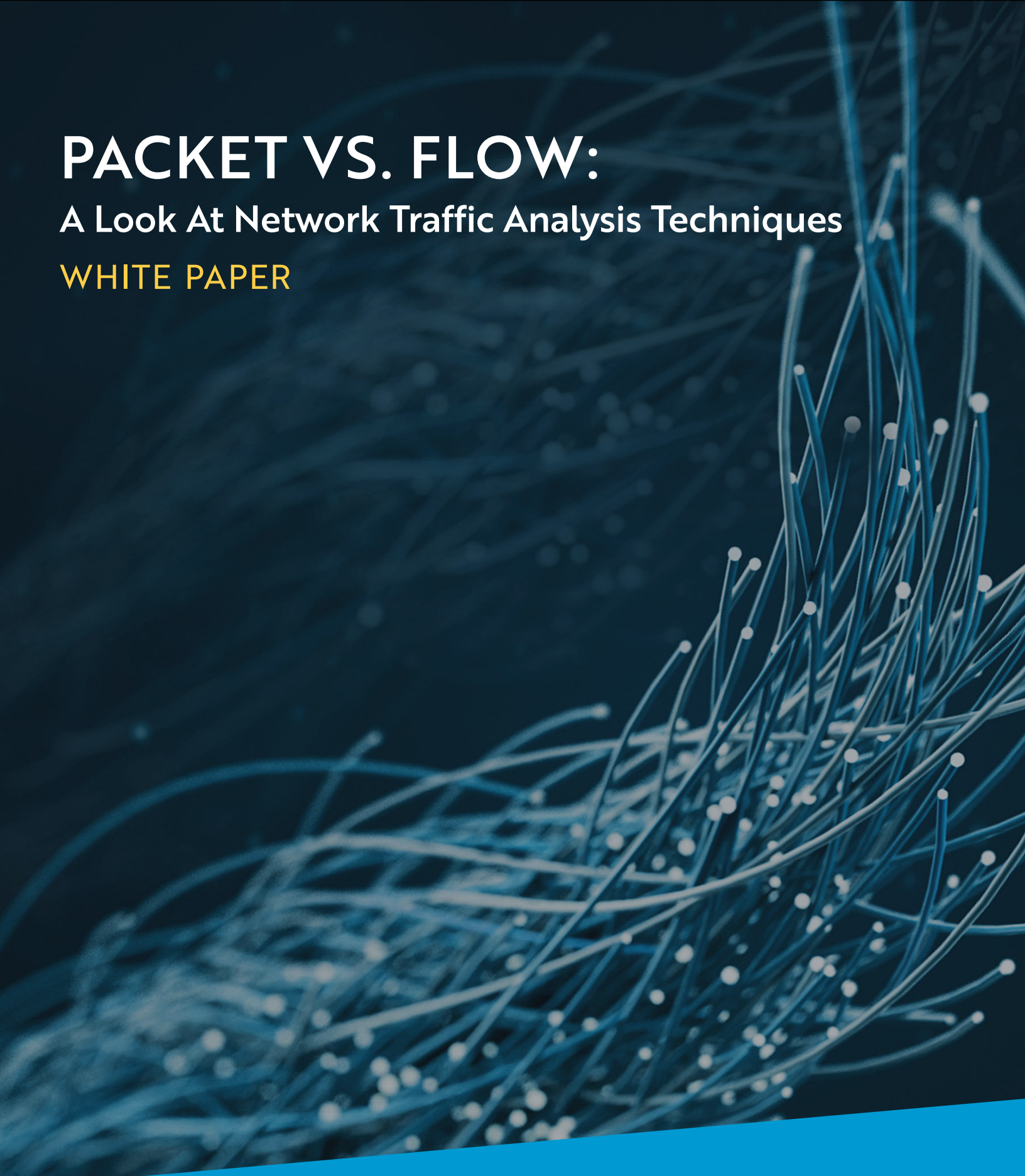


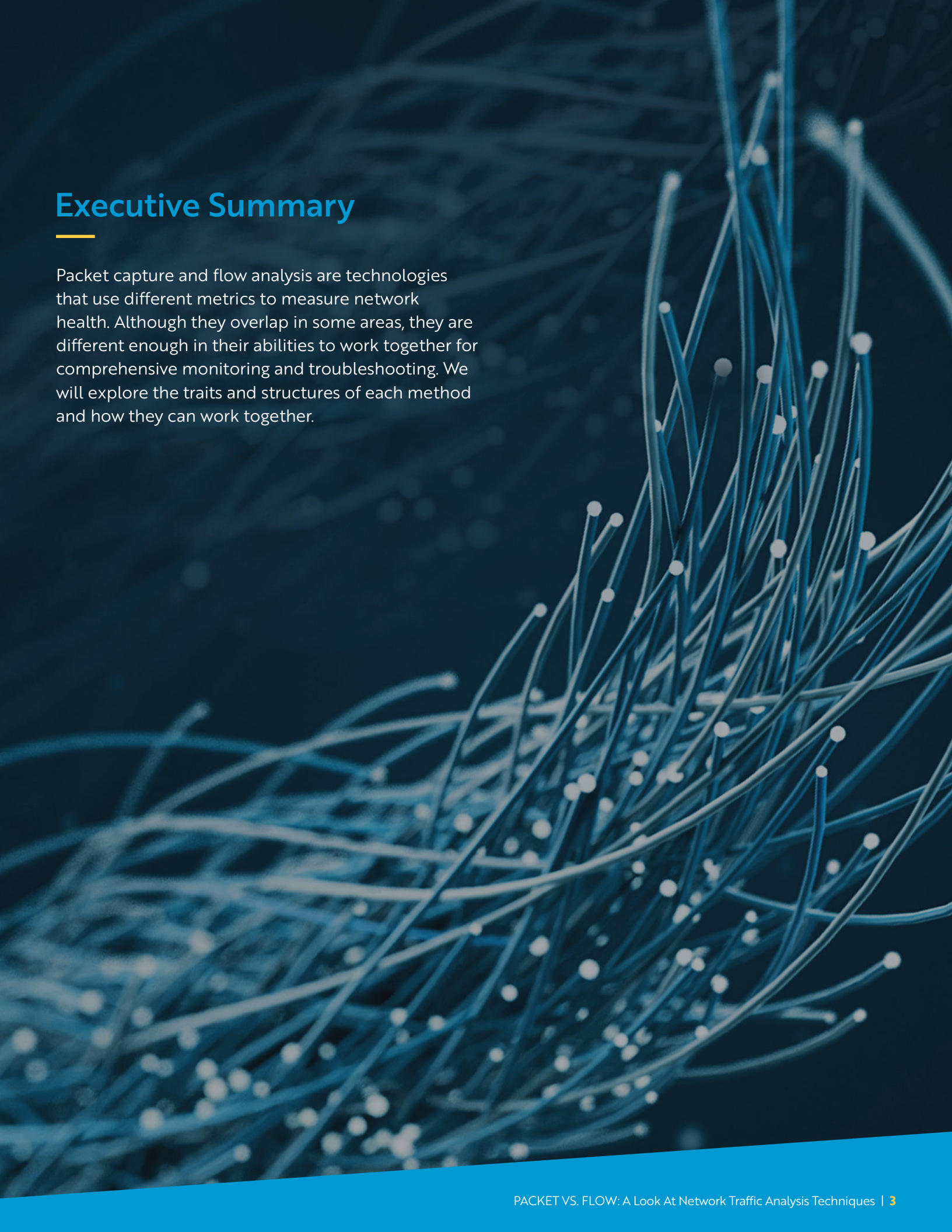
PACKET VS. FLOW:

A Look At Network Traffic Analysis Techniques

WHITE PAPER

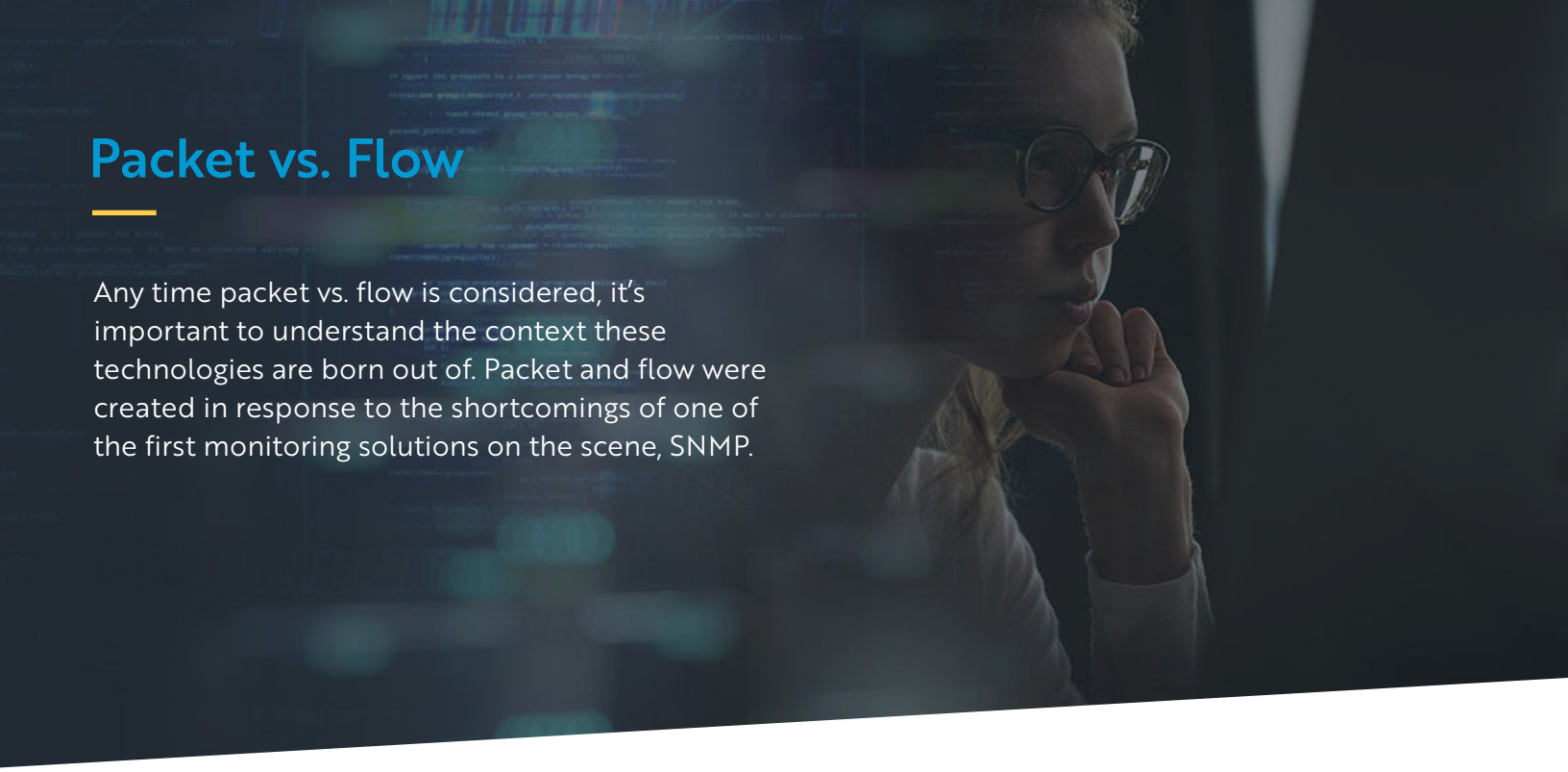
LiveAction®

Table of Contents



Executive Summary

Packet capture and flow analysis are technologies that use different metrics to measure network health. Although they overlap in some areas, they are different enough in their abilities to work together for comprehensive monitoring and troubleshooting. We will explore the traits and structures of each method and how they can work together.



Packet vs. Flow

Any time packet vs. flow is considered, it's important to understand the context these technologies are born out of. Packet and flow were created in response to the shortcomings of one of the first monitoring solutions on the scene, SNMP.

SNMP or simple network management protocol came about in the 80s as an application-level network protocol. SNMP lets you see what applications are running on your network and if the network is congested or down. While helpful with capacity planning and monitoring, SNMP is limited in detail because it is an analysis of the devices on the network, rather than the traffic itself.

Packet capture and flow analysis go beyond **if** a network device is congested, and answer the question of **why**. These methods work together with SNMP for a complete network traffic analysis solution.

Before we explain the pros and cons of each method, let's define the terms.

Packet

- defined as a segment of data traveling from the sender's origin to its destination. Individual packets travel from a source address to a destination address and may make hops along the way. Multiple packet segments can combine to create larger messages at the receiving address.

Flow

- defined as a sequence of packets that share seven attributes. Once any of the attributes change, a new flow begins.

These seven attributes are:

1. Incoming traffic interface
2. Source IP address
3. Destination IP address
4. IP protocol
5. Source port
6. Destination port
7. IP type of service

Flow Analysis

What is Flow Analysis?

Flow analysis was designed by Cisco in 1996 under the product name NetFlow. NetFlow and the term flow analysis are often used interchangeably, but there are other types of flow analysis like sFlow and IPFIX.

Flow analysis gives a high-level look at network statistics. It detects anomalies in traffic behavior that could indicate security incidents and enables look-back forensics to identify patterns in the network data. Flow analysis does not take you down to the packet level, but it does allow you to drill down to an individual IP address.

Ideal Use Case: A network with several WAN links and a need for high-level visibility.

How Flow Analysis Works

Flow analysis enabled devices like routers and switches generate flow data from their IP traffic.

The flow data can be accessed from the command line interface CLI, or it can be exported to a reporting server called a flow collector. The flow collector processes and condenses the information to make it easier to analyze. A flow analysis application (like **LiveNX**) analyzes the data and creates reports and summaries from the flow updates.

Consider the diagram below showing the process of flow analysis through a flow collector and analysis application.

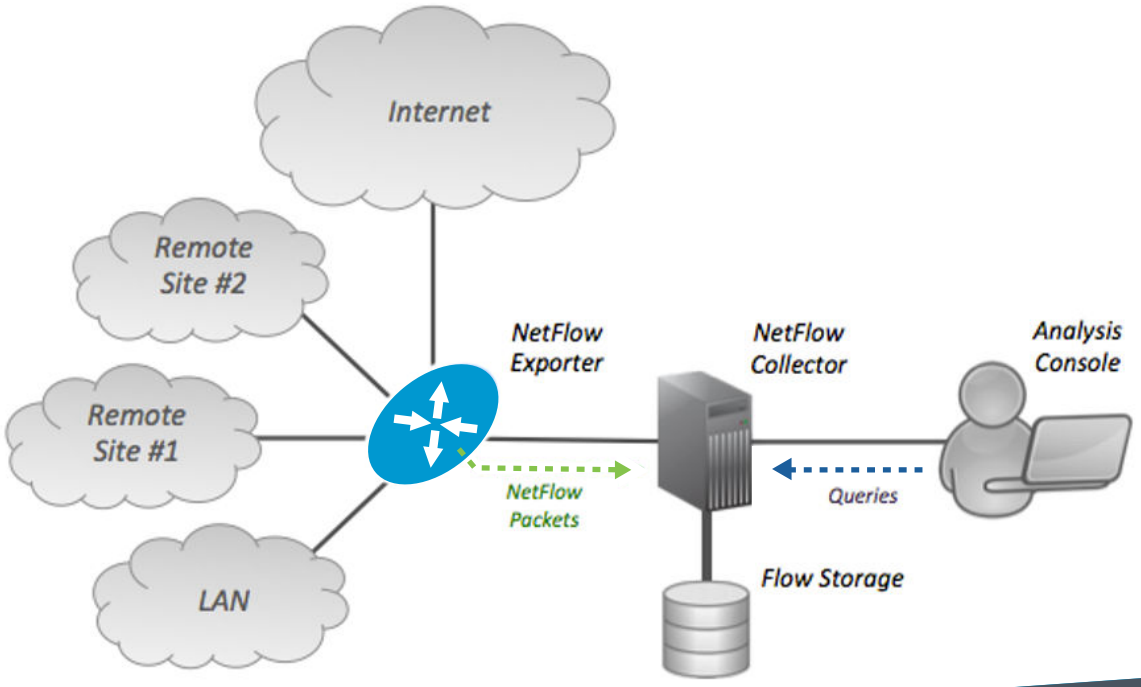


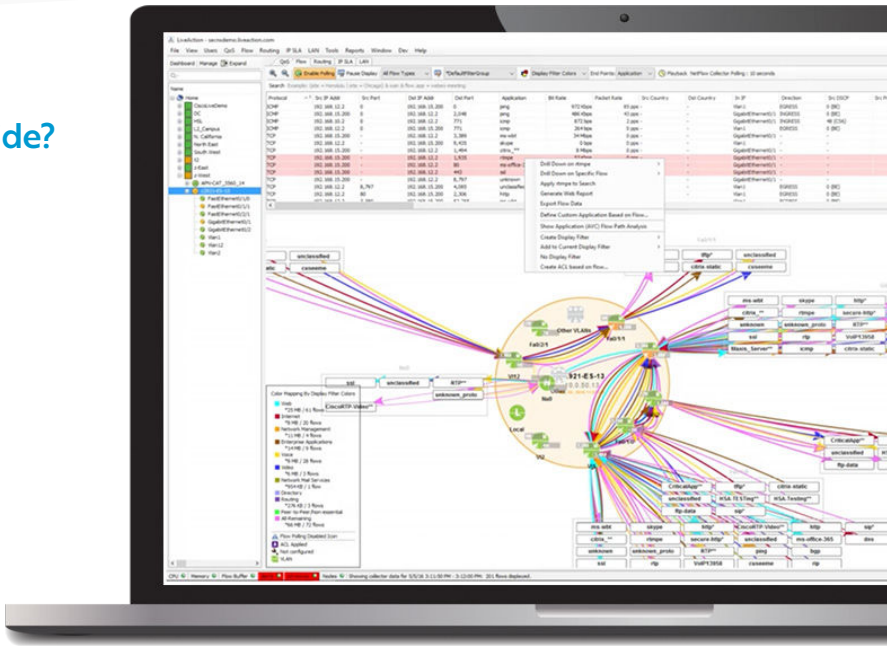
Image source: **Cisco**

Flow Analysis

What Information Can Flow Analysis Provide?

Flow analysis provides information like:

- Source interface
- Source IP address & Destination IP address
- OSI **Layer 4** Transport Layer protocols ex: TCP, RDP, SPX, IL, UDP, etc.
- If the Layer 4 is TCP or UDP the flow application will also look at the source and destination port number
- Class of service



Unlike packet capture, flow analysis is not an exact copy, but a statistical summary. Because it is summarized, it takes up less storage space and allows for more historical data to be archived over time.

Flow analysis can be displayed through colorful graphical interfaces like this example from our Live NX platform.

Challenges with Flow Analysis

Flow is IP-based and cannot drill into the granular packet-level details needed to find the root cause of network events.

Packet Capture

Packet capture, also known as packet analysis, or PCAP sniffing, is a process that captures and stores live packet data from Layers 2-7, traveling across your network.

Packet capture uses deep packet inspection (DPI) to extract metadata on the names of websites, files, hosts, applications, users, and more so you can identify what resources are being used where. Packet data is recorded as files, where each packet includes a header with extra information like the timestamp and the length. Packet capture is used to identify the root cause of performance problems.

Packet capture can be done through two different techniques, network taps, and port mirroring. In general, network taps are more reliable and comprehensive if you can afford them, but port mirroring is adequate for lower traffic requirements.

NETWORK TAP

a device that is put between the switch and the destination server

Pros: no packets can be dropped, complete full-duplex network visibility, complete capture

Cons: expensive and requires hardware installation, cannot capture traffic between switches, can only capture traffic between network devices

PORT MIRRORING

uses existing capabilities of network switches to send network packet copies from one switch port to a network monitoring connection on a second switch port.

Note: In Cisco systems, port mirroring is called Switched Port Analyzer (SPAN).

Pros: low cost, can be configured remotely throughout the network, captures traffic between switches

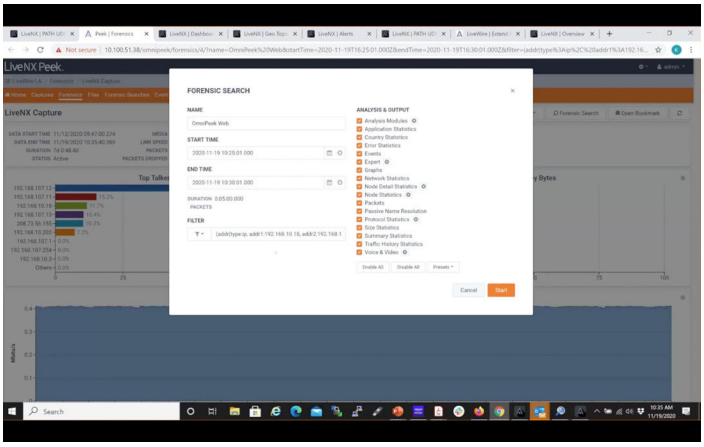
Cons: can drop packets on full-duplex links that are overburdened, does not capture physical layer errors when network is saturated

Once the packets are captured, they can be used to troubleshoot problems in the past. How far into the past you can troubleshoot problems with packets depends on how much disk space you have to store them. In most systems, including LiveWire, when the disk fills up, the oldest packet file is removed to make room for new packets. This is one of the differences between packets and flow, because flow takes less space and the data can be saved for longer periods of time.

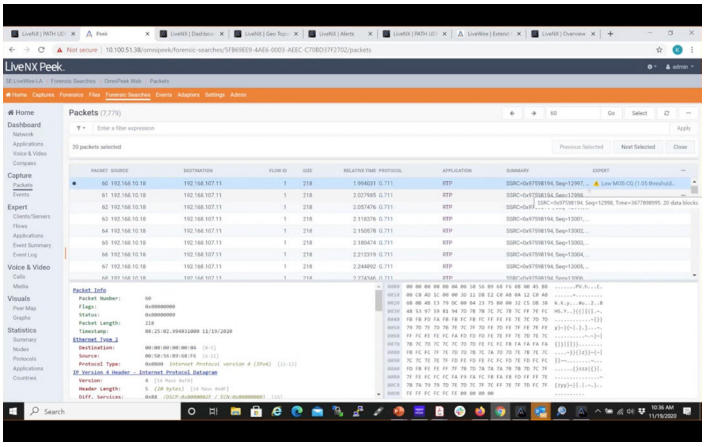
Packet Capture

Here is an example of a forensic search from our **LiveWire** platform using a specific time frame to drill down to the VoIP performance issue. By using LiveNX to find the call or alert related to the call you can cross-launch over to the packets for the call with a single click. By using this platform, admins can even replay the call to understand the exact experience the end-user had.

STEP 1 | **Search within a timeline**

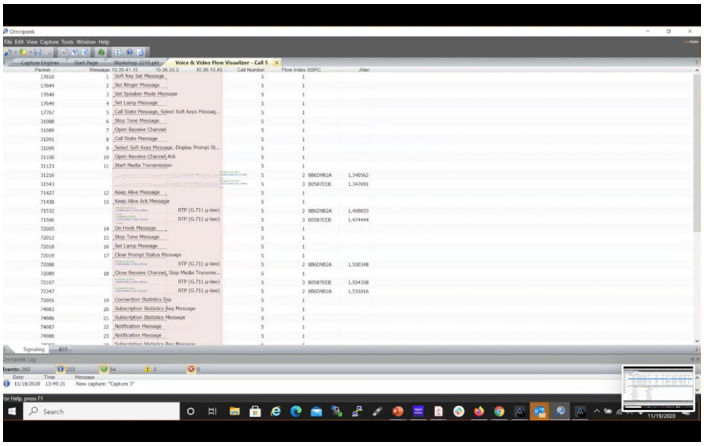


STEP 2 | **Find the packet with the alert**



Once the packets are found, LiveWire will re-analyze them and use deep forensic analysis to provide greater detail. For example, the one alert that may have been generated by the flow, can result in many lower level expert events in LiveWire, helping you to better understand the situation, and leading you closer to solving the problem.

STEP 3 | **Gain granular packet details to troubleshoot the root cause**



Through the use of ladder diagrams which provide correlation with different types of analysis, the flow of the call and what problems happened along the way become clear.

Packet Capture

Challenges with Packet Capture

Too Much Data

While packet capture has all the details needed to get to the root cause of network problems, this volume of information can lead to data overload.

It can be hard to zoom out and identify long-term historical patterns and network trends like you can with the topology graphic views and reporting functions in flow analysis. Packet capture is so much information that even if it is compressed and filtered down to just the packet header, the most you can store packet history is a few weeks back.

Free Tools Are Not Often User Friendly

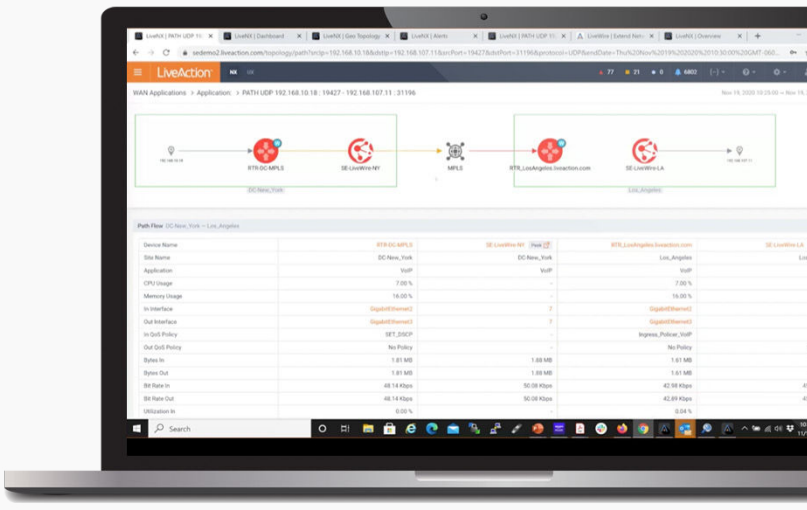
Unlike flow analysis, most free packet capture tools require users to have a high technical acumen. They were built with the assumption that they would be used by experts who understand everything about network operations and protocols. This can be a little intimidating and inaccessible for someone newer to their NetOps journey and may push them from packets to flow.

Additionally, cables must be connected between the mirror ports and the DPI application if you use the port mirroring technique.

The Best of Both Worlds

You can easily identify problems using flow analysis and then drill down to the root cause using packet capture. A combination of these methods allows you to detect and address bandwidth greedy applications sooner than later and see usage trends on an app and user level.

In our screenshot below, we show an example of an integrated system of both flow analysis and packet capture.



LiveAction allows you to hop from LiveNX directly into LiveWire's Omnipeek within the same interface.

We've summarized and compared the features of each technology in this table so you can see where they overlap and where they require the other for full coverage.

Packet vs Flow Comparison

FEATURES	PACKET	FLOW
Real-time analysis	✓	✓
Historical data	Cannot store more than a few weeks at best because of large data volume.	✓
Web Domain reporting	✓	
VoIP reporting	✓	Useful for high-level reporting but packets are often needed to troubleshoot problems
Easy set up / user-friendly	This depends on the packet capture tool, but generally this is not its strength.	✓
Contains granular details	✓	
High-level visibility		✓
Can monitor edge of network	✓	
Help detect rogue DHCP servers	✓	✓
DNS resolution	✓	✓
Does not require a lot of storage space		✓

Conclusion

Although both technologies are effective and useful in different situations, a truly comprehensive network traffic analysis requires both. The conclusion is Packet + Flow, not Packet vs. Flow.

With a combined solution you get top-level network visibility (without needing cables) and then can jump down into packet-level detail to investigate. Looking at packet data alone can be too zoomed in to reveal broader network trends. And using just flow analysis can miss critical information that reveals the root cause of a problem.

These tools work naturally as an extension of each other, along with SNMP for complete monitoring visibility.

LiveAction®

960 San Antonio Rd, Suite 200, Palo Alto, CA 94303
+1 (888) 881-1116

About LiveAction

LiveAction has invested in creating user-friendly packet capture tools like **LiveWire** that integrate with flow analysis and other metrics in our **LiveNX** tool for total network visibility. LiveAction's Network Traffic Analysis tools offer the broadest telemetry available anywhere.