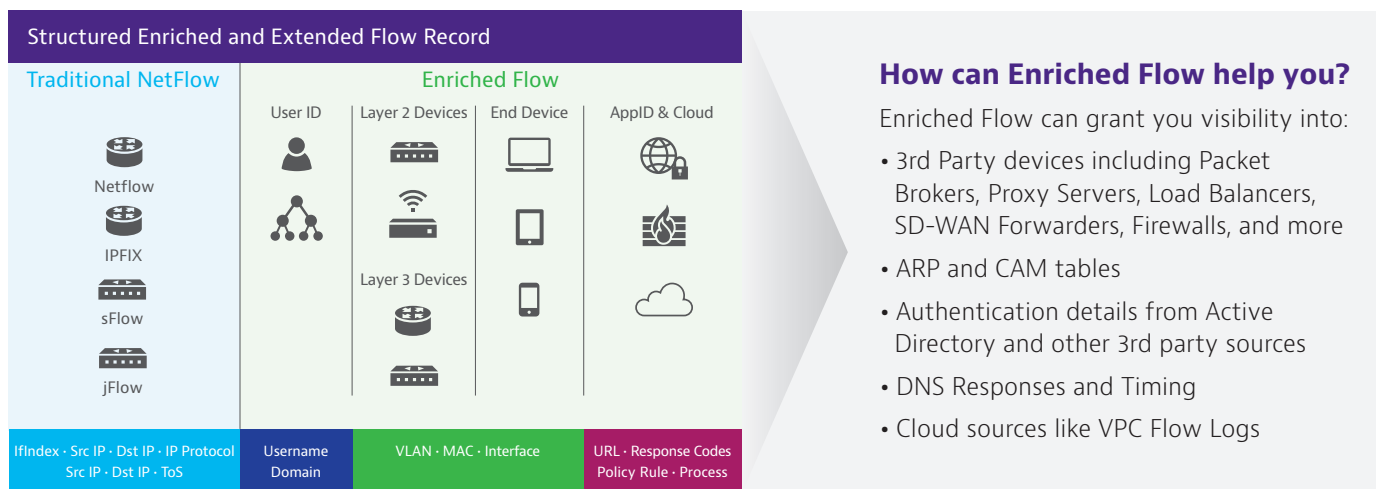
## GigaFlow Enriched Flow Records

When is a flow not a flow? When it's an enriched GigaFlow record. Traditionally collecting and storing of flow traffic like NetFlow involves aggregating, pruning, or de-duplicating information. This results in a corresponding loss of fidelity that compromises forensic evidence and reduces effectiveness to solve issues.

In an industry first, GigaFlow reimagines flow to deliver its full potential. GigaFlow intelligently stitches and structures multiple sources of data (flow, SNMP, user identity, and session syslog) together into an enriched flow record.

Doing so provides in-depth details on network device types, connectivity, traffic control, and usage patterns down to individual users for all communication traversing the environment from any point of view.

Created in real-time, enriched records are then stored unaltered over time in a relational database, so IT teams can easily search and locate on any operational variable for long-term protection and assurance.

VIAVI brings the network to the table and exposes the infrastructure and traffic clearly to all business stakeholders serving as the go-to platform for every IT team.

### Structured Enriched and Extended Flow Record

**Traditional NetFlow**
- Netflow
- IPFIX
- sFlow
- jFlow

**Enriched Flow**

User ID | Layer 2 Devices | End Device | AppID & Cloud

Layer 3 Devices

| IfIndex · Src IP · Dst IP · IP Protocol Src IP · Dst IP · ToS | Username Domain | VLAN · MAC · Interface | URL · Response Codes Policy Rule · Process |

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

### 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

1057.900.0122

# Enriched Flow for SecOps and NetOps

GigaFlow offers real-time and long-term historical perspectives of end-user and device as a function of underlying service health at every network traffic interface. The enriched flow records of GigaFlow dynamically capture all relevant data including time-stamp and location continuously over extended periods. Because of this, IT teams can navigate to a specific event or anomaly in the past to troubleshoot and solve the problem by answering who it impacted and when, where, and how the incident occurred.

This is particularly helpful for SecOps teams who can leverage this flow-based analysis to reduce the dwell time of the bad actor and speed incident response for breaches. Most breaches go undetected for extended periods of time – having the flow, infrastructure, device, host, and user data available for retrospective forensic analysis is critical for timely remediation of security incidents.
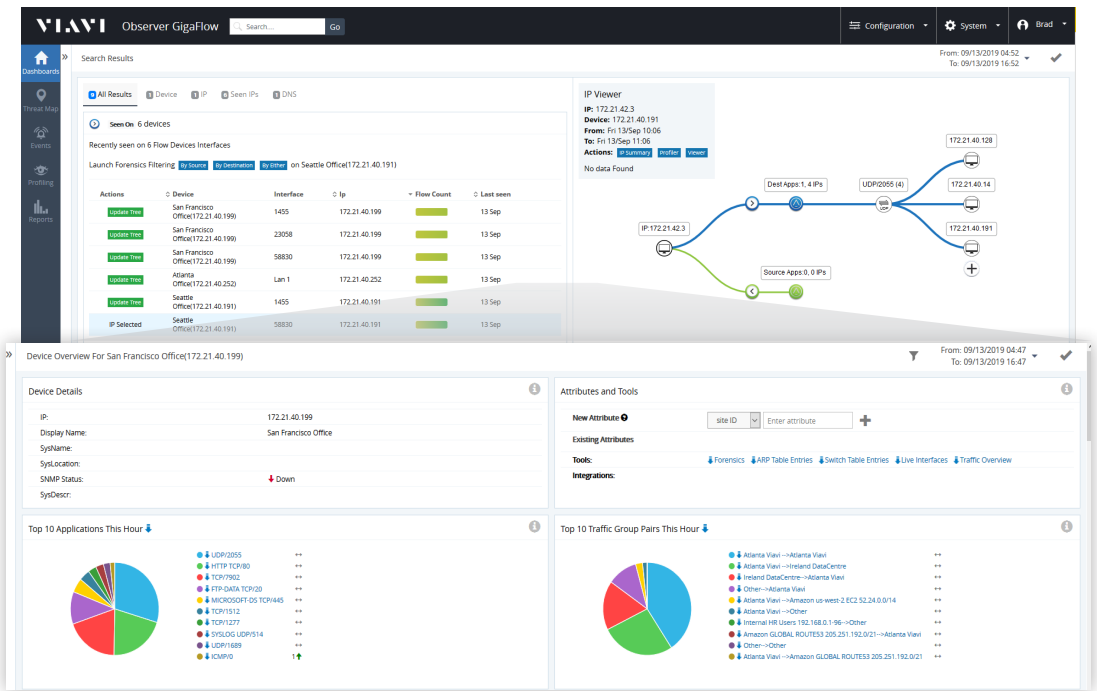


Full Flow Data Available for Forensic Analysis with IP Detail
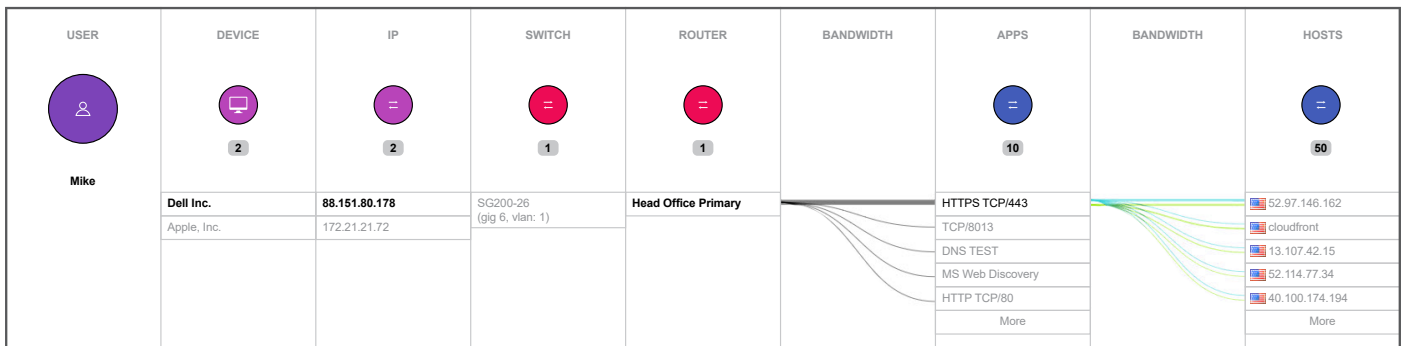


By compiling Layer 2 to Layer 3 insights into a single enriched flow record, Observer can produce unique, interactive visualizations that illustrate the relationships between User, IP, MAC, and application usage in the network. A NetOps or SecOps user can simply enter a name or username and immediately find all devices, interfaces, and applications associated with it. Finding out what's connected and who's communicating across your network has never been easier.

# Network Capacity Planning in Observer GigaFlow

Network capacity planning is an ongoing process that involves continually assessing network utilization, traffic volumes, and traffic type to identify shortcomings like performance chokepoints that can affect the end-user's experience.

Without investing in capacity planning measures, organizations risk decreased employee productivity from degraded network performance, Service-Level Agreements not being met, and ultimately a poor experience for the end-user.

### Device-Based and Site-Based Workflows

GigaFlow grants usage and utilization insights on a per interface basis down to the layer 2 switch, with graphical summaries of the busiest sites or devices and further drilldown into individual WAN links. This is ideal for general assessments of end-user experience at points anywhere along the conversation route, and valuable for quantifying asset cost/benefit efficiencies, such as when deciding where new enhancements should be made.
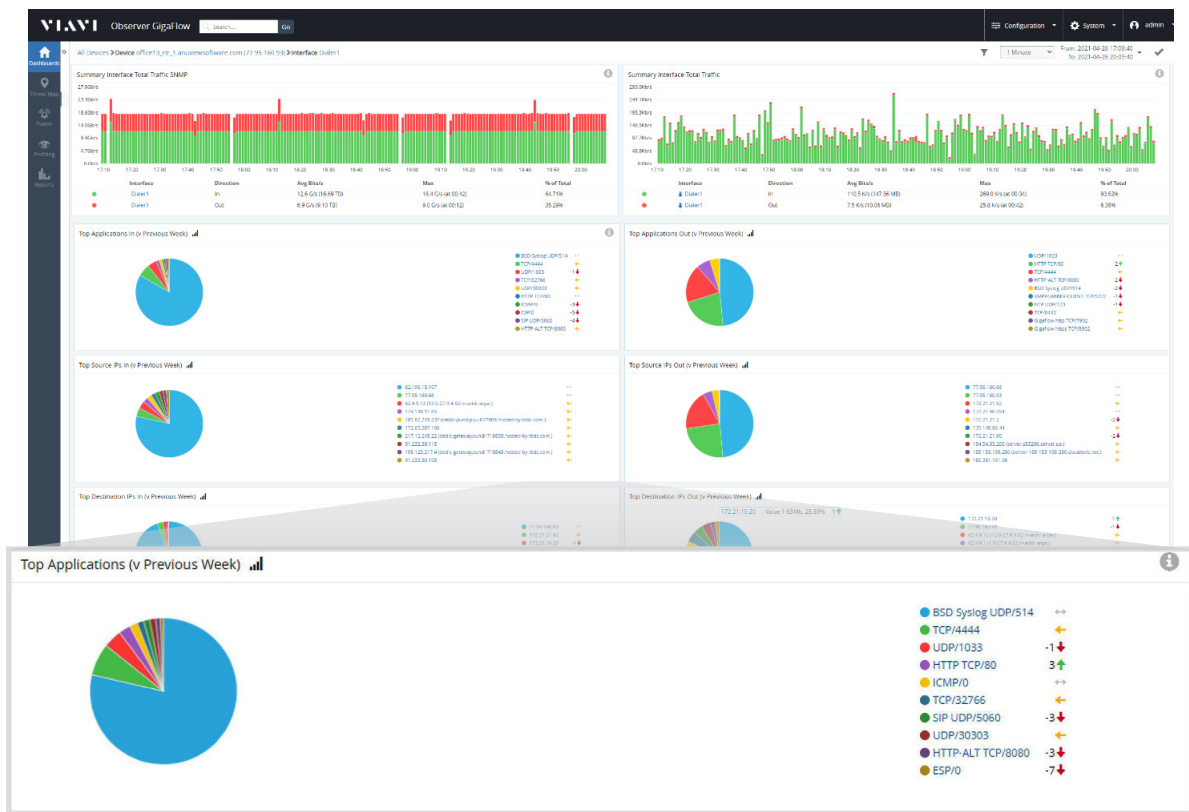


Device-Based and Site-Based Dashboards for Usage and Utilization Insight

## Capacity Planning Reporting with Drilldown for Forensic Analysis

With intuitive capacity planning reporting, GigaFlow lets IT teams conduct proactive assessments for WAN spending as well as reactive resolution of capacity-related issues. A simple, color coded dashboard highlights interfaces that are highly utilized for the most amount of time. If already congested sites see increasing traffic, the utilization report will reflect this by showing more red and orange warnings. Application summary graphs can help IT teams discern which application is responsible for any growth. Drilldown into the network data for forensic analysis is also available from the capacity planning reports, which can be useful for investigating performance or security issues.
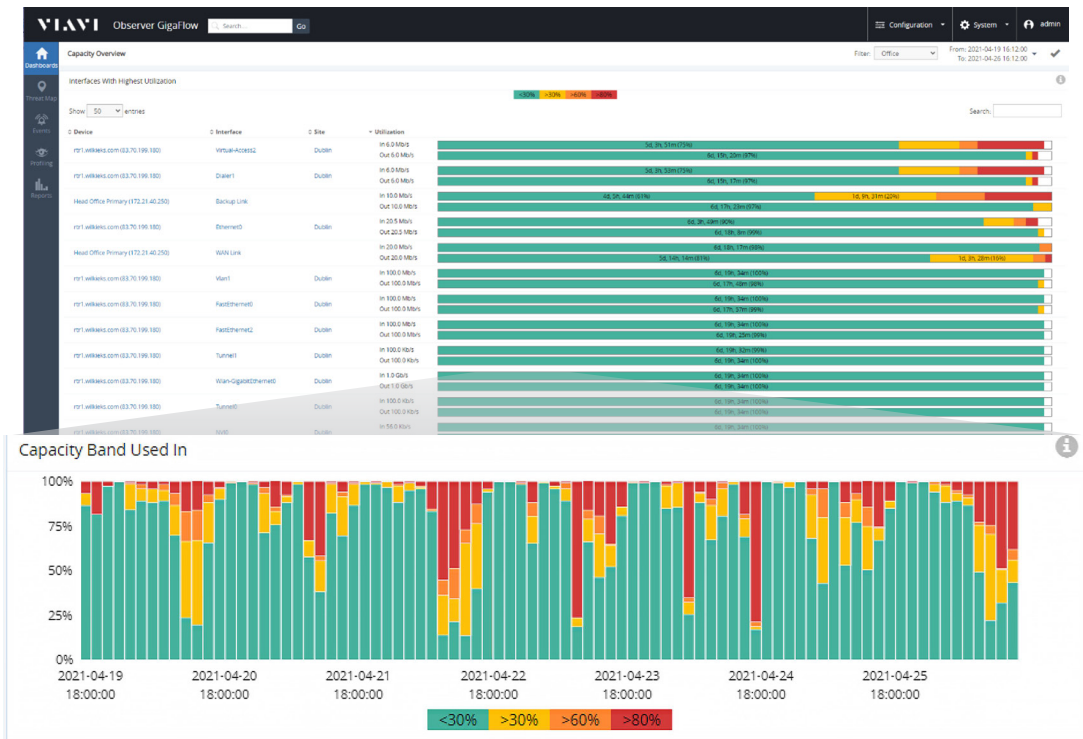


Color-Coded Capacity Planning Reports on WAN Spending



Observer Use Cases

## Features and Benefits Summary

- High-fidelity forensic visibility into every network conversation over time reducing mean time to resolution
- Advanced service path visibility ensures immediate problem domain isolation across a complex hybrid IT environment
- Intuitive capacity planning reporting to help with proactive assessments of WAN utilization
- Interactive IP Viewer that visualizes relationships between User, IP, MAC, and application usage in the network.
- New workflows detailing utilization at any given site or device interface with easy drill-down into forensic level data
- Comprehensive baselining, capacity planning, and QoS setting validation

# Observer 3D Overview

Observer 3D is a comprehensive network performance monitoring (NPM) solution that offers valuable insight and assistance to network, operations, and security teams. GigaFlow plays a crucial part of Observer 3D, providing enriched flow metadata to Apex for use in problem resolution and forensic investigations.

As the integrated dashboard and reporting resource, Observer Apex serves as point of central global visibility and the launch point for rapid troubleshooting with pre-engineered workflows that help identify root cause using packets, enriched and enhanced flow, and active test.

Observer 3D helps IT teams in three key ways:

- Location of Services – Observer 3D provides observability into every hosting environment, whether private cloud, public cloud, SaaS applications, remote users, on premise in branch offices or in the data center. No matter the location, VIAVI has you covered. To learn more about how Observer 3D leverages predictive analytics to proactively deliver visibility into performance issues, visit the interactive platform demo.
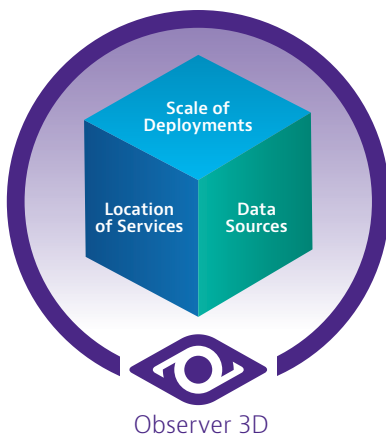


Observer 3D

1043.900.1221

- Data sources – With Observer 3D, choose between a combination of wire data, enriched and enhanced flow visibility, active test insights, and metadata generation to enable smooth, timely resolution of performance and threat issues. Automated, role-based workflows make it easy to dive down into the network data for forensic level analysis, regardless of the type of data or source.
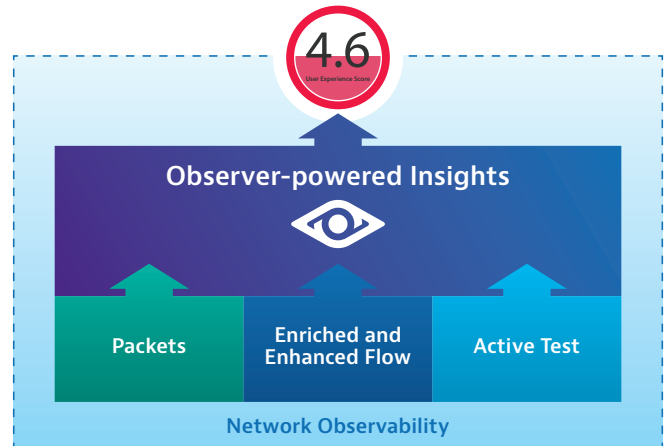


1041.900.1221

- Scale of deployments – Start small and grow as your business and monitoring needs and operational demands change. Whether that means flexibility in deployment with our 24T or ObserverONE solutions, or flexibility in pricing with our new tiered pricing and subscription models—VIAVI has you covered. Buy what you need when you need it using OpEx or CapEx budget, allowing you to balance your observability and budgetary needs without compromise.
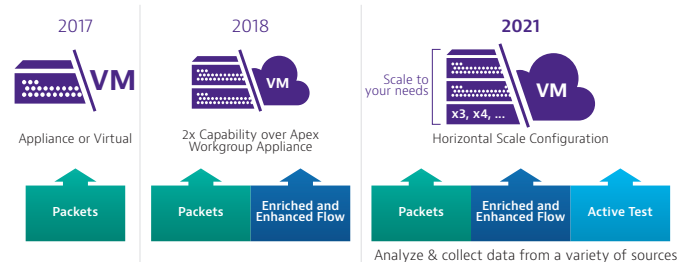


1042.900.1221

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

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

**viavisolutions.com**