

# Observer Apex

**Built for NetSecOps: See More. Resolve Faster.**

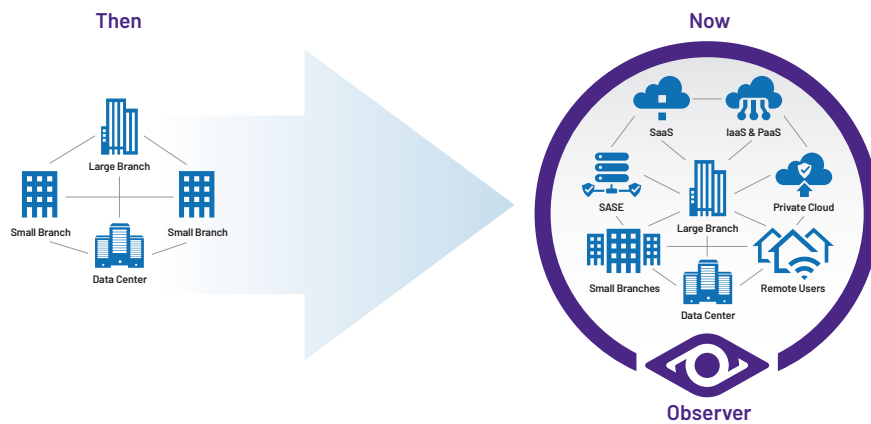
**Providing comprehensive network and security visibility through advanced analytics.**



# 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. Apex offers adaptability and visibility via multiple data sources: packets, metadata, and enriched flow. Organizations can select the sources that best fit their budgets.

Apex provides global IT service health and status awareness, aligning with its commitment to delivering comprehensive visibility. 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.

## 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
- 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 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

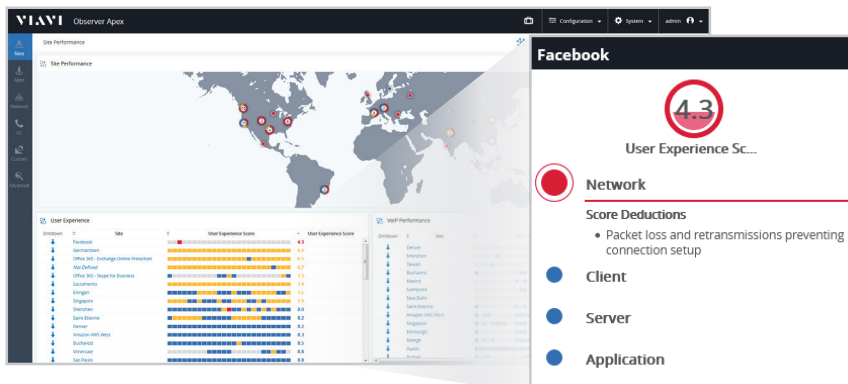
- Deep Packet Inspection (DPI) capabilities address the challenge of understanding network traffic composition and determining if non-critical traffic is negatively impacting key business services and end-users
- Observer Threat Forensics with Threat Intelligence powered by CrowdStrike® combines packet-level insight with embedded adversary context to enrich investigations, supporting faster triage, high-confidence validation, and actionable threat visibility across hybrid environments
- 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 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.





## Custom Business-Level Dashboards

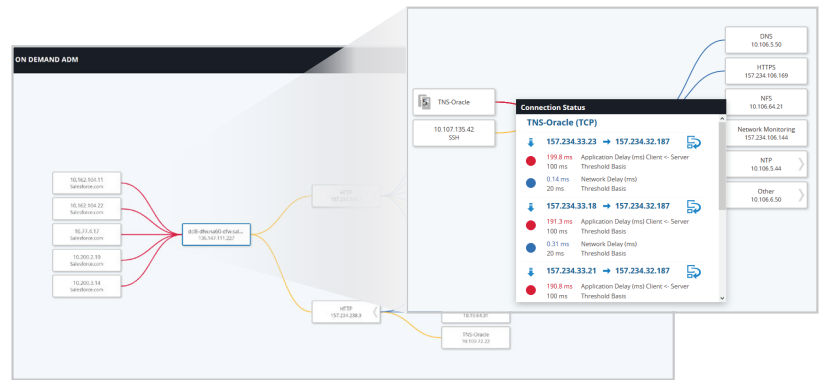
Geolocation-based, user-defined dashboards enable integrated, enterprise-wide situational awareness into service delivery health.

## 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

On-demand application dependency mapping 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.



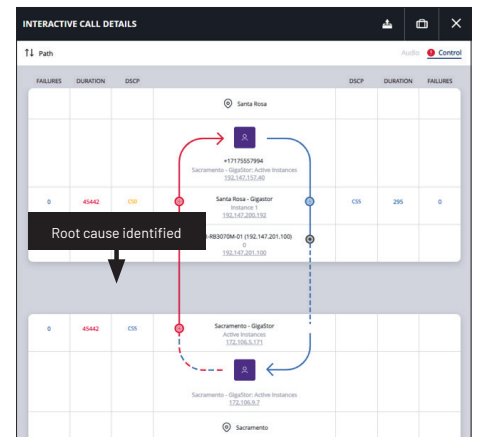
Automated application dependency maps with integrated end-user experience scoring

## 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.

### 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



Interactive Call Details identify root causes of quality degradations.

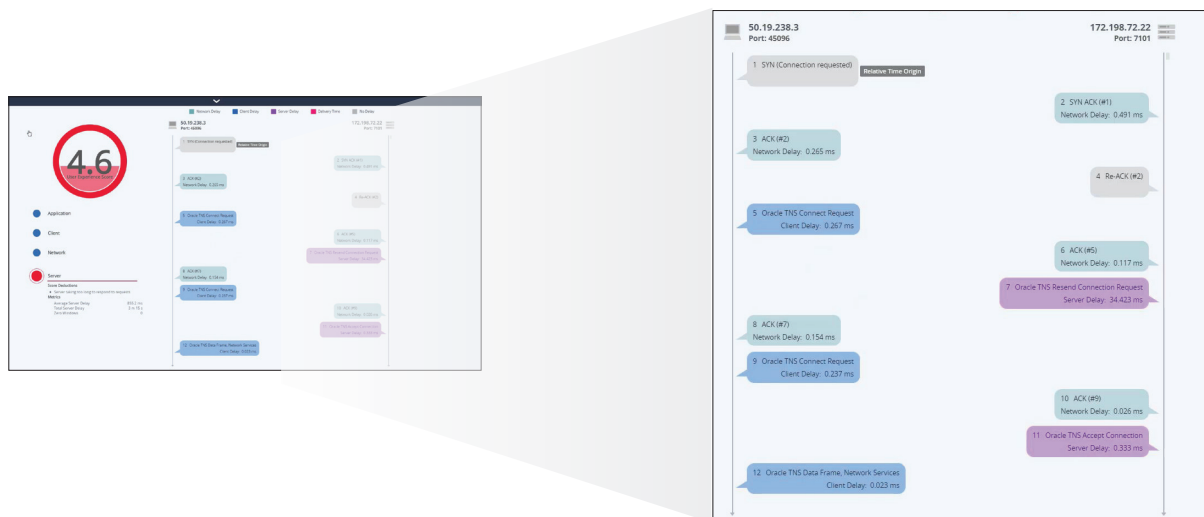




## NETWORK AND SECURITY FORENSICS

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.



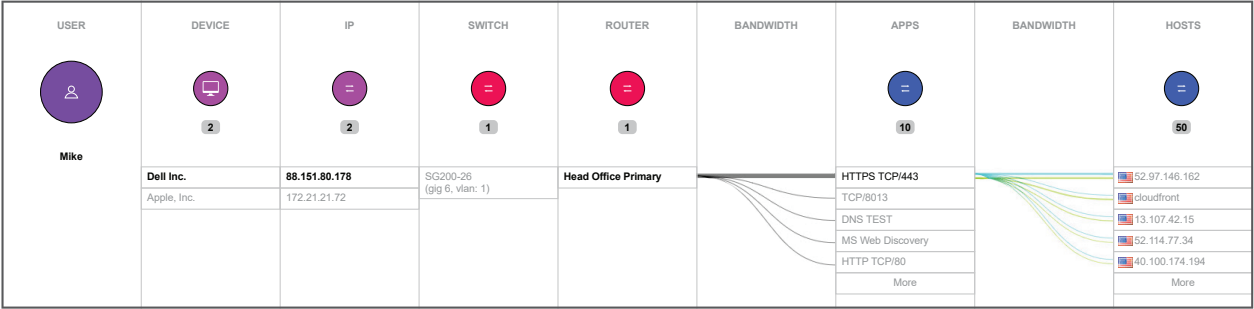
End-user experience score with associated connection dynamic conversation breakout

# 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



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

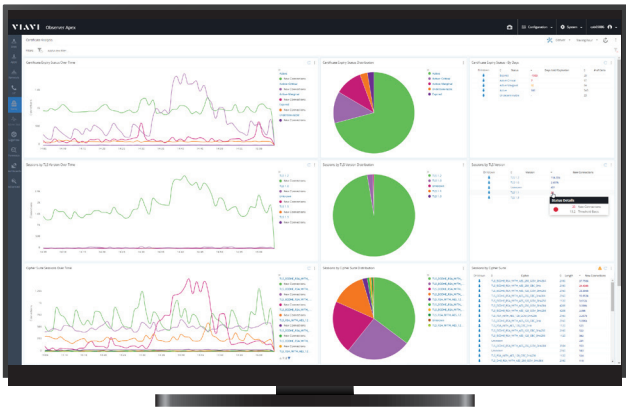
By compiling Layer 2 to Layer 3 insights into a single enriched flow record, Observer can produce unique, interactive visualizations that illustrate the relationships between User, IP address, MAC address, and application usage across the network. Users can simply enter a name/userid or IP address and 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.

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.



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

## 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  |
|--|--|---|---|
| <ul style="list-style-type: none"> <li>• Firewalls</li> <li>• DDoS Prevention</li> <li>• Data Loss Prevention</li> <li>• Intrusion Prevention</li> <li>• Anti-Virus &amp; Malware</li> </ul> | <ul style="list-style-type: none"> <li>• Encryption</li> <li>• Anti-Spam/Phishing</li> <li>• Access Controls</li> <li>• Endpoint Security</li> </ul> | <ul style="list-style-type: none"> <li>• Intrusion Detection</li> <li>• Security Event Mgmt (SIEM)</li> <li>• Endpoint Discovery</li> </ul> | <ul style="list-style-type: none"> <li>• Network Forensics</li> <li>• Security Event Mgmt (SIEM)</li> </ul> |



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?



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.



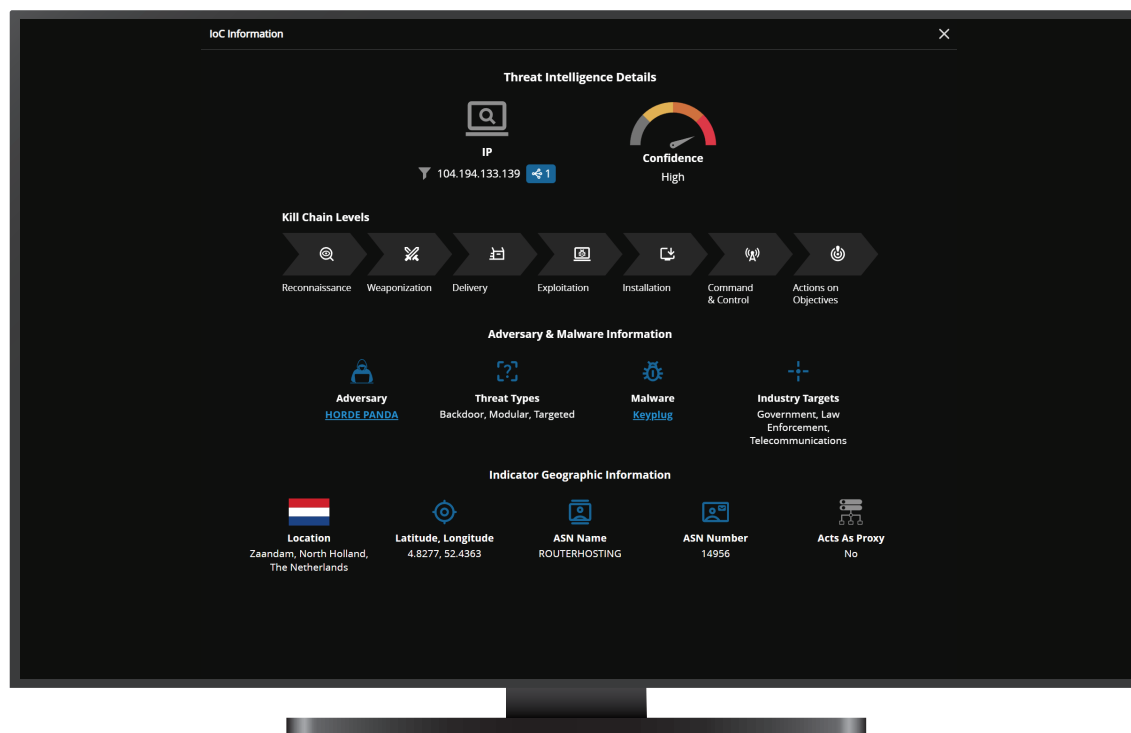
# OBSERVER THREAT FORENSICS

## Actionable Threat Visibility for Confident 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 empowers security teams to correlate adversary behavior with suspicious traffic patterns and performance degradations, all in real time.

By embedding Indicators of Compromise (IOCs), attacker TTPs, and other adversary details at the moment of detection, Observer enables immediate, high-confidence threat validation, without manual stitching or delayed enrichment.

Whether triggered by known threat or unexpected behavior in network traffic patterns, each alert includes pivot-ready access to raw packet data and enriched flow metadata providing analysts with the evidence needed to assess impact, investigate scope, determine root cause and take decisive action across hybrid environments.



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 data retained over time, analysts can reconstruct the complete attack timeline, even before initial detection, to uncover root cause, entry points, and lateral movement within one source of truth.

**Key benefits include:**

- **Real-time correlation** between network traffic and threat intelligence reducing mean-time-to-resolve (MTTR) or guesswork
- **Retrospective analysis** provides Day Zero visibility, providing security analysts with the forensic evidence needed to investigate threat activity prior to initial detection
- **Embedded attacker context** and TTPs support confident triage and investigation
- **Direct links to packet evidence** enable rapid drill-down for scope and impact assessment
- **Shared visibility** drives collaboration across NetOps and SecOps workflows

Observer Threat Forensics helps unify network and security operations with a shared, high-fidelity view that correlates performance and threat activity, enhancing investigations and improving confidence across workflows. Integrated enriched flow and metadata provide the granularity and retention needed for real-time triage and post-breach forensics, eliminating guesswork and accelerating resolution.





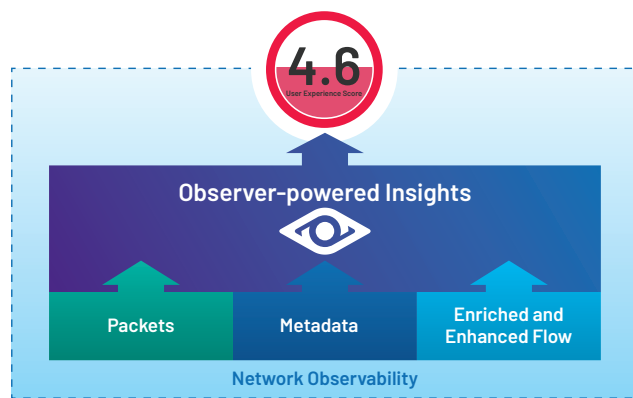
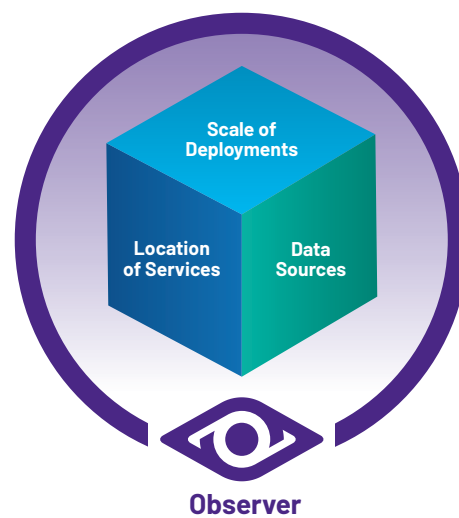
# OBSERVER OVERVIEW

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](https://viavisolutions.com/apex)



[viavisolutions.com](https://viavisolutions.com)

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

To reach the VIAVI office nearest you, visit [viavisolutions.com/contact](https://viavisolutions.com/contact)

© 2025 VIAVI Solutions Inc.

Product specifications and descriptions in this document are subject to change without notice.

Patented as described at [viavisolutions.com/patents](https://viavisolutions.com/patents)

apex-br-ec-ae  
30176200 914 1025