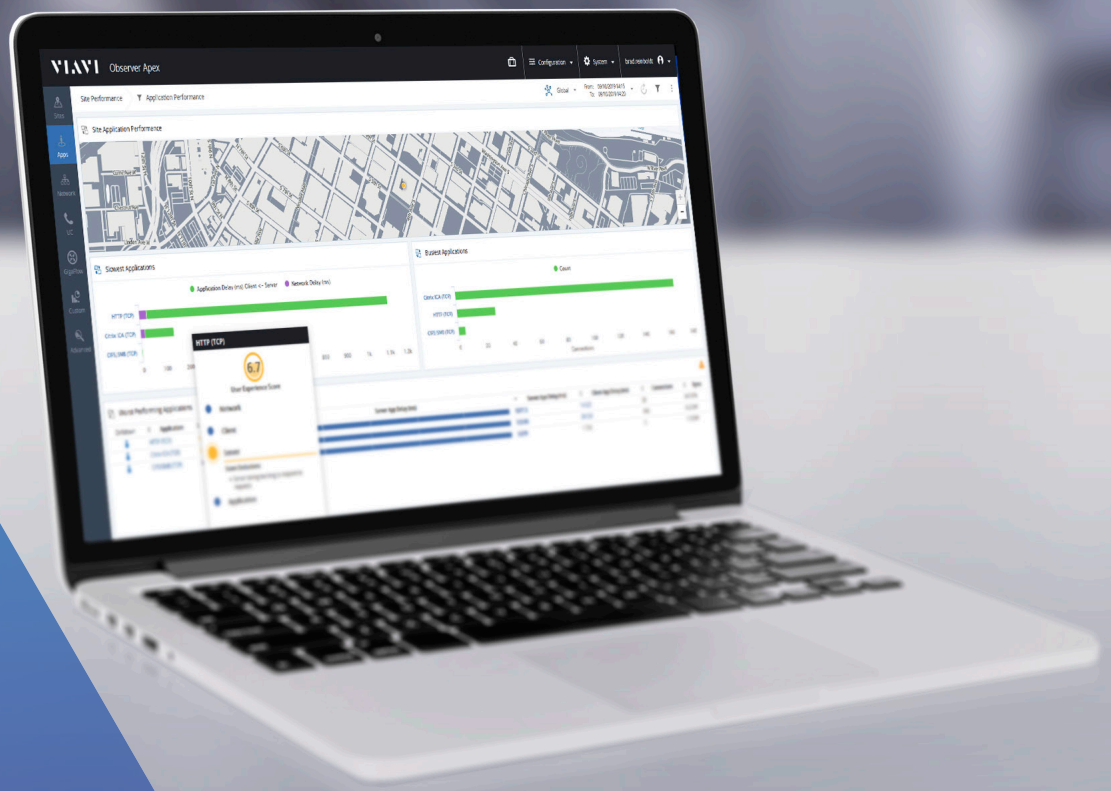




VIAVI Solutions



Brochure

VIAVI Observer Apex and GigaTest

Core-to-Cloud End-User
Experience Scoring

The Network is Everywhere

Today's network knows no borders yet every IT service still depends on it. If the network falters, app delivery can quickly degrade resulting in poor customer satisfaction and reduced business profitability.

Observer Apex to the rescue. Apex is the first network performance monitoring (NPM) solution to generate an end-user experience (EUE) score on every transaction whether remote user, SaaS cloud-based apps, or on-premises assets.

Observer GigaTest, available on Apex adds active test insight to packet details for clarity into cloud-hosted apps and users wherever they reside. When combined with enriched flow, Apex eliminates the challenges of maintaining service visibility of hybrid IT.

When service anomalies do arise or potential security breaches are detected, efficient workflows empower NetOps, DevOps, and SecOps groups to uncover root cause and fix it, fast.

How GigaTest Works

Active testing eliminates blind spots, complements packet and flow data, and builds on the recently announced Observer 3D initiative. Select from three different agents to work alongside your packet capture and flow analysis to provide complete network visibility. Mix and match agents depending on where your visibility gaps exist:

- Windows Agent – for Windows-based server or workstation user devices
- Virtual Agent – available for most popular VM environments
- Raspberry Pi Image – for use on Raspberry Pi hardware within any on-premises enterprise environment

Once your agents are deployed, add the GigaTest functionality to your Apex instance to process the metadata created by the agents—it's that simple and you are up and running.

Why do I need GigaTest?

There are two primary use cases for integrated active testing:

- Providing visibility into cloud-based SaaS applications
- Understanding and assuring the remote users' service experience

Integrating active test data with packet and flow, delivers comprehensive end-to-end network monitoring coverage. IT teams can confidently answer questions such as:

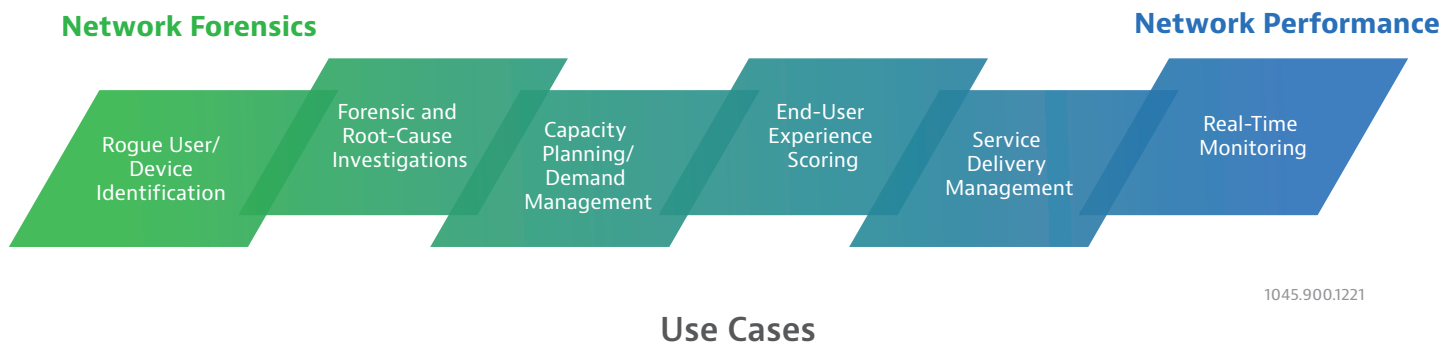
- Which specific domain is being impacted, can the issue be isolated to the network, application, server, or client?
- Is there a problem affecting a single site or multiple sites?
- Is there a problem affecting access to a SaaS application by users? Is it the SaaS provider or a problem on our side, whether on-premises or remote user?

Continuous, ongoing monitoring enables IT teams to maintain visibility proactively and build baselines of current SaaS and UC health — greatly increasing availability by detecting when service levels begin drifting problematically.

Get proactive and in-front of user complaints using integrated monitoring with automated analysis and scoring. It will optimize your operational efficiency, keep end-users productive, and minimize disruption to your business and your customers.

Active + Passive = the Optimal Combination

	Passive: Packets/Flow	Active Test	Active + Passive
24/7 monitoring	X	✓	✓
Availability	X	✓	✓
Real User Visibility	✓	X	✓
SaaS App Assurance	✓	✓	✓
Work form Home	✓	✓	✓
Forensic Analysis	✓	X	✓
Utilization/Storage	✓	X	✓
Site-to-Site Quality (e.g. UC)	✓	✓	✓



"The most recent study found data center networks vulnerable to downtime events across the network. Core data centers experienced an average of **2.4 total facility shutdowns per year** with an average duration of more than **two hours (138 minutes)**."

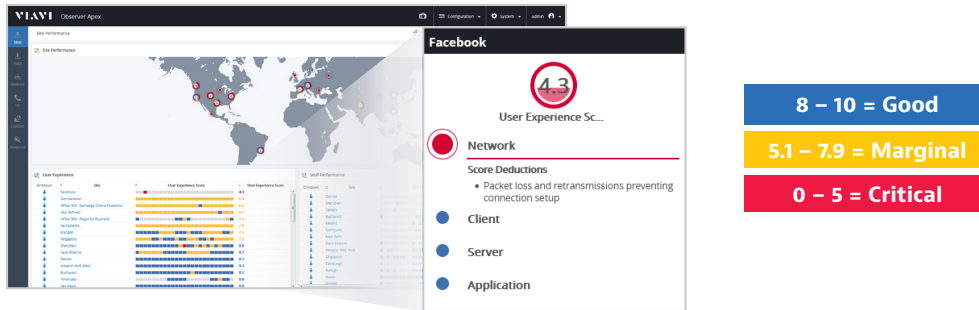
Poneman Institute, Data Center Downtime at the Core and the Edge: A Survey of Frequency, Duration and Attitudes. January 2021

Network Performance

End-User Experience Scoring

Apex removes the guesswork from assessing user satisfaction using patented analytics powered with machine learning to accurately measure all conversations. Each is scored between 0 to 10 using color coding and grading to represent performance from the user's perspective taking into account unique environmental and application behavior to eliminate false positives.

Scores provide visibility into a single user's experience or can be expanded to view groups of users defined by site, geolocation, or other constructs as needed. Apex takes this a step further by isolating the problem to the network, client, server, or application domain with easy-to-understand problem statements.



Custom Business Level Dashboards

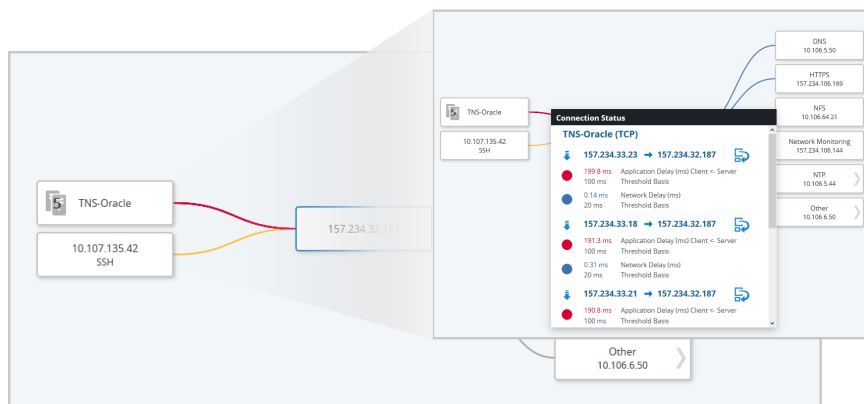
Geolocation-based, user-defined dashboards enable integrated, enterprise-wide situational awareness into service delivery health.

Troubleshooting Workflows

Site and technology driven workflows integrated with end-user experience scoring means IT teams can gain instant world-wide situational awareness of all resources and then quickly drill down to an individual user for rapid problem resolution.

On-Demand Multi-Tier Application Intelligence

On-demand application dependency mapping offers fast discovery of app interdependencies and ad hoc rendering of maps visualizing these complex relationships with clarity. With a single mouse-click, Apex generates the entire map, and automatically determines the worst connections based on application and network delay threshold deviations. All connections are then sorted by status (critical, marginal, and good), so users can quickly assign troubleshooting priority.

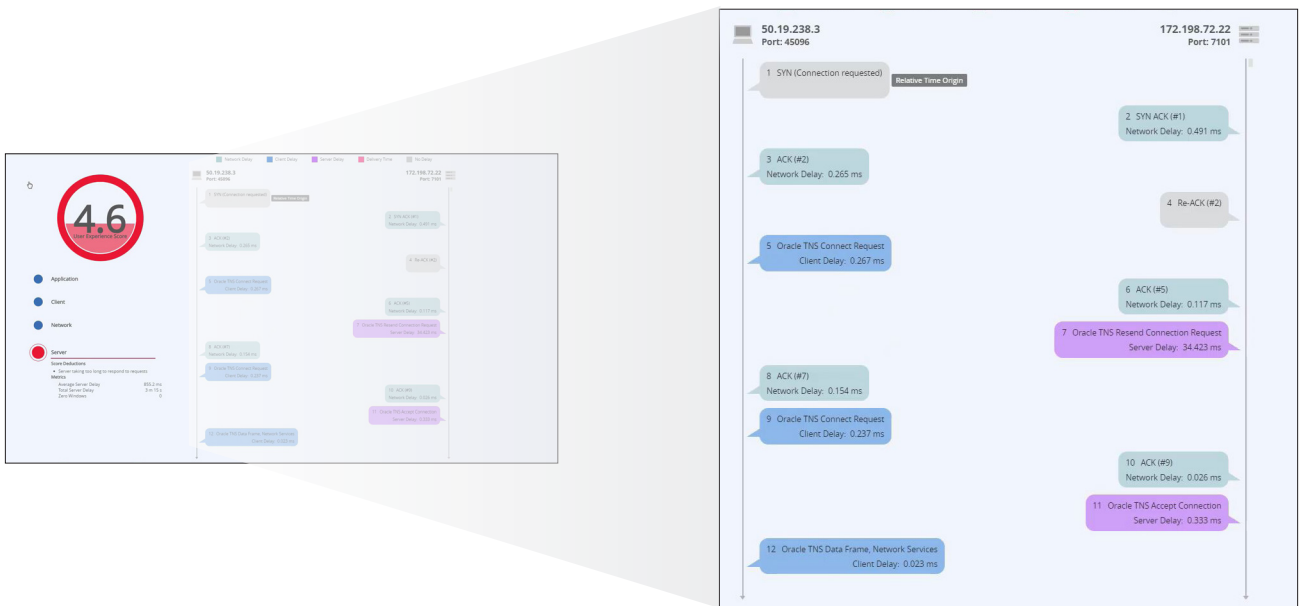


Network Forensics

Observer network forensics integrates two complementary data sources; traffic and enriched flow while maintaining access for extended periods of time. Getting to the root cause of many performance issues and most cybersecurity breaches begins with metadata and intuitive dashboards but frequently ends with logical workflows leading to visibility into underlying data, sometimes days after the event. That's why Observer keeps supporting details for longer periods of time.

As described above, nearly all performance anomalies are quickly isolated with end-user experience scoring. However, when higher fidelity details are required, supporting data is instantly available.

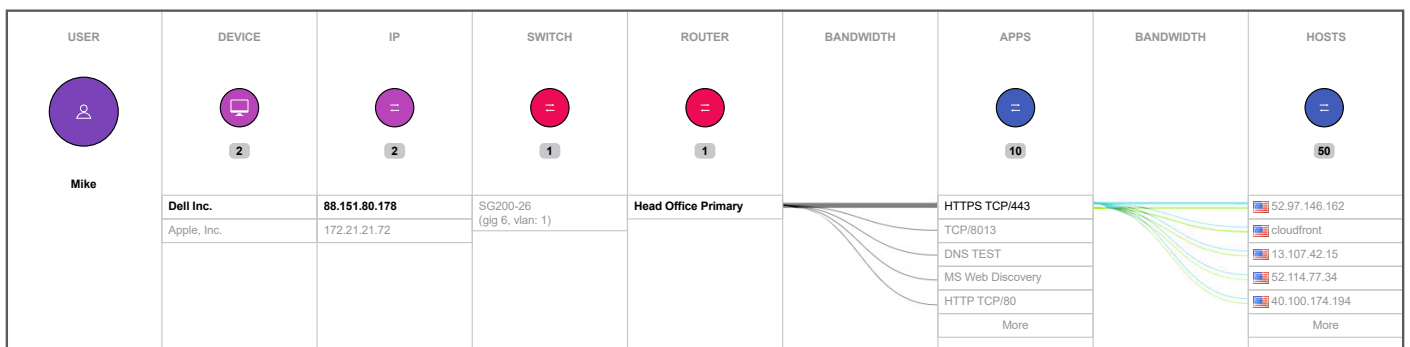
Traffic Forensics



End-user experience score with associated connection dynamic conversation breakout

With packet data captured by Observer GigaStor, the entire conversation of every transaction—from beginning to end—is available for review and investigatory actions. Global dashboard to individual packets, whenever required in just a few steps.

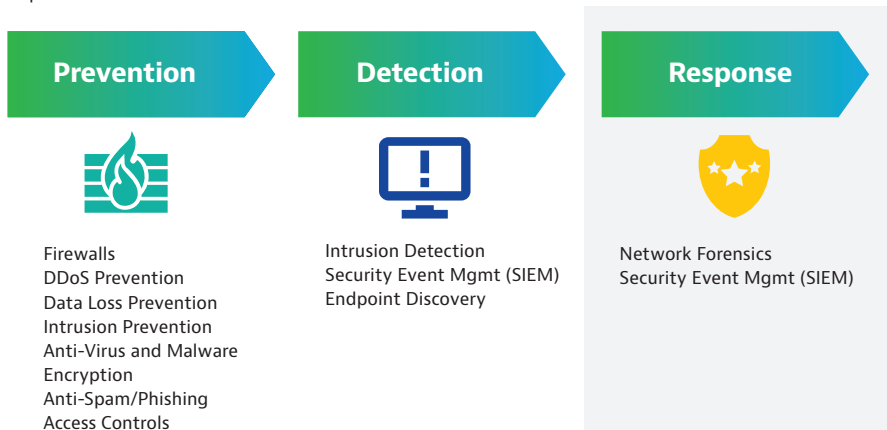
Enriched Flow Forensics



Observer GigaFlow IP Viewer visualization of user activity across the network infrastructure for every transaction

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 address, MAC address, and application usage in the network. Users can simply enter a name/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.

When it comes to cybersecurity, the best protection against threats demands a three-prong strategy of prevention, detection, and response.

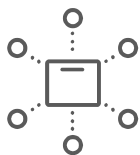


1044.900.1221

For many organizations, the focus is frequently prevention and detection—until a breach is confirmed and the urgent war room scenario begins to respond to the threat. It is at this point having ready access to all network activities going back-in-time from the present is critical to limiting damage and confidently sounding the “all clear”.

This is where network forensics is priceless. Observer delivers with the combined power of traffic and enriched flow forensics getting your business back and running by answering the how/who/what/where of every cybersecurity breach and the bad actor(s) that perpetrated the event.

Traffic Forensics / **Enriched Flow Forensics**



How are or were devices connected?



Who is or was communicating?



What is or was transmitted?



How far did the questionable actions extend?

By answering these questions, IT teams can quickly determine the “attack vector” (how the malefactor circumvented prevention and detection measures to gain entry) and what IT services, devices, or sensitive customer/business data were compromised. Once this is accomplished, containment is possible and damage assessment finalized.

Features and Benefits Summary

- Machine learning powered EUE scoring takes the guesswork out of troubleshooting
- Site or technology-based workflows synchronized with EUE scoring for fast-path to resolution navigation
- Available integrated GigaTest active test for enhanced scoring into EUE SaaS applications

- On-demand application dependency mapping enables fast multi-tier application visibility with no configuration required
- Business level dashboards for global awareness into IT service availability for NetOps, SecOps, and DevOps
- Integrated network performance and forensics for fast service anomaly and rapid cybersecurity breach response

Observer 3D Overview

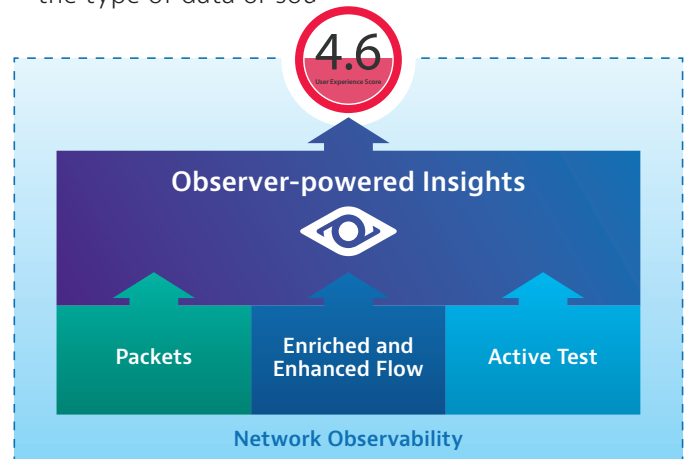
Observer 3D is a comprehensive network performance monitoring (NPM) solution that offers valuable insight and assistance to network, operations, and security teams. Apex collects transaction metadata from multiple data sources for calculation of the EUE score.

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:

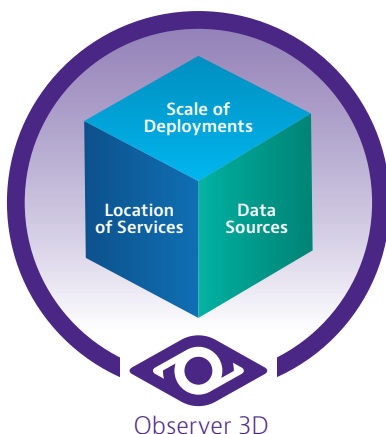
- **Location of Services** – Observer 3D provides observability into every hosting environment, whether private cloud, public cloud, SaaS applications, remote users, on premise in branch offices or in the data center. No matter the location, VIAMI has you covered. To learn more about how Observer 3D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

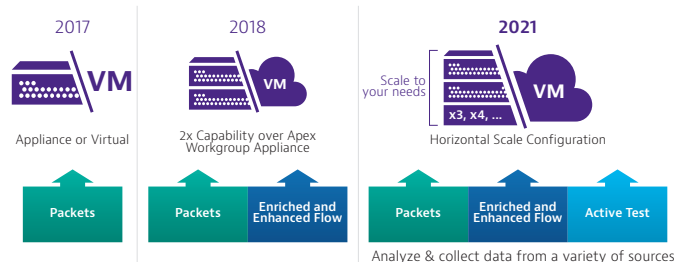


1041.900.1221

- **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—VIAMI 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.



1043.900.1221



1042.900.1221



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

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

© 2021 VIAMI Solutions Inc.
Product specifications and descriptions in this
document are subject to change without notice.
Patented as described at
viavisolutions.com/patents
apex-br-ec-ae
30176200 909 1221

viavisolutions.com