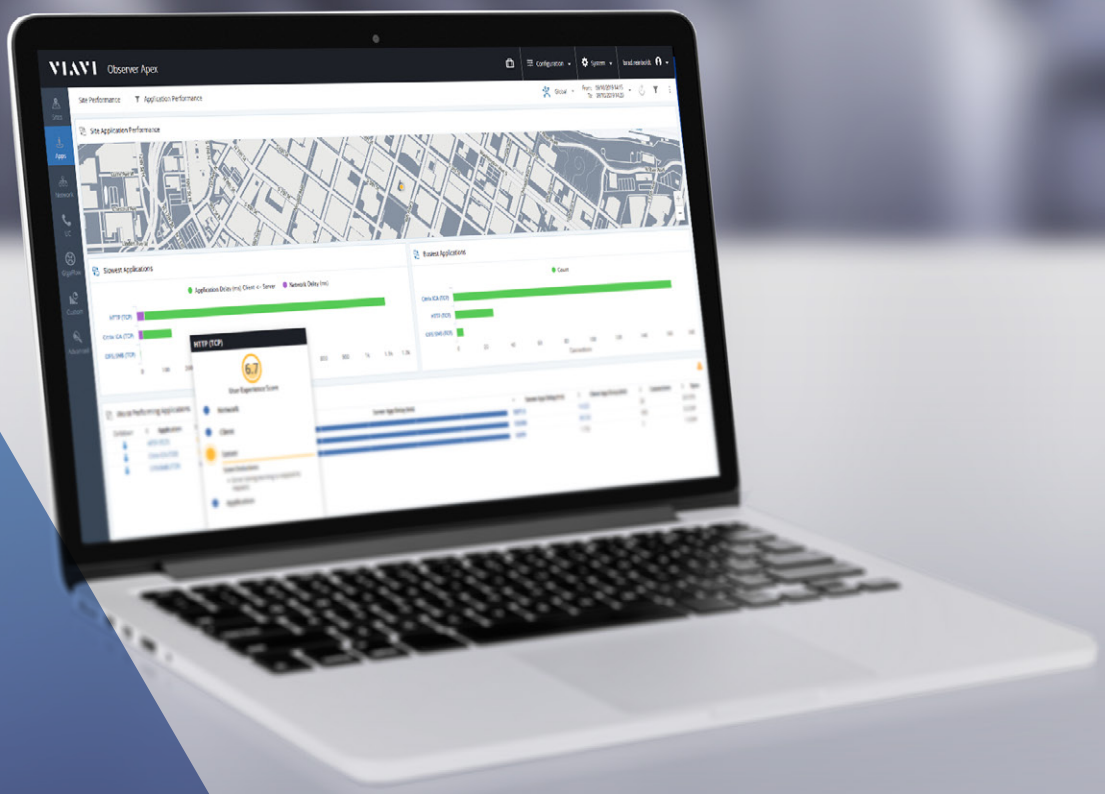
VIAVI Solutions



Brochure

VIAVI Observer
Apex
Centralized Performance and Security Management

Core-to-Cloud IT Operational Clarity

Observer® Apex leverages End-User Experience Scoring and advanced threat intelligence to deliver unified, comprehensive visibility into IT resource health and status.

When service problems do arise or potential security issues are detected, efficient workflows lead IT teams quickly to root cause and resolution.

Built-in security features like real-time threat mapping, host/device traffic profiling, and threat hunting aids IT teams when passive security initiatives like firewalls, IDS/IPS, and SIEMs are circumvented.

Know Your Network Like Never Before

What's connected? Who is talking on the network? What are they saying? Log files and scanning IP addresses alone will not always provide the answer. Only Apex can do it by combining high-fidelity transaction, infrastructure, device, host, and user data then applying advanced analytics and machine learning.

Metadata and underlying records are retained for extended periods of time to power real-time intelligence or post-event investigations.

Network Security | **Network Performance**

Threat Mapping/ Assessments	Host/Device Traffic Profiling	Rogue User/ Device Identification	Forensic and Root-Cause Investigations	End-User Experience Scoring	Service Delivery Management	Real-Time Monitoring

Use Cases

"Although often separate, NetOps and SecOps teams share the common goal of maintaining secure, high-performance network infrastructures. Infrastructure and operations leaders can leverage shared data and tools to optimize budgets, avoid duplication of effort and improve the end-user's experience."

"Align NetOps and SecOps Tool Objectives With Shared Use Cases"
By Gartner analysts Sanjit Ganuli and Lawrence Orans, July 24, 2018

Introducing Observer v18

Now, with the release of Observer v18, packet and enriched flow data now coexist in Observer Apex. This means all levels of expertise access to various tiers of IT visibility, using their 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.

Network Performance

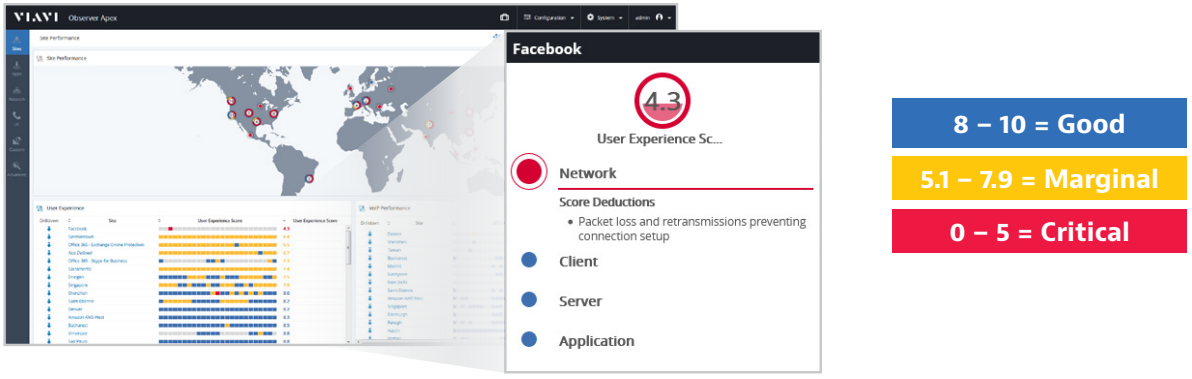
Site Dashboards and Workflows

Geolocation-based dashboards provide global intelligence of IT service health at the regional, country, city, or data center levels, with even more granularity to individual service groups such as accounting. When combined with End-User Experience Scoring, IT teams can gain instant world-wide situational awareness of all resources and then, when required, quickly drill down to an individual user for rapid problem resolution.

End-User Experience Scoring

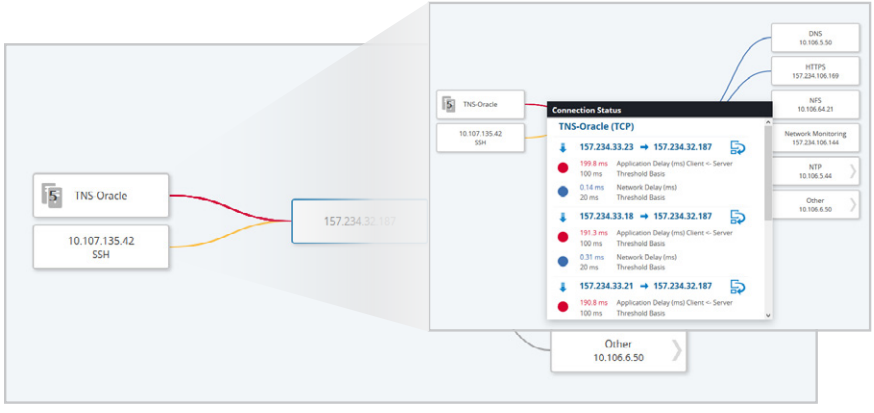
Apex removes the guesswork from assessing user satisfaction using patented analytics powered with machine learning to accurately measure all conversations. Each is scored between 0 to 10 using color coding and grading to represent performance from the user's perspective taking into account unique environmental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



On-Demand Multi-Tier Application Intelligence

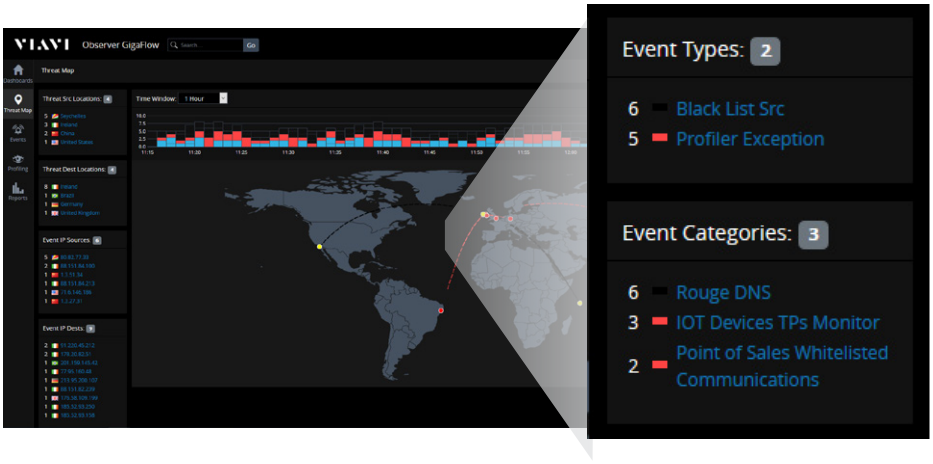
On-demand application dependency mapping offers fast discovery of app interdependencies and ad hoc rendering of maps visualizing these complex relationships with clarity. With a single mouse-click, Apex generates the entire map, and automatically determines the worst connections based on application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



Network Security

Threat Map with Security Workflows

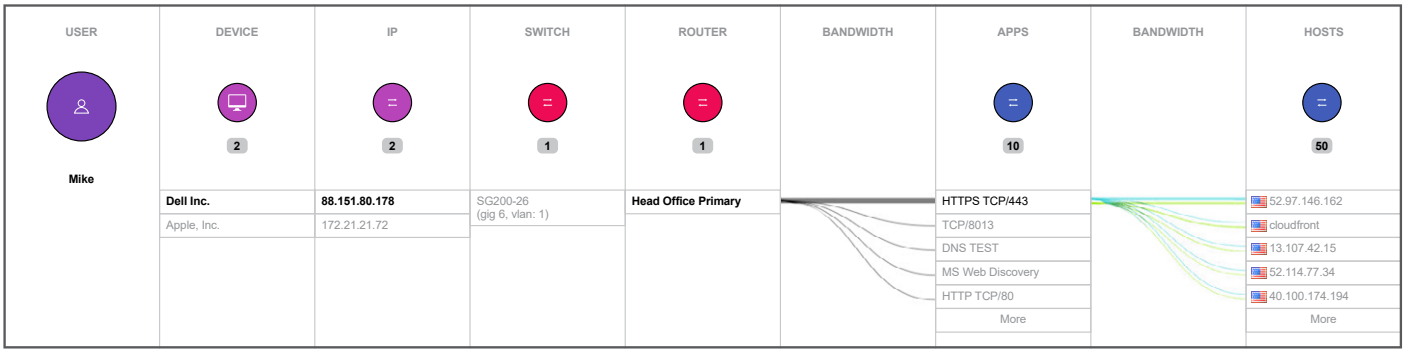
Integrated threat maps offers IT teams global, real-time visibility into the current security risk vectors that are potentially impacting IT resources and users. IT teams can quickly gain situational awareness and initiate rapid response actions with targeted workflows or hunting efforts based on severity assessments.



Host/Device Traffic Profiling

Define groups of critical or at-risk assets like point-of-sale or ATMs; then gain instant visibility via alerts when exception activities or sessions not defined in white list rules are detected on these existing or new devices.

IP Viewer



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.

Features and Benefits Summary

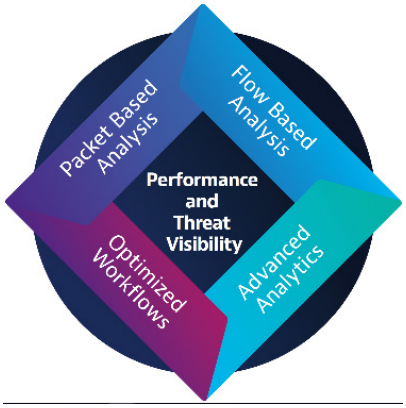
- Machine learning powered End-User Experience Scoringtakes the guesswork out of troubleshooting application and service issues
- Dual site or technology-based workflows synchronized with End-User Experience Scoring for fast-path to resolution navigation
- On-demand application dependency mapping enables fast multi-tier application visibility with no configuration required
- Security forensics and reconstruction using wire-data from GigaStor provides detailed breakouts into every network conversation
- Integrates with GigaFlow for in-depth global threat identification and advanced traffic profiling of every host and device
- 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
- An IP Viewer that lets you navigate between User, IP, MAC Address, and application usage in the network

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.

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

Putting Flow and Wire Data together with Apex's Workflows

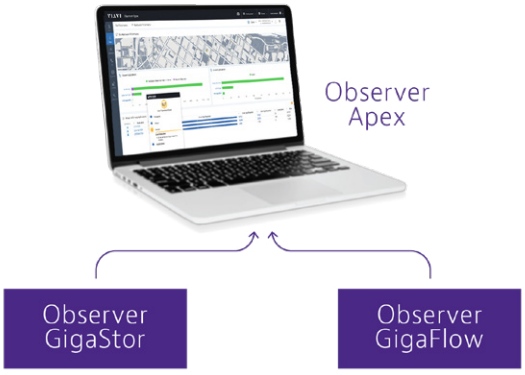


Observer v18 delivers unification of packed and enriched flow data with optimized workflows and powerful analytics. As a result, the complementary nature of wire data and flow data becomes clear:

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.

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 Apex 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.

apex-br-ec-ae
30176200 907 0320