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 forensics.

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 Stitching and Enriched Flow Records

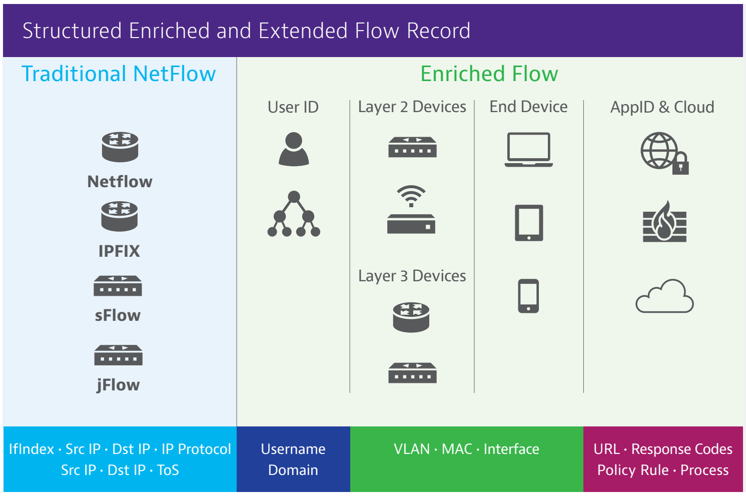
When is a flow not a flow? When it's an enriched GigaFlow record. Traditionally collecting and storing of flow traffic like NetFlow involves aggregating, pruning, or de-duplicating information. This results in a corresponding loss of fidelity that compromises forensic evidence and reduces effectiveness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



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

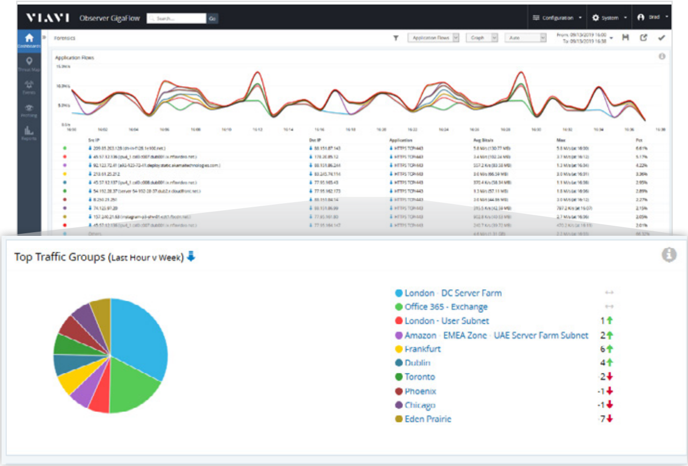
Network Performance

End-User & Application Capacity Management

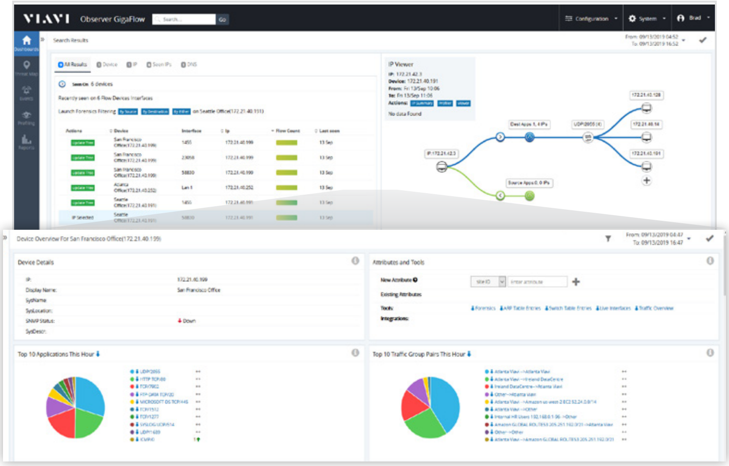
GigaFlow provides network traffic visibility on a per interface basis down to the layer 2 switch. Gain usage and utilization insight by individual user or in aggregate spanning the service delivery environment from core to edge and into the cloud. This is ideal for general assessments of end-user experience at points anywhere along the conversation route, and valuable for quantifying asset cost/benefit efficiencies. For example, assessing the cost effectiveness of cloud deployments and accurately attributing costs of underlying IT assets to the resource users (e.g. department, business unit).

Enriched Flow Forensics

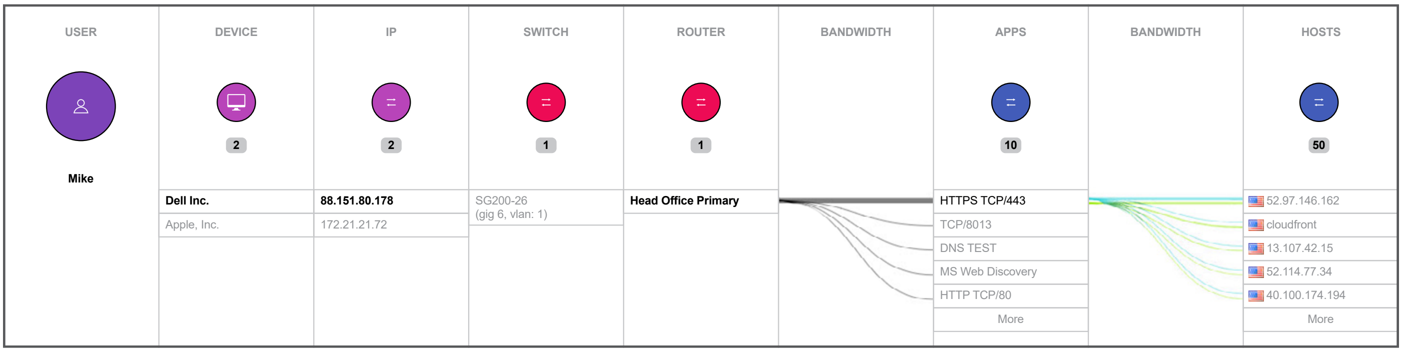
GigaFlow offers real-time and long-term historical perspectives of end-user and device as a function of underlying service health at every network traffic interface. The enriched flow records of GigaFlow dynamically capture all relevant data including time-stamp and location continuously over extended 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.



Summary Dashboard with Detailed Drill-Down


VIAVI Observer GigaFlow
Search Results
IP Viewer
Device Overview For San Francisco Office
Device Details
Attributes and Tools
Top 10 Applications This Hour
Top 10 Traffic Group Pairs This Hour

Full Flow Forensics with IP Detail



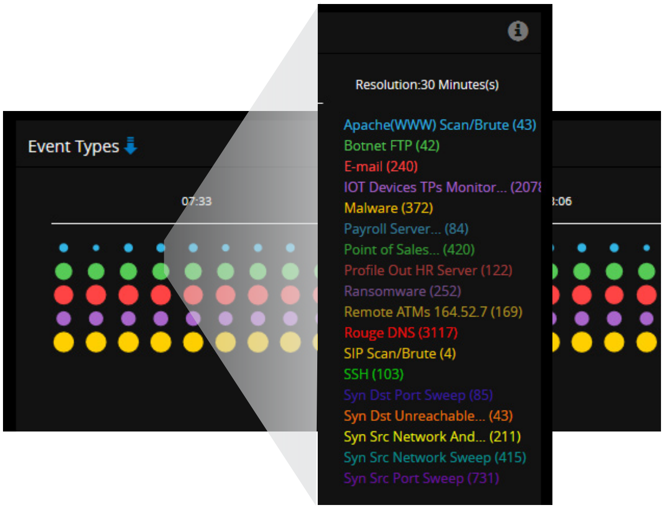
USER	DEVICE	IP	SWITCH	ROUTER	BANDWIDTH	APPS	BANDWIDTH	HOSTS
Mike	2	2	1	1		10		50
	Dell Inc.	**88.151.80.178**	SG200-26 (gig 6, vlan: 1)	**Head Office Primary**		**HTTPS TCP/443**		52.97.146.162
	Apple, Inc.	172.21.21.72				TCP/8013		cloudfront
						DNS TEST		13.107.42.15
						MS Web Discovery		52.114.77.34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

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 enter in a 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 Security

Threat ID with Scope & Impact Context

Out of the box, GigaFlow will automatically call home to obtain the latest black lists IPs, then checks it against all enriched flow records over time. GigaFlow can also alert on syn only flow records, often associated with rogue activity. Incidents from other security solutions can be passed to GigaFlow providing search and identification capabilities. This helps answer questions like: What was the host or device communicating with earlier? Where is the rogue host/device now? Who was using the host/device? This aids SecOp teams in their investigations and enhances existing security solutions.



Event Types

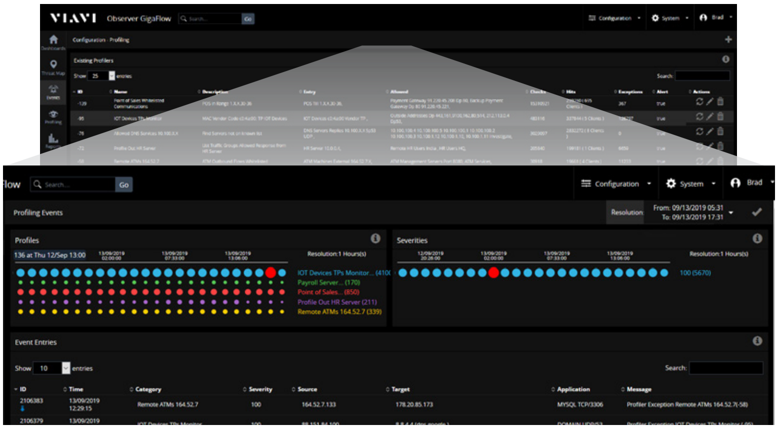
Resolution:30 Minutes(s)

Apache(WWW) Scan/Brute (43)
Botnet FTP (42)
E-mail (240)
IOT Devices TPs Monitor... (2078
Malware (372)
Payroll Server... (84)
Point of Sales... (420)
Profile Out HR Server (122)
Ransomware (252)
Remote ATMs 164.52.7 (169)
Rouge DNS (3117)
SIP Scan/Brute (4)
SSH (103)
Syn Dst Port Sweep (85)
Syn Dst Unreachable... (43)
Syn Src Network And... (211)
Syn Src Network Sweep (415)
Syn Src Port Sweep (731)

Event Overview with pinpoint breakout of threats

Host/Device Traffic Profiling

A core capability of GigaFlow is the ability to build a traffic profile of devices on the network. Hosts are characterized by type, usage, application, and communication activity. This can be used to assess acceptable usage (e.g. white lists). Profiles are maintained in real-time with all future network-generated device traffic evaluated against past behavior for unusual or anomalous activity. Ongoing SNMP polling has the added benefit of quickly detecting new and possibly rogue activity. For example, discovering compromised or bogus assets that serve as entry points for security threats (e.g. When is a printer not a printer?).



Profiling Events

Resolution: From: 09/13/2019 05:31 To: 09/13/2019 17:31

Profiles

136 at Thu 12/Sep 13:00

Resolution:1 Hours(s)

IOT Devices TPs Monitor... (410
Payroll Server... (170)
Point of Sales... (850)
Profile Out HR Server (211)
Remote ATMs 164.52.7 (339)

Severities

Resolution:1 Hours(s)

100 (5670)

Event Entries

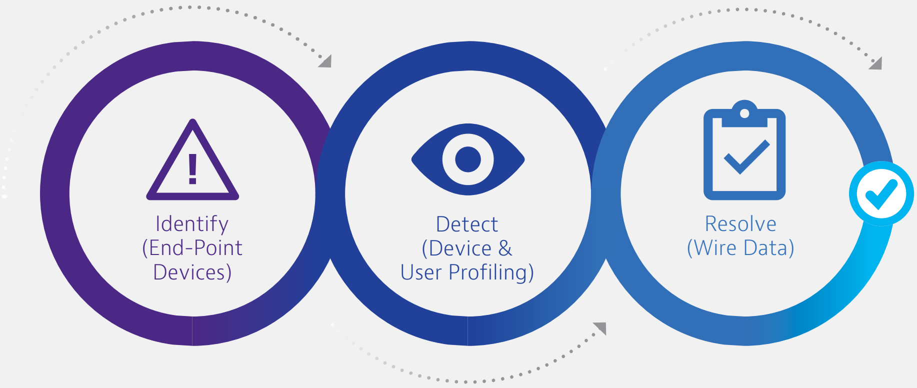
Show 10 entries

Search:

ID	Time	Category	Severity	Source	Target	Application	Message
2106383	13/09/2019 12:29:15	Remote ATMs 164.52.7	100	164.52.7.133	178.20.85.173	MYSQL TCP/3306	Profiler Exception Remote ATMs 164.52.7(-58)
2106379	13/09/2019	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Easily create profiles and then alert on any exceptions

SecOps Network Security Workflow



Identify (End-Point Devices)

Detect (Device & User Profiling)

Resolve (Wire Data)

Features and Benefits Summary

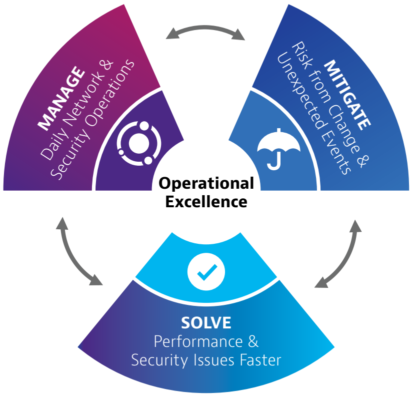
- End-user experience delivers in-depth situational awareness for each IT stakeholder; thereby ensuring optimal service delivery
- High-fidelity forensic visibility into every network conversation over time reducing mean time to resolution
- Advanced service path visibility ensures immediate problem domain isolation across a complex hybrid IT environment
- Automated threat assessment, creating a new line of defense utilizing an enriched flow record for immediate identification of rogue activity
- An interactive IP Viewer that visualizes relationships between User, IP, MAC, and application usage in the network.
- A new, easy wizard-driven configuration method for Threat Profiles allows you to quickly and confidently define the hosts and services you want to monitor for suspicious traffic patterns

GigaFlow Deployment

GigaFlow offers an extensible, easy deployment architecture with carrier grade scalability and a "pay-as-you-grow" pricing model. Options are available in various software capacities based on number of flows supported and emitting sources to satisfy the needs of any size organization.

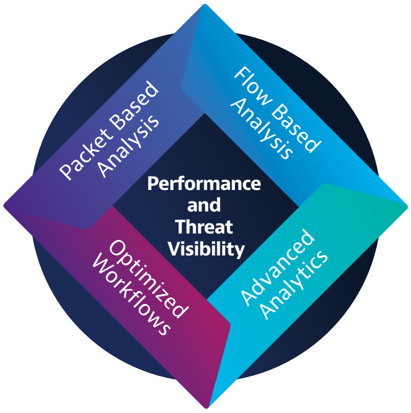
Observer Overview

Observer is a network performance monitoring and diagnostics (NPMD) solution is ideally suited for satisfying business goals and overcoming challenges across the entire IT enterprise lifecycle.



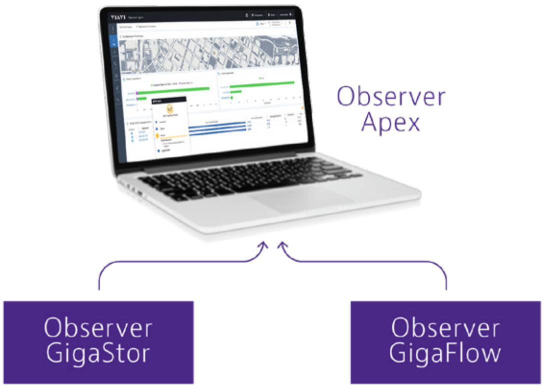
With the release of Observer v18, enriched flow data from GigaFlow and packet-level wire data from GigaStor now coexist in Observer Apex. This means all levels of expertise have access to comprehensive views of performance and threat landscapes across their environments, using preferred data sources for QoS measurements, baselining, capacity planning, and more. This single, integrated interface improves operational efficiencies through boosted data quality, intuitive visualizations, and simplified workflows for any level of IT user.

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.



Leveraging high-fidelity data from GigaFlow and GigaStor, Apex serves as the launch point for fast troubleshooting workflows or security investigations

Using this data Observer offers active defense security capabilities like threat hunting and profiling giving NetOps and SecOps teams actionable operational information on IT resource health and status.



VIAVI Solutions

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

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

Product specifications and descriptions in this document are subject to change without notice.
gigaflow-br-ec-nse-ae
30187572 902 0320