Brochure

VIAVI

Observer Apex

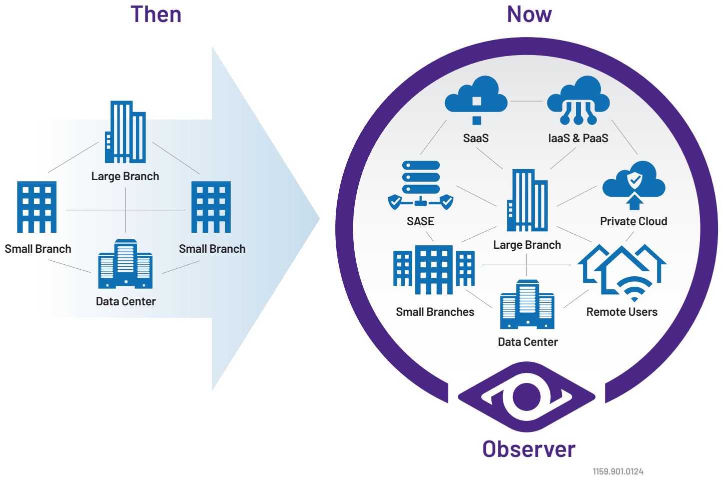
Built for NetSecOps: See More. Investigate Faster.

Delivering shared network and security insight with advanced analytics and evidence-driven investigation.

THE NETWORK IS EVERYWHERE

Complex, multi-tier applications hosted on-premises or in cloud-based resources including SaaS, IaaS, PaaS,and SASE. Users accessing apps anywhere and everywhere is the new norm. Today's network knows no borders, yet every IT service still depends on it.

If any component of the network or service architecture falters, app delivery can quickly degrade resulting in poor customer satisfaction and reduced business profitability. To avoid this, comprehensive service observability is a must.



Observer Apex delivers visibility where you need it most, and is the first performance management solution to generate an End-User Experience (EUE) score on every transaction. By correlating packets, metadata, and enriched flow, Apex provides deep insight into how applications, services, and infrastructure perform across hybrid environments. Organizations can choose the data sources that best align with their operational needs and budgets while maintaining the flexibility to expand visibility as environments evolve.

Apex provides global awareness of IT service health and performance while also enabling teams to move quickly from detection to investigation when anomalies arise. Integrated alerts, contextual analytics, and investigation workflows help NetOps, DevOps, and SecOps teams rapidly determine whether issues originate from the network, application, client, or a potential security event.

By combining performance insight with forensic-level investigation capabilities, Apex accelerates root-cause analysis and enables teams to resolve both operational and security incidents with greater confidence.

COMMAND CENTER FOR NETSECOPS

- **Machine learning powered automated EUE Scoring** converts multiple KPIs into a single easy-to-understand metric combined with detailed score deductions that automatically isolate the problem domain(s) providing the information needed to prioritize swift remediation
- **Observer Threat Forensics with Threat Intelligence powered by CrowdStrike®** combines packet-level insight with adversary intelligence to enrich detection and investigation workflows. By embedding threat context directly into the investigation experience, teams can accelerate triage, validate threats with high confidence, and gain actionable visibility across hybrid environments.
- **Flexible data source options** including packets, metadata, and enriched flow offer the right view for every stakeholder from network engineer to line of business owner
- **Customizable dashboards** for global operational intelligence with efficient workflows enable fast problem identification and resolution for NetOps, SecOps, and DevOps

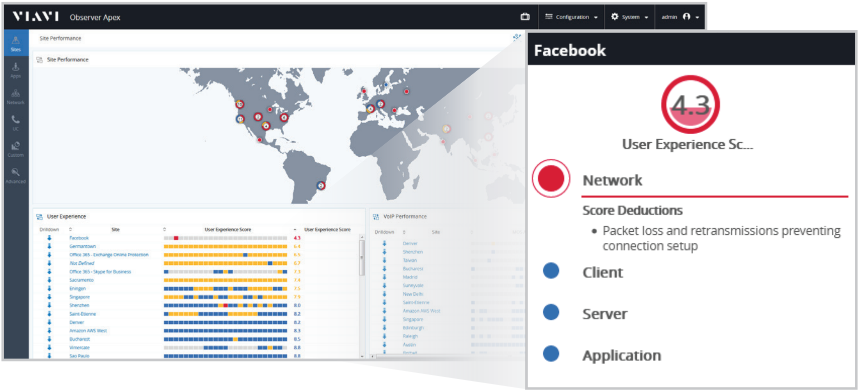
- **On-Demand Application Dependency Mapping (OD-ADM)** enables fast, accurate multi-tier application visibility with no configuration required
- **Integrated performance management and forensics** for fast service anomaly and rapid cybersecurity breach response
- **Deep Packet Inspection (DPI)** capabilities address the challenge of understanding network traffic composition and determining if non-critical traffic is negatively impacting key business services and end-users
- **Digital certificate analysis**, identifies certs that have expired or are coming up for expiration and highlights outdated protocols, helping to ensure both compliance and uninterrupted service for users
- **Unified Communications (UC)** workflows guide UC experts from global summaries and site-specific views to interactive call details. Packet and flow data are seamlessly integrated to visualize a single point-to-point or complex multi-point call's path through the network infrastructure
- **Cloud flow log ingest**, and analysis provides needed visibility into cloud traffic, aiding in security threat detection, anomaly identification, and compliance adherence for cloud environments such as Amazon Web Services (AWS) and Microsoft Azure
- **Flexible deployment options** from purpose-built appliances for the data center to virtual machine images for simple, efficient cloud deployments

PERFORMANCE MANAGEMENT

End-User Experience Scoring

Apex removes the guesswork from assessing user satisfaction with patented analytics powered by machine learning to accurately analyze and evaluate 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 a site, a service, or a global enterprise view. Apex takes this a step further by isolating the problem to the network, client, server, or application domain with easy-to-understand problem descriptions.



Packet loss and retransmissions preventing connection setup

8 – 10 = Good

5.1 – 7.9 = Marginal

0 – 5 = Critical

Custom Business-Level Dashboards

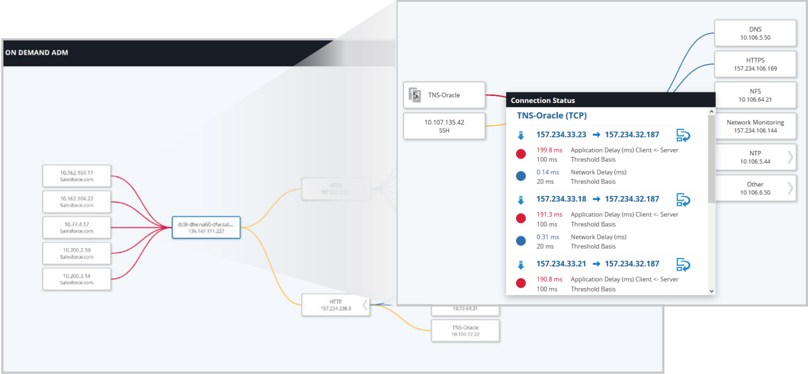
Geolocation-based, user-defined dashboards enable integrated, enterprise-wide situational awareness into service delivery health.

Troubleshooting Workflows

Site and service 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

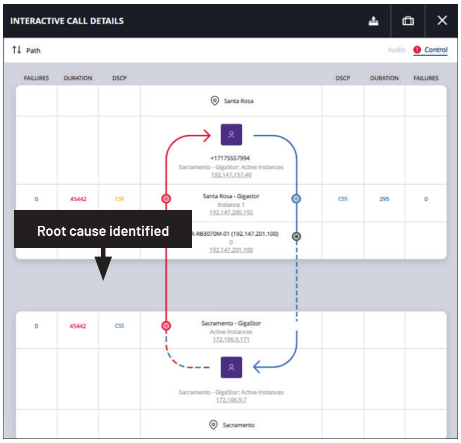
OD-ADM offers multi-tier service awareness, fast discovery of app interdependencies, and ad hoc rendering of maps visualizing these complex relationships with clarity. With a single mouse-click, Apex generates the entire map, and automatically pinpoints and highlights the worst connections so users can quickly assign troubleshooting priority.



Automated application dependency maps with integrated end-user experience scoring.

Unified Communications (UC)

Apex UC dashboards and workflows efficiently guide VoIP and UC experts from global summaries and site-specific views to unique and interactive visualizations of call details. Only Observer seamlessly combines packet and flow data to visualize a single point-to-point or complex multi-point call's path through the network infrastructure, pinpointing the origins of quality degradation while offering one-click access to relevant packet data when needed.



Interactive Call Details identify root causes of quality degradations.

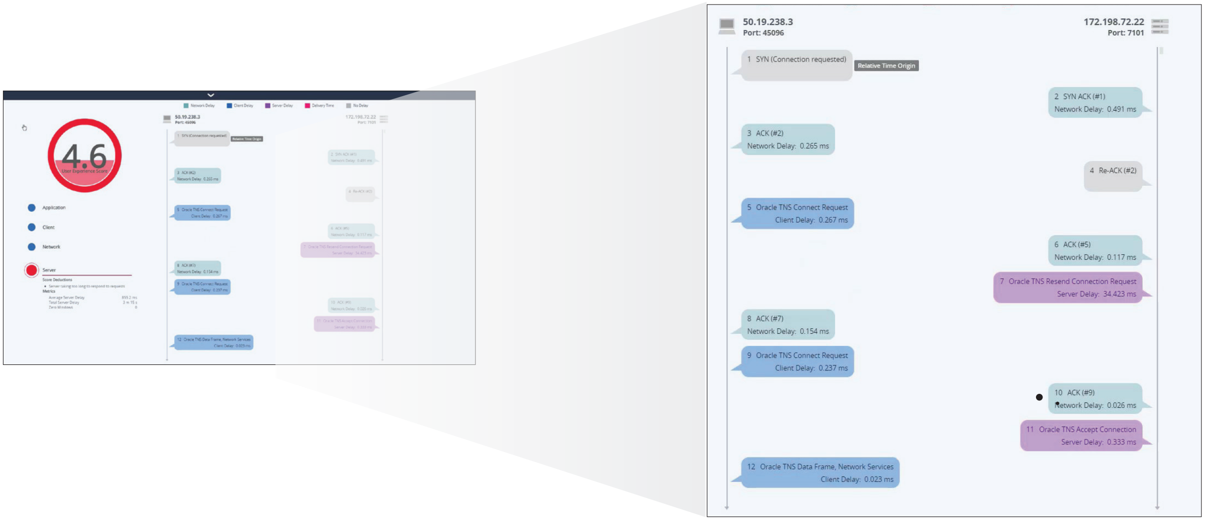
Key benefits include:

- **Visual Journey Mapping:** Transforming packet and flow data into intuitive visualizations for call journeys
- **Swift Issue Resolution:** Significantly reduce MTTR with easy root cause identification for UC performance issues
- **User-Friendly Interface:** Easy-to-use and understand interface that allows you to empower non-experts with simplified depictions of complex multi-point and point-to-point UC calls

NETWORK AND SECURITY FORENSICS

Observer network forensics integrates two complementary data sources; packets and enriched flow along with the ability to retain this data for extended periods of time. Virtual machine image deployment options enable collection and analysis of enriched flow and packets for cloud hosted apps. Getting to the root cause of many performance issues and 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, many performance anomalies are quickly isolated with end-user experience scoring. However, when higher-fidelity details are required, supporting data is instantly available.



50.19.238.3
Port: 45096

172.198.72.22
Port: 7101

1 SYN (Connection requested)

2 SYN ACK (#1)
Network Delay: 0.491 ms

3 ACK (#2)
Network Delay: 0.265 ms

4 Re-ACK (#2)

5 Oracle TNS Connect Request
Client Delay: 0.267 ms

6 ACK (#5)
Network Delay: 0.117 ms

7 Oracle TNS Resend Connection Request
Server Delay: 34.423 ms

8 ACK (#7)
Network Delay: 0.154 ms

9 Oracle TNS Connect Request
Client Delay: 0.237 ms

10 ACK (#9)
Network Delay: 0.026 ms

11 Oracle TNS Accept Connection
Server Delay: 0.333 ms

12 Oracle TNS Data Frame, Network Services
Client Delay: 0.023 ms

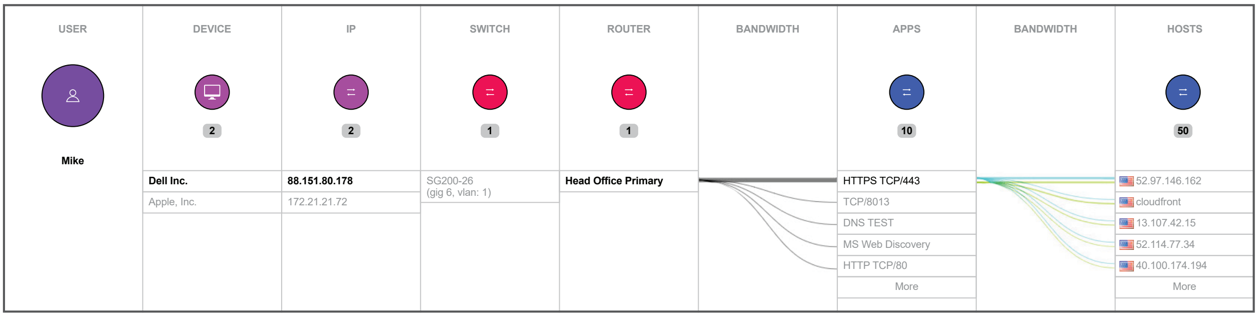
End-user experience score with associated connection dynamic conversation breakout.

Conversation Forensics

With packet data captured by Observer, every transaction—from beginning to end—is available for review and investigatory actions. Efficient workflows guide users from the global dashboard to individual packets, whenever required, in just a few steps.

With the added visibility provided by DPI-driven application identification, Observer delivers advanced network traffic insights. This capability allows network engineers to easily identify traffic running on non-standard ports, quantify non-critical traffic, and take a deeper look into protocols like HTTP and HTTPS. Observer's DPI capabilities empower you to identify over 4,300 applications, providing at-a-glance clarity on whether a conversation is a business transaction or something else.

Enriched Flow Forensics



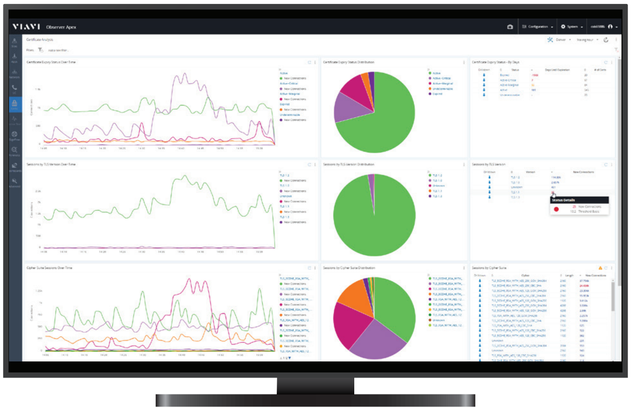
USER	DEVICE	IP	SWITCH	ROUTER	BANDWIDTH	APPS	BANDWIDTH	HOSTS
	2	2	1	1		10		50
Mike	Dell Inc.	88.151.80.178	SG200-26 (gig 6, vlan: 1)	Head Office Primary		HTTPS TCP/443		52.97.146.162
	Apple, Inc.	172.21.21.72				TCP/8013		cloudfront
						DNS TEST		13.107.42.15
						MS Web Discovery		52.114.77.34
		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

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

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 across the network. Users can simply enter a name/userid or IP address 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.

Digital Certificate Management

Observer monitors SSL/TLS handshakes as it analyzes your network traffic, identifying digital certificates that have expired or are nearing expiration and providing proactive notifications. It identifies servers publishing insecure sessions, highlights outdated protocols, validates compliance, and helps to ensure uninterrupted service for users.



Certificate Analysis Dashboard provides TLS version, certificate expiry status, and Cipher Suite distributions.

For Network Engineers and administrators, ensuring uptime and customer satisfaction is essential for delivering web-based services. Transitioning from manual reporting methods, such as spreadsheets, to a proactive certificate analysis approach simplifies the process, safeguarding your company against potential certificate-related outages.

Key benefits Include:

- **Proactive Monitoring:** Real-time analysis, reporting, and notifications keep you ahead of certificate expiration
- **Enhanced Security Insights:** Obtain a clear view of the SSL or TLS versions in operation, enabling swift retirement of outdated or insecure protocols
- **Uninterrupted Service:** By identifying and remediating certificate-related issues, potential outages are averted, ensuring a seamless user experience

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

Prevention		Detection	Response
• Firewalls • DDoS Prevention • Data Loss Prevention • Intrusion Prevention • Anti-Virus and Malware	• Encryption • Anti-Spam/Phishing • Access Controls • Endpoint Security	• Intrusion Detection • Security Event Mgmt (SIEM) • Endpoint Discovery	• Network Forensics • Security Event Mgmt (SIEM)

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.

Traffic Forensics

How are or were devices connected?

Who is or was communicating?

Enriched Flow Forensics

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.

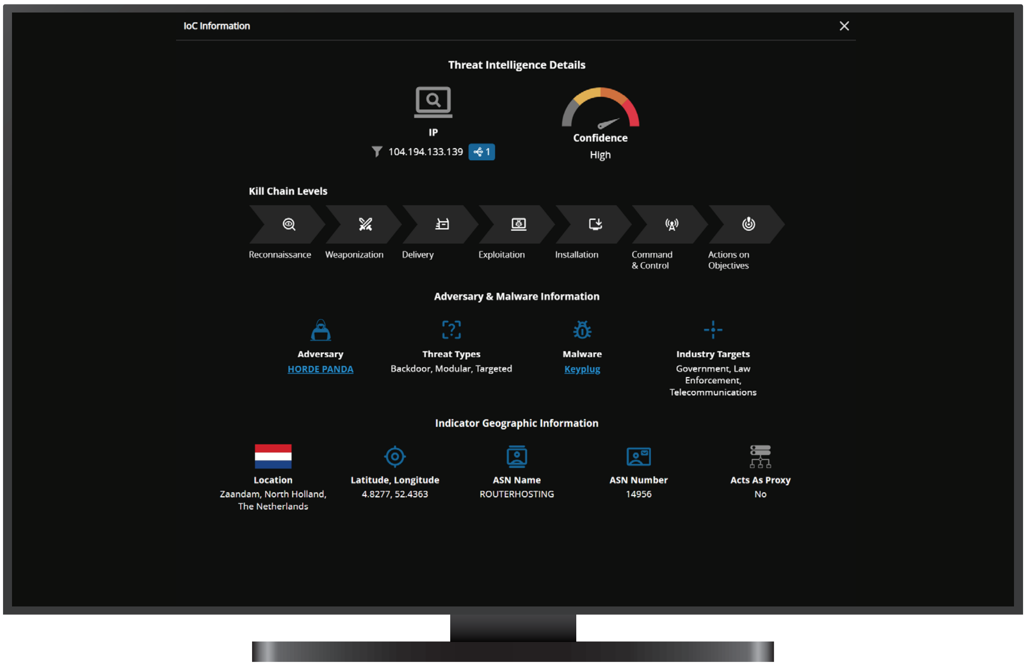
OBSERVER THREAT FORENSICS

Actionable Threat Visibility for Confident Investigation and Response

Observer Threat Forensics adds a new dimension to network forensics, infusing enriched flow and packet-layer evidence with continuously updated Threat Intelligence powered by CrowdStrike®. This enables teams to correlate adversary behavior with suspicious traffic patterns, security alerts, and performance degradations in real time.

By embedding Indicators of Compromise (IOCs), attacker TTPs, and adversary context directly into the investigation experience, Observer enables analysts to validate threats quickly without manual data stitching or delayed enrichment. Integrated alerts and investigation workflows allow security and network teams to begin triage and analysis directly within the platform, accelerating time to understanding and action.

Whether triggered by known threat indicators or unexpected network behavior, each alert provides pivot-ready access to raw packet data, enriched flow metadata, and contextual threat intelligence. This allows analysts to quickly assess impact, investigate scope, determine root cause, and respond decisively across hybrid environments.



IoC Information

Threat Intelligence Details

IP
104.194.133.139 1

Confidence
High

Kill Chain Levels

Adversary & Malware Information

Adversary
HORDE PANDA

Threat Types
Backdoor, Modular, Targeted

Malware
Keyplug

Industry Targets
Government, Law Enforcement, Telecommunications

Indicator Geographic Information

Location
Zaandam, North Holland, The Netherlands

Latitude, Longitude
4.8277, 52.4363

ASN Name
ROUTERHOSTING

ASN Number
14956

Acts As Proxy
No

Unlike traditional solutions that typically begin at "Day One," Observer Threat Forensics enables true retrospective analysis, allowing security teams to trace threats back to Day Zero. With full-fidelity network data retained over time, analysts can reconstruct the complete attack timeline, even before the first alert, to uncover root cause, entry points, and lateral movement from a single source of truth.

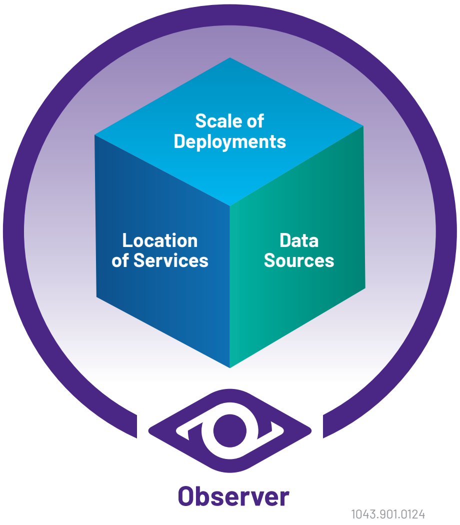
Key benefits include:

- **Real-time correlation** of network activity with adversary intelligence, reducing mean-time-to-resolve (MTTR) or uncertainty
- **Retrospective analysis** with Day Zero visibility, to uncover threat activity using forensic evidence needed prior to initial detection
- **Embedded attacker context** and TTPs that support confident triage and investigation
- **Direct pivot from alerts to packet evidence** and enriched flow data for rapid scope and impact assessment
- **Shared visibility** that strengthens collaboration between NetOps and SecOps teams

Observer Threat Forensics helps unify network and security operations with a shared, high-fidelity view that correlates performance, behavior, and threat activity. By combining network forensic evidence, enriched metadata, and threat intelligence within a unified platform, teams experience the clarity needed to accelerate response and resolve incidents with confidence.

OBSERVER OVERVIEW

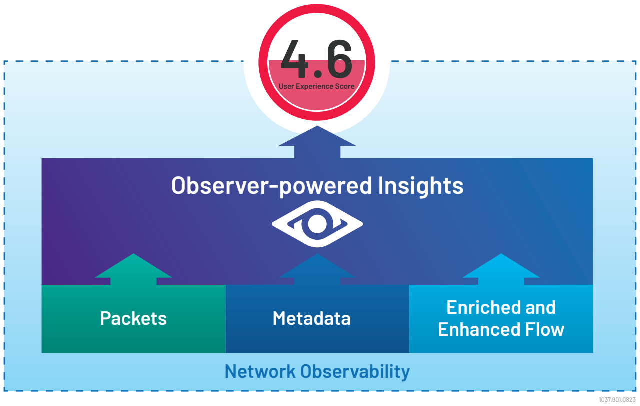
The VIAVI Observer Platform is a comprehensive performance and security management solution that empowers network, operations, and security teams with actionable insight across hybrid environments. Observer Apex collects transaction metadata from multiple data sources for calculation of the EUE score. It integrates forensic-level threat detection and investigation to deliver shared visibility and a single source of truth for NetOps and SecOps teams.



As the integrated dashboard and reporting resource, Apex serves as point of central global visibility and the launch point for rapid troubleshooting with optimized workflows that help identify root cause using packets, metadata, and enriched and enhanced flow. With embedded threat context and direct access to forensic data, security teams can validate incidents, assess impact, and rapidly isolate root cause.

Observer helps IT teams in three essential ways:

- **Location of Services** — Observer provides observability into every hosting environment, whether private cloud, remote users, on premises in branch offices or in the data center. No matter the location, VIAVI Observer has you covered.
- **Data Sources** — Observer offers flexible visibility options using packets, enriched flow, and meta data. This multi-layered approach supports both performance troubleshooting and post-breach forensics. With role-based workflows and context-rich alerts, teams can investigate confidently, from service anomalies to security threats, using the right data at the right time.
- **Scale of Deployments** — Start small and scale as operational and security demands evolve. VIAVI offers flexible deployment models and tiered subscription pricing to align with your OpEx or CapEx needs—enabling scalable visibility and NetSecOps convergence without overextending budget or resources.



Learn more at viavisolutions.com/apex

VIAVI

viavisolutions.com

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.
Patented as described at viavisolutions.com/patents