Plixer One™

Why Buy Plixer One

- Comprehensive end-to-end network observability and detection
- Proven ability to aggregate network telemetry and forensic data
- Eliminates blind spots by extracting data from every point in the network
- Leverages AI to speed threat detection, investigation and reporting
- Elevates IT, NetOps and SecOps with the best value to price ratio

Elevating network security and operations is crucial to remain competitive, efficient, and adaptable to business needs.
Gartner/IDC commentary

Modern enterprises entrust everything to the network, and with continuous digital transformation, cloud computing, and use of AI, CIOs and CISOs must focus efforts strategically, efficiently, and smarter to deliver, maintain, and secure the complex, sprawling IT infrastructure.

Plixer One takes IT, NetOps & SecOps to the next level by optimizing operations with unmatched observability across the network estate, continuous expert insight, and tools with enhanced defensive controls. It provides performance assurance with a means to more effectively minimize outages, defuse threats, and maximize investments, resulting in greater efficiency.

Experience Unmatched Network Observability and Defense

With Plixer One IT teams can see more, know more, and do more to maintain high-performing network availability, security, and connectivity at speed across the entire hybrid ecosystem.

As the industry's most advanced Network Observability and Defense Platform, Plixer One ensures multi-layered data ingestion and combines leading NetFlow/IPFIX analysis, with performance monitoring, threat detection and response capabilities, and advanced multifaceted AI to help IT organizations effectively maintain a secure, high-performing, and responsive hybrid network, even when facing increasing loads, shifting flows, digital transformation, and the most evasive targeted attacks.

See More, Know More, and Do More

- **Maintain comprehensive network visibility,** continuously monitoring without blind spots
- **Distill telemetry noise** from managed and unmanaged devices, systems & services
- **Gain multi-layered assurance** across owned and un-owned IT infrastructure
- **Drive security from the network** to counter emerging threats and attacks faster
- **Enhance data accuracy** for threat detection, network forensics, & root analysis
- **Reduces the IT operations strain** where expertise and headcount are lacking

Elevate IT with Plixer One

Comprehensive NetFlow/IPFIX Ingestion

Visibility across the entire ecosystem is the route to IT success. Enterprises require a wealth of data from a variety of locations to inform and ensure an understanding of the network and the overall state of the environment - health, performance, and security. The more network data collected, distilled, and analyzed, the stronger the telemetry becomes that signals problems, potential outages, and security threats. With Plixer One, IT can easily achieve end-to-end visibility, beginning with the richness of NetFlow Data.

Gain insight from the range of network components enabling your business

Switch	**Router**	**Concentrators**
Load Balancers	**Gateways**	**Firewall**
Servers	**Encrypted Traffic**	

With Netflow/IPFIX ingestion, Plixer One serves as the foundation for network reliability and security, collecting data from more network locations than any network analysis and visibility (NAV) tools. Using flow data, Plixer One automatically analyzes over 9,000 attributes from exporting devices, including switches, routers, concentrators, firewalls, load balancers, servers, and more, without requiring additional software agents or appliances. IT can easily activate export settings on specific network devices, then watch as Plixer One discovers devices and begins ingesting volumes of traffic data immediately. The vendor-agnostic approach enables you to easily visualize how traffic flows across the network, identify performance threats, and optimize security best using a single tool without complexity.

Unified Network Intelligence

Built to provide the clearest picture of today's dynamic, complex, hybrid environments, it consolidates various types of forensic telemetry across the enterprise from physical, virtual, or cloud resources, allowing teams to visualize traffic behavior, investigate anomalies, trace root causes, analyze and exchange security data, and confidently respond—faster and with increased accuracy and greater context. The unified approach acts as a single source of network truth.

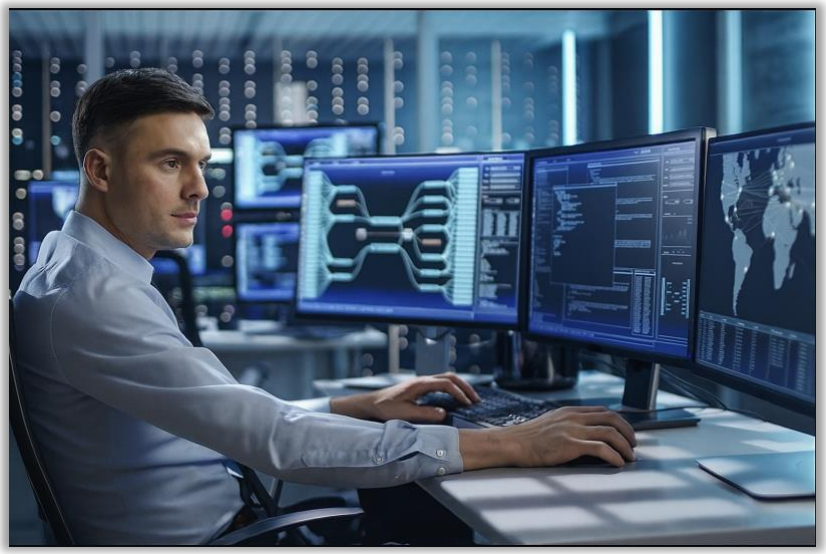
Table: Single source for Forensic Telemetry

Netflow/IPFIX	**STIX/TAXII**	**SNMP**
Consolidated source-enriched network traffic flow data existing in the network, for every connection, and is available at each critical point throughout the IT infrastructure	Amalgamate threat Intelligence Data with other security tools for streamlined detection accuracy and threat hunting	Gather insight on the health of network devices and interfaces, and see how flows traverse from IT device to IT device
UDP/Syslog	**PCap**	**Upstream**
Collect system and application status and event messages - timestamps, hostnames, severity levels, and the message content - from various sources for compliance, monitoring, debugging, and root cause analysis.	Real-time select packet captures to reconstruct network events, identify the source of attacks, and gather threat evidence without traditional PCAP storage requirements, especially where NetFlow data is unavailable	Insights from edge devices connecting outwardly beyond the perimeter, identifying path-vector information and interconnected networks that lead to traffic routes across the internet.

Multifaceted Data Analysis

Plixer One Enterprise transforms traditional network monitoring into intelligent, AI-native network observability, empowering NetOps and SecOps teams with a unified source of forensic telemetry. This delivers comprehensive, contextual insight into the changing network topology, services, connections, and activity.

Whether you are in IT operations overseeing network planning, maintaining aspects of infrastructure, or part of the SOC or cloud team, when you absolutely need to understand the network and are looking for in-depth traffic intelligence and insights into who, when, why, where, and how, Plixer One puts the information before you.



Advanced Analytics in Plixer One analyzes critical network data across every point in the data center, as well as distributed remote environments, connections across SD-WAN, and cloud-based traffic vital to the mission. It benchmarks performance levels and ensures a more accurate understanding of network traffic, components, and interactions as data flows through the network. With data analysis methods focused on understanding traffic patterns and host behavior with examination of multisource data NetOps and SecOps gain a clear picture of key issues faced and are alerted to performance issues and incidents with increased accuracy, security concerns and risks in real-time and gain increased clarity and precise discernment needed to distinguish benign anomalies from threats to performance of security, and confidently update links, configure settings and policies, and strengthen network controls and security proactively.

Artificial Intelligence (AI) extends advanced analytic capabilities with network-centric models, machine learning, and deep learning techniques designed to perform human-like expert analysis from the perspective of each device in the network. The approach provides unmatched depth in ascertaining network security events and IOC affecting performance, often regarded as benign. The integrated AI engine continually evaluates data and incidents to correlate events and uncover, prioritize, and triage salient and highly evasive attacks – deriving more profound insights from network data and facilitating proactive measures to prevent service disruptions.

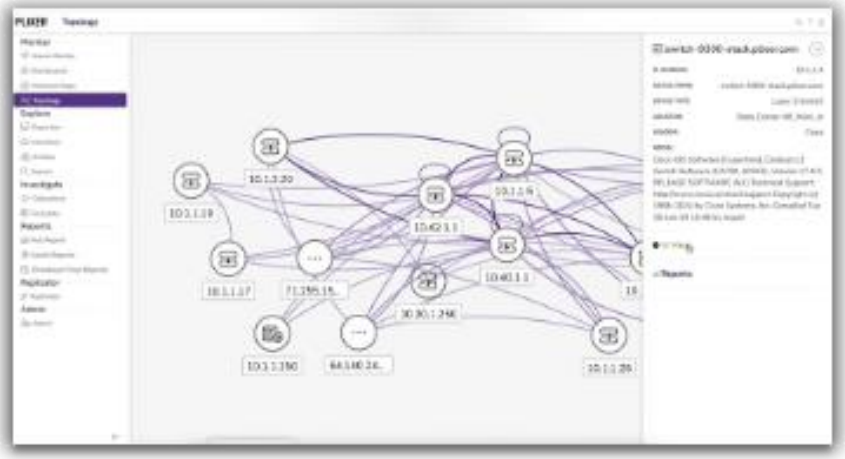
Machine Learning is at the heart of AI in Plixer One, combining the local fidelity of network traffic patterns with global insight from curated threat intelligence to learn continuously. With ML capabilities in Plixer One, AI algorithms learn from changing data to enhance analytics used for recognizing patterns and making the best predictions. The supervised and unsupervised learning approach, as well as deep learning, is essential to anomaly detection. Models retrain automatically, as stream analytics run in real time, feeding results to Plixer One and any connected downstream systems. The outcome is more accurate detection and forecasting with reduced false positives, and a single authoritative telemetry stream- without the operational overhead of managing separate ML, database, or messaging stacks. Learn about Plixer AI and Machine Learning.

Plixer AI Assistant

Within Plixer One, AI optimizes usability, with an expert AI assistant that ensures users can accomplish key tasks regardless of their level of expertise or familiarity with Plixer One. Using natural language prompts, Plixer AI Assistant engages to quickly help users navigate the UI, add or manage users, build dashboards or network maps, and understand the full state of the network and the issues at hand. It transforms report generation for both complex, custom, and standard reports – automatically building queries, identifying data sources, selecting relevant metrics, KPI, and visualizations that best demonstrate impact and effectiveness.

Using our large language models (LLMs) designed for network operations and security and trained on vast amounts of data, it easily understands and generates human language with each input. Although you can use your own proprietary LLMs, our native LLMs leverage decades of Plixer expertise with contextual embeddings that ensure it communicates the right information and operational tasks in the best way and with speed. Organizations have the flexibility to tune models or leverage their own proprietary LLMs for increased assurance of the effectiveness of the AI assistant in providing specific guidance, answers, and information with little to no human effort. It enables everyone to become the expert they aim to be.

Cohesive Network Monitoring and Reporting



With the most comprehensive real-time and historical network data ingestion, Plixer One simplifies efforts to visualize the entire structure of your network. It ensures the ability to monitor the changing infrastructure across the interconnected data center topology, including branch offices, campuses, facilities, and workloads running in cloud environments – all with one tool monitoring all network devices in your environment and at each juncture along the way.

Easily visualize the entire network estate

With device discovery and *Endpoint Analytics*, it fingerprints managed and unmanaged network devices to profile and track each using its unique MAC address as the primary identifier. Other attributes collected include authentication status, DHCP factors, risk level, interfaces, and more. From this, IT teams can easily depict the full graphical network topology in various ways that help them best observe the big picture, narrow down possible devices to monitor and investigate, and zoom in to get the information they need, leveraging hundreds of customizable **dashboards and reports**. Additionally, *Endpoint Analytics* layers device intelligence on top of the network discovery data for real-time insights into device identity, location, behavior, and risk

Observe traffic across every hop

Plixer One ensures IT maintains a thorough understanding of the entirety of traffic flows from point to point across each transaction. It automatically captures details that reveal each hop as data flows to a specific destination, tracing interactions, visualizing activity with all network devices and interfaces along the way. Topology views easily bring this information to light, depicting each device discovered on the network and illustrating relationships between routers, switches, servers, and more, so you spend less time troubleshooting root causes and gathering evidence needed for critical decision-making and resolution.

Get insight into traffic traversing the cloud

Plixer One ingests cloud flow logs in real-time, providing end-to-end awareness and visualization across multi-cloud environments, including **AWS, OCI, GCP, and Azure,** without the need to deploy probes or reconfigure cloud networks. It simplifies efforts to visualize and monitor intra-cloud traffic, traffic entering or leaving cloud environments, app performance and utilization, and interpret and detect concerning traffic patterns, anomalies, and trends from the datacenter switch to the cloud and back again.

Understand flows between containers

For containerized workloads and applications, Plixer One ensures network admins maintain container visibility within and between different pods, especially service endpoints that route traffic to multi-container pods. Even when a pod disappears, communication footprints and impact on the network remain visible.

Illuminate Zero Trust Tunnel

As organizations transition from VPN to modern SASE/SSE solutions, encrypted tunnels can create dangerous blind spots for network monitoring. Plixer One eliminates these gaps by ingesting Zscaler Zero Trust Exchange™ logs and merging them with NetFlow and SNMP telemetry. The result is real-time visibility into user and application flows across internet access points, data centers, and cloud environments. With this unified view, administrators gain the insight into each encrypted user traffic flow needed to validate policies, detect anomalies, and ensure secure, high-performance connectivity—without pivoting between tools.

Unveil network blind spots

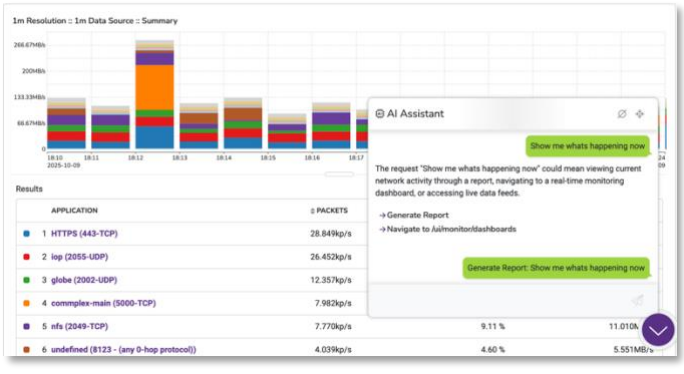
Plixer One brings the entire network infrastructure into view, identifying all aspects of the network within minutes, including devices, their configurations, connections, health, and traffic that bypasses traditional security measures. It regularly identifies new devices or changes to the network, revealing bandwidth consumers and unauthorized access points to help you maintain accurate and up-to-date network documentation and reporting. Each endpoint discovered is profiled and fingerprinted with the MAC address used as the primary identifier. Data points captured for profiling include authentication status, DHCP factors, risk level, and other stats.

With the abundance of data collected and analyzed, Plixer One monitors north/south traffic that crosses the enterprise perimeter with granularity, as well as east/west communications, to provide complete traffic visibility and detection of performance issues and attackers as they move laterally within the network.

The platform enables you to monitor individual hosts and network devices, or entire subnets, from multiple levels within the network. Using intelligent de-duplication, users see alarm data that's accurate and streamlined to only what they need to see, without any blind spots.

Report Generation

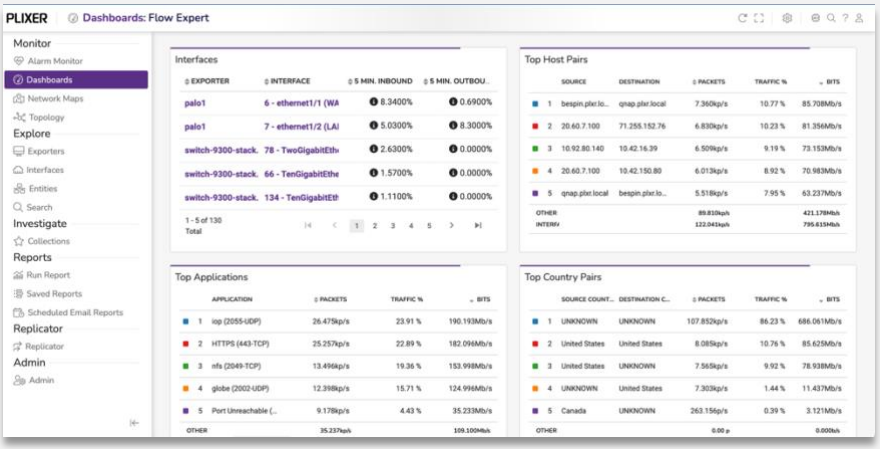
Plixer One ensures that your teams across IT, NetOps, and SecOps have comprehensive, actionable reports that provide deep insights into network health, performance, and security with just a few simple clicks or by prompting the Plixer AI Assistant.



With Plixer One every report provides specialized observability that helps specialists understand and monitor network utilization, pinpoint performance bottlenecks, forecast future needs, and proactively identify and resolve security threats and operational issues. Plixer One offers hundreds of out-of-the-box reports, as well as the ability to create custom reports tailored to specific needs based on the data source, telemetry types, key metrics, correlated insights, and more.

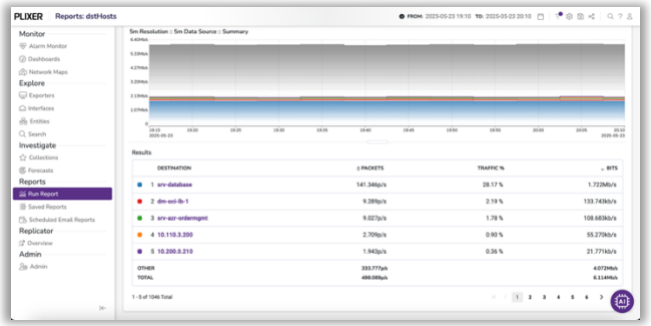
Access Insightful dashboards and hundreds of reports that consolidate data to help users make quicker, more informed decisions around...

- Network Utilization
- Application Performance
- Security threat detection
- Capacity Planning
- Root Cause Analysis
- User connectivity

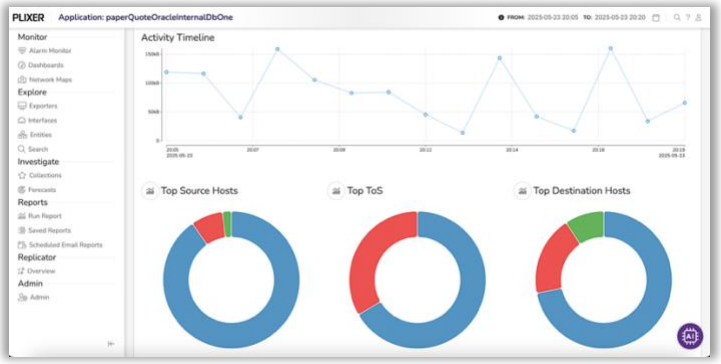


Efficient Data Replication

With Plixer One, IT can implement and maintain a single point for centralized data replication that the entire organization can use. It provides the most efficient method for copying data to multiple locations, without the complexity, performance overhead, and resource costs associated with data replication using other tools, or within applications, storage systems, and hypervisors.



Replication is an integration with Plixer Replicator easily activated from Plixer One UI, without requiring additional hardware or tedious configuration. It distributes data to multiple locations simultaneously with performance controls, high availability, tracing, and monitoring to ensure consistent and reliable replication.



Click here to learn more about Plixer Replicator.

Strengthen Network Defenses

With the most comprehensive network data ingestion, multifaceted AI-driven analytics, Plixer FlowPro capabilities, and a Suricata engine, Plixer One unveils security gaps and accelerates threat detection and response, surfacing malicious activities with precision and insights often lacking in other tools –optimizing SOC productivity and eliminating risk to business.

How Plixer One Elevates Security Defenses

Aggregated NetFlow Retention for access to valuable IPFIX contextual information over extended periods of time

Accelerated Threat Investigation unifies siloed data sources and ensures end-to-end threat context for rapid expert-level triage & response

Optimized DDoS Defense distinguishes legitimate traffic surges from malicious floods targeting devices & apps

Powerful ML/AI Anomaly Detection turns flow data into behavioral models and identifies hidden patterns in IPFIX data, revealing anomalies and zero-day threats

Intrusion Detection[1] uses select packet capture, powerful IDS rules and a signature data base to alerts of evasive protocol usage

Cohesive DNS security that detects and mitigates threats like DNS spoofing, pharming, and poisoning, while

Endpoint Analytics[1] layers endpoint intelligence for real-time insights into device identity, location, behavior, and risk

Noise Reduction with AI-driven precision detection & prioritization that addresses minor alarms, to focus teams on what truly matters

Click to expand and read the full details

Maximize your Plixer One Investment

Active Directory	Enrich NetFlow data with end-user telemetry from **Kerberos**, **RADIUS** and **TACACS+** for insight into who is accessing the network.
endace	Correlate flow data with full packet capture to increase granularity in network traffic analysis by leveraging integrations with packet recording technologies like **Endace**
zscaler™	Activate **Zscaler ZTE™** log ingestion to illuminate traffic across encrypted access tunnels connecting users via the internet to workloads in the cloud and the datacenter.
Hundreds of integration	Analyzes data from a variety of tools to uncover gaps in threat detection and response, access and security controls, risk management and compliance.

Learn More.

Click the links below

- Why Buy Plixer One
- Why Zscaler customers are embracing Plixer One
- Read how Plixer One is making SAP run better

About Plixer: Plixer is committed to helping organizations continually elevate IT and the power of the network by collecting and analyzing the vast amount of flow data held in their IT infrastructure to respond and optimize overall operations. Plixer One is the foremost NetFlow traffic collector and analyzer deployed in more than 500 data centers allowing IT to harness the data and experience unmatched network observability. Learn more at plixer.com or follow us on LinkedIn and Twitter.

- ZIA
- Zscaler Private Access