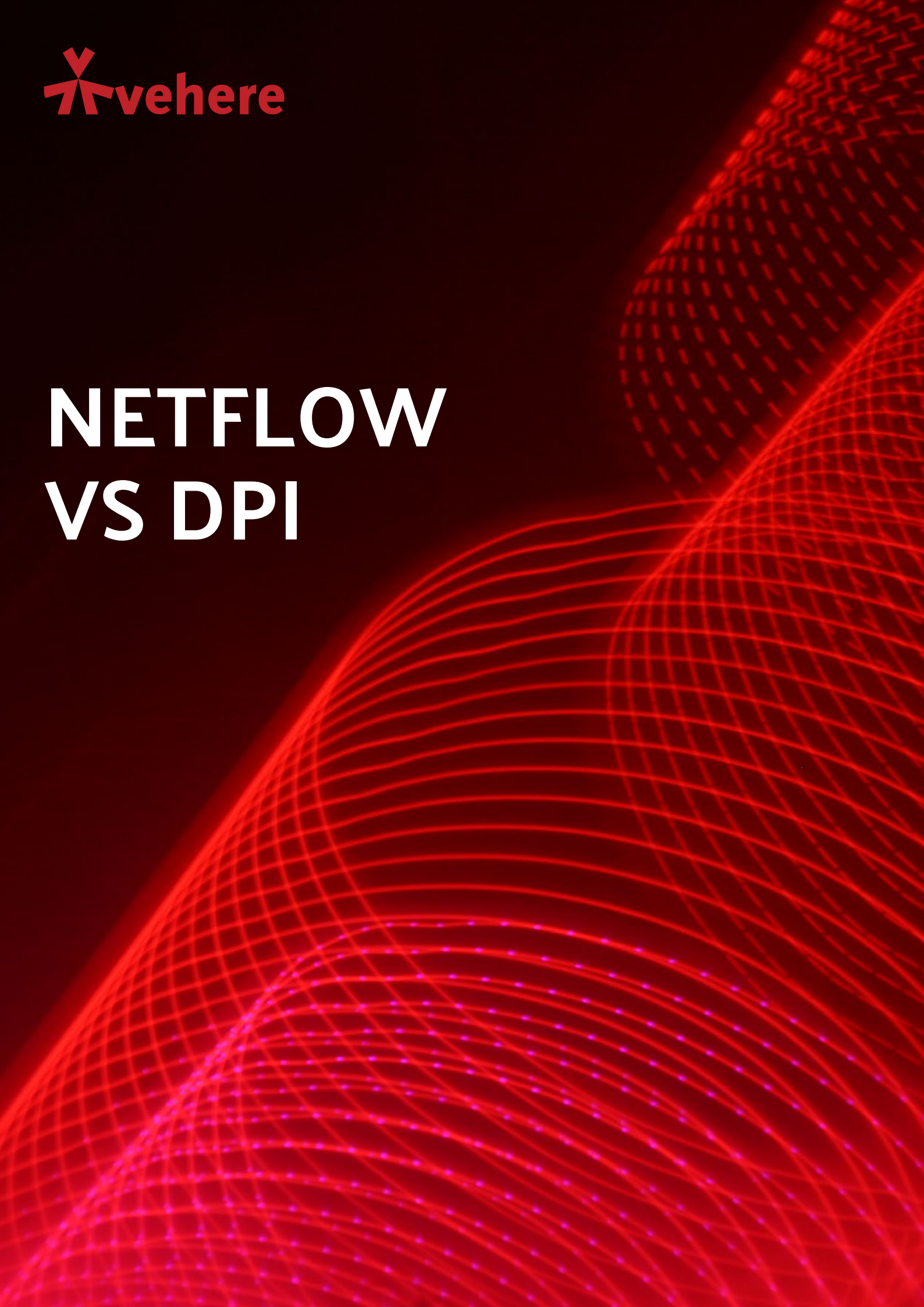
vehere

NETFLOW VS DPI



NETFLOW VS DPI

Know the difference

"NetFlow is a feature that was introduced on Cisco routers around 1996 that provides the ability to collect IP network traffic as it enters or exits aninterface. By analyzing the data provided by NetFlow, a network administrator can determine things such as the source and destination of traffic, class of service, and the causes of congestion". https://en.wikipedia.org/wiki/NetFlow.

NetFlow was traditionally designed for network performance monitoring and visibility. It existed well before the proliferation of security teams and is now present in many organizations. As a result, many security teams have leveraged NetFlow data and do so even today. Unfortunately, NetFlow doesn't provide enough visibility or context required for today's incident response teams as it lacks application level details and was never designed from a security teams' perspective.

The downside is that NetFlow doesn't provide nearly the level of detail that full packet capture data provides. While it is useful in alerting to potential issues, it can't necessarily tell you exactly what happened, or allow you to rebuild and examine files that have been exfiltrated from the network, for example.

The other issue with NetFlow, is that it was originally designed just to provide trend data for historical changes in network performance and trend analysis. For this purpose, sampled data is sufficient, so many of the devices that generate NetFlow data are configured to sample packets to generate that data, rather than looking at every packet. While many can be reconfigured to generate 1:1 NetFlow records (where every packet is examined), some cannot. Which means they are not reporting on all the activity on the network.

The demand of generating NetFlow on routers and switches can take a significant performance toll. For this reason, they are often configured to generate sampled NetFlow only, in order to reduce load.

Netflow is great to solve network performance issues but falls short of network security forensics and has much more dependency on the underlying network infra compared to just ingesting SPAN/Mirror traffic of the core switch.

NetFlow Pros:

- Easy to setup on devices which operate at layer 3
- No cabling required
- No software clients or agents needed on end user systems

NetFlow Cons:

- Lacks much of the context required for security incident analysis
- No flow options on some switches
- Lacks detail when you want to troubleshoot a problem
- Not ideal for monitoring at the edge of your network where applications piggy back on other protocols

Deep Packet Inspection (DPI), or full packet capture, gives you the full story. Packets let you accurately reconstruct exactly what happened and when it happened so you can uncover the cause of security incident quickly and definitively

Using deep packet inspection, you can reconstruct a data exfiltration attempt to see precisely what was taken or focus in to microscopic level to unearth short-lived security events that simply don't show up at NetFlow's meta level of detail

While it might not be feasible to store years of full packet capture history, it is certainly feasible to store weeks to months. Particularly if packet data is compressed, and irrelevant data truncated to remove the unwanted packet payloads for certain payload types for example do not store the video calls, songs, video transmissions, etc.

When it comes to the provision of information, packet capture brings it all in. Full packet capture allows extracting events to your real-time tools for back in-time investigation and removes the needle-in-a haystack approach of attempting to assemble and correlate evidence from multiple sources such as log and transaction files and NetFlow data. This factor makes for an essential point. Simply put, packet capture tools carry out Deep Packet Inspection (DPI) on targeted fields to provide extensive detail on its target, while probes carried out by NetFlow can be said to be superficial, as most of the times, they sample packets to generate data instead of assessing each packet as they travel through the network. Where NetFlow skips a trend, packet capture will place its beam on the dark corner and create visibility on previously undetected activities.

DPI Pros:

- Better for analysis of application and user behaviour. Detect bad vs. good use of bandwidth
- Ideal for monitoring important applications, servers or Internet connections where low level information is critical
- You get a lot more 'names'. Application, file, website and host names.
- No software clients or agents needed on end user systems

DPI Cons:

- You need to connect cables between mirror ports and your DPI application
- Need to watch that mirror ports don't get overloaded on busy networks
- Requires high amount of storage as compared to NetFlow

How NetFlow and Packet Capture work together

NetFlow enables very efficient on-the-fly monitoring and allows your team to keep up-to-date with network events as they happen. But it is significantly strengthened by access to network packet history. You can quickly drill down to packet level, examine incidents and determine their root cause and severity.

With full, packet-level detail, investigations are both faster and more conclusive. Network and security analysts can keep on top of the mountain of alerts they receive every day, ensuring an unexamined issue doesn't escalate to become a serious security breach or service outage.

As you see, each method has its own strengths and weaknesses in providing engineers with the right data in the right place at the right time. And which method should we use in a network security monitoring solution, you asked? It doesn't have to be an either/or, you need a security solution that leverages the best of both methods by extracting metadata from the raw packet files to help speed up in real time and back in time analysis.

What you need is a single, cost-effective solution that addresses both local and remote monitoring to keep shortening the MTTR. Vehere NDR Cyber Situational Awareness solution, combining the strengths of both DPI and netflow methods in an effective and scalable form as in the end, that's what it's all about—lessening time to resolution when an incident occurs on your network. Combing the two technologies can lessen investigation time from hours or days to just minutes. To make a long story short, you need both.

So don't be fooled into thinking your organization needs only one of the two. The reality is you need both since they support and feed off each other. And as digital transformation continues to push rapid change in IT, it is even more critical that NetFlow and PCAP – working together – become a significant piece of your CIRTs detection arsenal.