PLIXER

Plixer Scrutinizer

Flow-first Visibility for Network Performance & Security

What Plixer Scrutinizer Delivers

Plixer Scrutinizer is a flow-first network observability solution that collects and analyzes NetFlow and IPFIX telemetry across on premise, hybrid, and cloud environments.

It turns raw traffic data into clear, searchable conversations and visual investigation timelines. When something breaks or looks suspicious, you can see exactly what happened.

Instead of jumping between tools, teams open one interface and see:

- Who talked to who
- Over which protocol and port
- Through which device and interface
- At what time, for how long, and how much data moved

For Network Operations Teams

When users say, "The network is slow," Scrutinizer lets you see if it is and where. Open a path view and trace the conversation hop by hop across routers, firewalls, switches, and cloud gateways. Identify the interface adding latency, confirm utilization trends over time, and compare current behavior against historical baselines. Teams follow the flow timeline, isolate the segment causing delay, and resolve the issue using shared, visible evidence.

For Security Operations Teams

Scrutinizer helps security teams detect abnormal behavior early and investigate with confidence. It surfaces unusual authentication spikes, rare outbound connections, DNS anomalies, tunneling patterns, and signs of lateral movement between internal hosts. From a single alert, analysts pivot into a timeline that shows who communicated with whom, over which ports and protocols, and how much data moved. Each finding ties directly to flow evidence, creating a clear investigation path and an exportable Incident Brief that documents scope, peers, and impact. Analysts can prove what happened and move faster to containment.

Plixer AI Assistant

Plixer AI Assistant is built directly into Scrutinizer. It turns plain language into reports, filters, and guided investigations so teams resolve issues faster with fewer clicks.

Users can type questions such as:

- "Is there any Telnet traffic on my network?"
- "Show devices with high latency this week"
- "Top external destinations for this host."

It guides tasks, edits reports, and speeds root cause analysis so teams can investigate without relying on senior engineers. This shortens investigations and reduces escalation.

Every result is traceable to real network conversations, keeping findings explainable and ready for audit or incident review.

> Investigation timeline in Plixer Scrutinizer shows conversation paths, affected entities, and flow evidence that leads to verified root cause

Platform Highlights

CAPABILITY	DESCRIPTION
End to End Traffic Visibility	Trace traffic across on-prem and cloud to pinpoint where performance breaks down or where an attack moves next.
Fast Root Cause Analysis	Trace latency, saturation, and path changes to the exact interface or hop so you can fix the right problem the first time.
Behavioral Analytics	Model normal network behavior and surface meaningful changes that indicate risk or instability.
Threat Detection	Identify lateral movement, brute force attempts, tunneling, and data exfiltration using flow evidence, so threats are caught before they spread.
Long Term Flow Retention	Search months of historical flow data to investigate intermittent issues and recurring threats long after they occur.
Integration Ready	API and webhook support for SIEM, SOAR, ServiceNow®, Tenable®, and Microsoft Defender® extends visibility, automation, and reporting. Detections turn into action without manual handoff.

Get Started with a 30-Minute Demo

From alert to proof in minutes, with visibility your teams can trust.

Book a personalized session to learn how unified analytics improve investigation in your environment.

plixer.com

sales@plixer.com