Plixer FlowPro

PLIXER

Enhanced Network Visibility and Security

Why use Plixer FlowPro in your visibility stack?

Increase granularity of visibility with **comprehensive forensic data across each OSI layer**

Ensure secure and high performing services and **reduce MTTR for active threats by 67%**

Get more granularity in visibility across the hybrid infrastructure and increase confidence in security

Plixer FlowPro is an advanced packet data collector integrated within the Plixer One Platform. It provides deep packet data analysis, offering unparalleled visibility into the network, application performance, and real-time detection of unknown and emerging environmental threats.

With FlowPro, IT, network and security teams can better identify hidden threats, resolve application issues, and ensure optimal network performance.

EXPAND VISIBILITY • MONITOR APPLICATION PERFROMANCE • DEFEND THE NETWORK

Elevate the network:

- Ensures visibility where NetFlow is not exported
- Enables Layer 7 Application Performance Monitoring
- Facilitates faster MTTR
- Isolate faults to systems, network paths, subnets, & users
- Visualize traffic and apps across your entire network

Enhance Security

- Detect abnormal behavior and security threats
- Monitor DNS traffic to catch malware and botnets
- Identify malicious C2 communications
- Visualize encrypted web traffic destinations

EXCLUSIVE PACKET CAPTURE

The unique packet capture technology within FlowPro uses a form of selective packet capture to minimize PCAP storage requirements while ensuring comprehensive forensic data collection, specifically focusing on application performance and traffic related to security events. FlowPro ensures greater clarity and deeper insights compared to other tools, ultimately optimizing IT operations, reducing risk, and accelerating incident response times.

APPLICATION PERFROMANCE MONITORING (APM)

FlowPro offers in-depth forensic analysis of your network, enabling you to identify the causes of slow connection times and unexpected spikes in bandwidth usage. By enhancing the capabilities of Plixer One, FlowPro illuminates issues such as packet loss, retransmissions, and round-trip time—factors that can significantly impact the application experience.

Capabilities for application performance monitoring enable network administrators to identify the root causes of performance issues. By using flow-based analysis combined with deep packet inspection the tool examines critical application traffic, whether its internal or cloud-bound. It offers detailed visibility into each connection revealing application latency, throughput, and server performance, ensuring the end-user experience and business operations remain optimized.

ENHNACED NETWORK SECURITY

FlowPro enables Plixer One user to enhance security measures by leveraging Suricata rules to alert on any unusual protocol usage, unexpected flow patterns, file transactions or extractions, anomalies, and application activities. With Suricata, FlowPro compares traffic patterns against a database of known threat signatures, which can easily be customized to focus on specific threats relevant to your network. This customization allows you to define the types of network traffic to monitor, specify the appropriate responses, and gain a comprehensive understanding of the network's status.

Additionally, FlowPro monitors DNS traffic and observes details about traffic entering and leaving your network over DNS, allowing you to see malicious attempts to bypass your firewall to establish C2 (command and control) connections and communicate directly with assets within your network. Plixer FlowPro quickly identifies and alerts on compromised assets, leveraging various forms of DNS abuse for data exfiltration or C2.

©Plixer LLC.2025, ALL Rights Reserved

Plixer FlowPro USE CASES



Deep Packet Inspections of critical network segments that requires more detailed insight into traffic. Retrieve and analyze event-triggered packet captures in tools like Wireshark for precise troubleshooting and investigations.



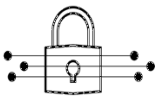
Risk of DNS compromise and other issues related to domain name resolutions including performance degradation, configuration errors, and security threats like DNS hijacking or cache poisoning. Identify any disruptions in DNS resolution across different locations



VoIP and phone QoS Monitoring by tracking key indicators such as ToS, packet loss, jitter, and codec usage. By exporting this information in a user-friendly format, Plixer FlowPro simplifies troubleshooting, leading to a reduced Mean Time to Resolution



Rule-based Intrusion Detection and prevention for added network defense against malware, data exfiltration and emerging threats. It ensures anomaly-based monitoring and reputation-based alerts. Tracks and analyzes events like BotNet activity, Command and Control (C2) communications, and encryption anomalies.



Encrypted Traffic Analysis that identifies threats and anomalies within encrypted communication using advanced techniques like deep packet inspection, app & behavioral analytics, and analyzing IP addresses, Ports, DNS traffic connections to detect attacks without decryption

Key capabilities that expand use of Plixer One

- Select Packet Capture for Targeted analysis
- Application Performance Monitoring
- Fingerprinting
- FQDN Reporting
- Rules-based IDS Threat Detection
- Detailed File Hash Analysis
- Real-time Alerts and Actionable Information
- Intuitive Insightful Visualization
- Pre-defined and Custom Report Generator
- Enhanced DNS Activity and Performance

Plixer FlowPro Deployment Options



40GB Hardware Appliance



Software deployable in a Hypervisor

Click here for “hardware appliance specifications” and configuration details. Speak with your account representative for information on custom requirements including increased storage options

©2025 Plixer LLC., ALL Rights Reserved

PLIXER