

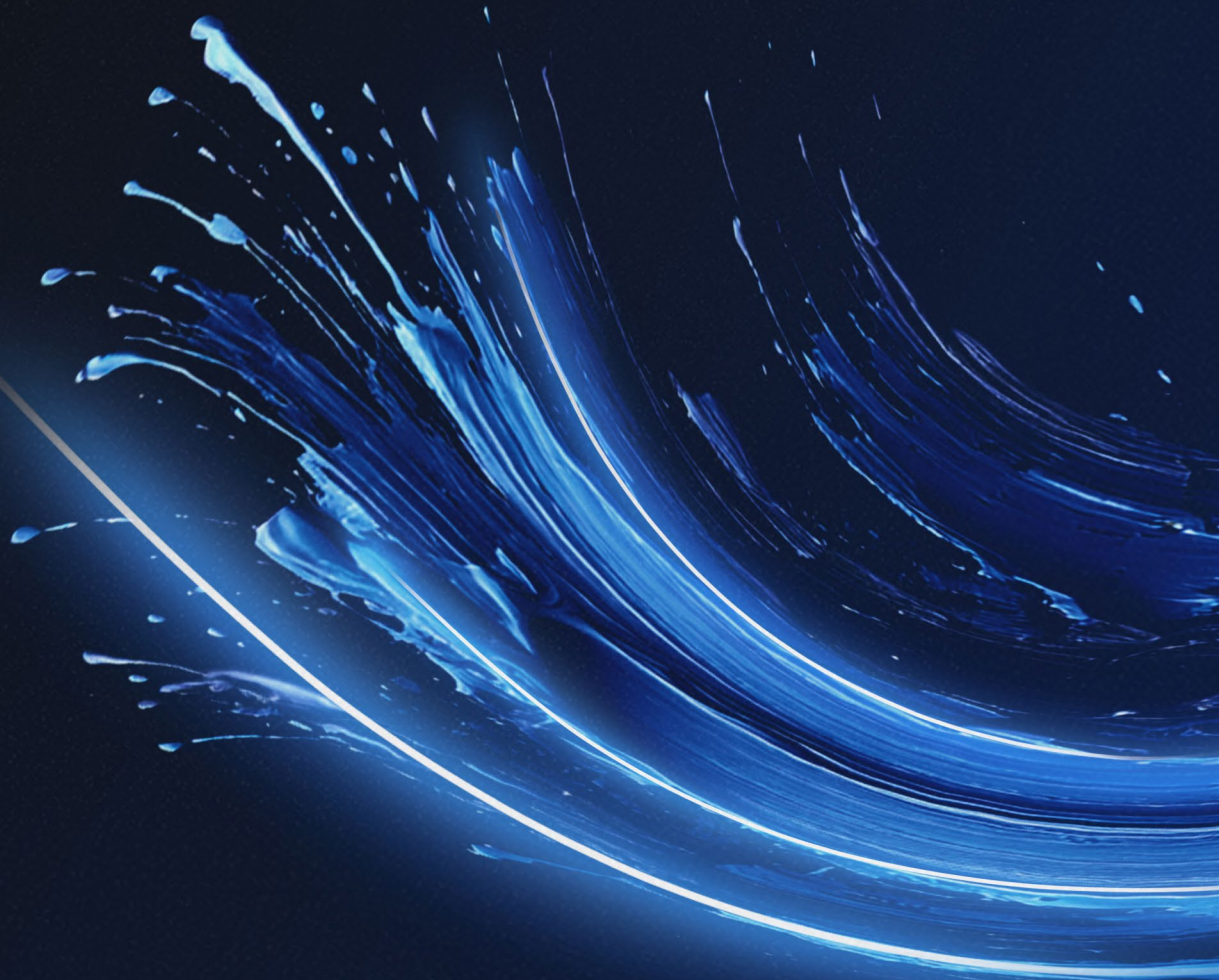
PLIXER

PROFITAP
DEEP NETWORK OBSERVABILITY

JOINT SOLUTION BRIEF

PLIXER AND PROFITAP

*Comprehensive ecosystem visibility with
packet and flow data*



Executive Summary

In today's complex and high-speed network environments, gaining comprehensive visibility is crucial for effective security and performance management. This joint solution brief outlines how the integration of Profitap's network TAPs and Network Packet Brokers (NPBs) with Plixer's FlowPro and Plixer One provides a powerful, end-to-end platform for generating rich network flow data and sending it to a Security Information and Event Management (SIEM) system. This combined solution empowers security and network teams to eliminate blind spots, improve threat detection, and accelerate incident response.

The Challenge: The Need for Actionable Data

Traditional network monitoring methods, such as SPAN ports, often suffer from packet loss, which creates significant blind spots and renders security and performance analysis unreliable. Furthermore, the sheer volume of raw packet data is overwhelming, making it difficult for security teams to quickly identify and investigate threats. To effectively utilize a SIEM, which relies on logs and network flows for correlation and analysis, organizations need a way to efficiently and reliably collect, filter, and transform network traffic into actionable intelligence.

The Solution: A Unified Network Visibility Platform

The joint solution addresses this challenge by combining the best of passive data access and intelligent data transformation. Here's how it works:

◎ Reliable Data Access with Profitap TAPs

Profitap's Network TAPs provide a fail-safe, non-intrusive way to create a copy of all network traffic, ensuring 100% data fidelity without affecting the production network. This eliminates the risk of packet loss, which is common with SPAN ports, and provides a complete, real-time data source.

◎ Intelligent Data Optimization with Profitap NPBs

TAPs is fed into a Profitap NPB. The NPB acts as a "traffic director," intelligently filtering, aggregating, and load-balancing the data. Key NPB features in this solution include:

- **Filtering:** Filters are applied to select only the most relevant traffic, such as specific subnets, VLANs, or applications, reducing the data volume sent downstream.
- **Deduplication:** The NPB removes redundant packets, further optimizing the data stream.
- **Aggregation:** Traffic from multiple TAPs can be aggregated onto a single port to feed a single Plixer FlowPro appliance.
- **Load Balancing:** Traffic can be distributed across multiple FlowPro appliances for scalable deployment.

◎ Flow Generation with Plixer FlowPro

The optimized packet stream from the Profitap NPB is sent to a Plixer FlowPro appliance. FlowPro is a network probe that performs Deep Packet Inspection (DPI) to analyze the packet data and generate rich, enhanced IPFIX (Internet Protocol Flow Information Export) flow records. Unlike basic flow exports from network devices, such as routers and switches, FlowPro's flow records include valuable Layer 7 (application-level) data, such as application names, DNS queries, and security-related metadata. This level of detail is critical for modern threat detection.

⦿ **Flow Analysis and SIEM Integration with Plixer One**

The enhanced flow records from Plixer FlowPro are then forwarded to Plixer One. Plixer One collects, analyzes, and visualizes the flow data, providing a complete picture of network activity. It can correlate flows with other data sources and has built-in features for deep network and security monitoring. Most importantly, Plixer One can export this rich flow data to a SIEM like Splunk or Elasticsearch, providing the SIEM with a high-fidelity data source for its correlation engine.

Key Benefits

⦿ **Complete Network Visibility**

Eliminate blind spots and packet loss by using passive TAPs, ensuring the SIEM receives a complete and accurate view of network conversations

⦿ **Actionable Security Intelligence**

Transform raw packet data into rich, contextual IPFIX flows that provide a deeper understanding of network threats and anomalies.

⦿ **Improved SIEM Performance**

By filtering and optimizing traffic at the NPB level, you reduce the data volume that needs to be processed, improving the performance and efficiency of the SIEM and other security tools.

⦿ **Accelerated Incident Response**

The high-fidelity flow data allows security teams to quickly perform root-cause analysis and respond to incidents with greater speed and accuracy.

⦿ **Scalability and Flexibility**

The modular nature of the solution allows for easy scaling to accommodate growing network speeds and complexity, from small offices to large data centers.

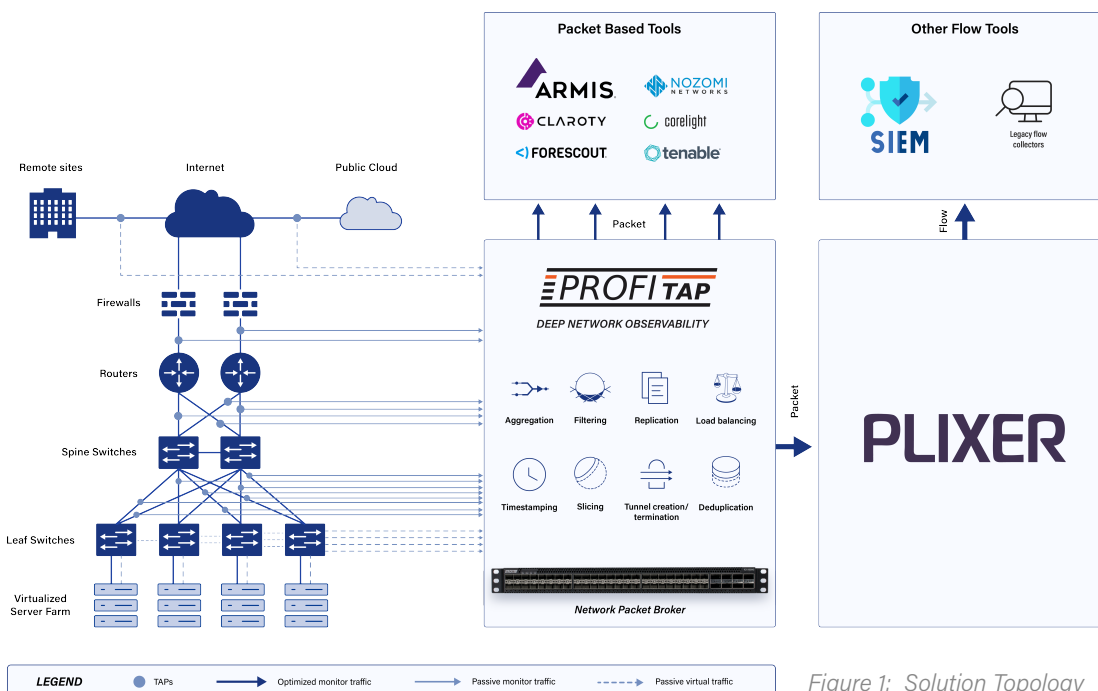


Figure 1: Solution Topology

PLIXER

Plixer empowers network and cyber security professionals by ensuring deep observability into the state of the network. This includes understanding network traffic— where it's going, why it's traveling there, and identifying potential risks and areas of great concern— as well as offering controls to optimize a global ecosystem.



DEEP NETWORK OBSERVABILITY

Profitap delivers packet-based network intelligence to enhance monitoring and bolster cybersecurity. Its unified observability platform offers reliable data access, traffic optimization, and robust capture/analysis. These solutions minimize troubleshooting MTTR, eliminate downtime, support lawful interception, simplify network complexity, and strengthen security for all networks. Serving over 1,100 clients in 70+ countries, Profitap provides comprehensive visibility and analytics across physical and virtual infrastructures globally.

To learn more about our joint solution go to <https://www.profitap.com/contact-us/>


FIND OUT MORE ON WWW.PROFITAP.COM

Profitap HQ B.V.
High Tech Campus 84
5656 AG Eindhoven
The Netherlands

sales@profitap.com
www.profitap.com

 Profitap

 @Profitap

 Profitap-international