WHITE PAPER

Network Detection and Response

A technical white paper

Plixer

Introduction

The days of relying on threat prevention are over. Preventative solutions are still important, but the reality is most threat actors are too sophisticated to be stopped by these methods and tools. Enterprises need to have a robust toolkit for detecting and responding to network compromises. The Plixer network detection and response (NDR) platform is an advanced tool for security operations teams that provides complete visibility into network traffic for threat detection and response.

The Plixer NDR platform bridges cloud and on-premises environments to provide real-time, end-to-end visibility for anomaly detection and correlation, network and application performance, and traffic patterns and trends.

Why we don't rely solely on packets

Most NDR solutions rely on packet capture to detect threats, which require probes or other collection agents. In theory, this seems fine, but as you begin to scope out collecting packets across your network, it very quickly becomes a problem. For one, it is often cost-prohibitive to place packet capture tools across your network. Additionally, packet capture infrastructure is complicated to deploy and requires a lot more storage than network flow data. Because of this, packet capture is almost always limited to a few key areas of the network. The most common areas to place packet capture tools are at ingress and egress points of the network. The inherent weakness of this method is that it limits visibility to the traffic coming into or exiting the network and only in those areas being captured—this leaves SecOps teams blind to potential compromises across the network.

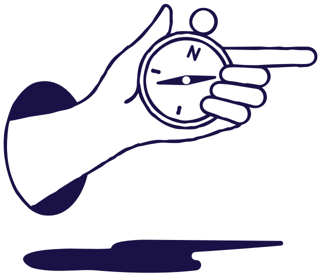
Packet analysis offers great insight into the conversation details between devices on your network, but they come with big caveats and exceptions. Deploying and operating a packet capture infrastructure is a highly complex process that requires SecOps to buy packet capture capabilities and physically deploy, monitor, and update them. As mentioned earlier, packets are very resource hungry. To help reduce space, packets are often compressed to metadata (headers, timestamps, etc.).

NDR feature	Plixer NDR	Packet-based NDR
Detects lateral movement	✓	✗
Detects C2 communication	✓	Sometimes
Detects movement of sensitive data	✓	Sometimes
Detects abnormal activity across the network	✓	Sometimes
Detects data exfiltration	✓	✗
Delivers host classification/ profiling	✓	✗
Confirms zero trust	✓	✗
Cloud visibility/detection	✓	✗

In contrast to packet-based solutions, the Plixer NDR platform taps into network flow data captured by your existing infrastructure to power its detection and response capabilities. Plixer's NDR platform monitors north/south traffic that crosses the enterprise perimeter, as well as east/west traffic, collecting and contextualizing both network-related data and metadata from physical, virtual, and cloud environments. Full network visibility enables SecOps to fine-tune desired alarm frequencies, thresholds, and patterns. These can then be pushed as alert data into existing solutions, like network access control (NAC), firewalls, web application firewalls, and SIEM/SOAR tools.

Why we use network flow data

Unlike packet-based solutions, the Plixer NDR platform ingests and analyzes network flow data from your existing enterprise infrastructure—switches, routers, firewalls, packet brokers, security tools, network monitoring systems, and more. We tap into the existing network infrastructure that you've already invested in. We use this readily available network flow data to provide insight into every conversation in the network. Network flow data gives you a real-time, end-to-end view of traffic across the network.



Network flow data can provide highly acute insight into behavior on your network. When processed through a sophisticated ML engine, network flow data reveals typical device behavior patterns across the entire network. By using this data as a baseline, the Plixer NDR platform helps make the tactics, techniques, and procedures of a threat actor more easily detectable than if you were monitoring only for signs of a breach.

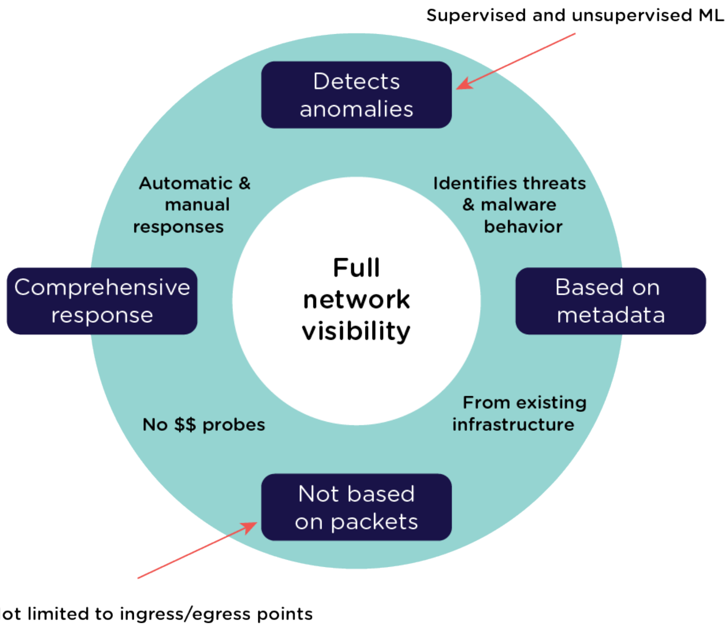
In contrast, packet capture probes are rarely placed across the entire network and so will not provide pervasive network visibility in the same way that network flow data can. Most packet-based NDR vendors use packet analysis to extract metadata similar to flow data and then supplement network blind spots with flow data. However, because these vendors do not focus on network flow data as the primary source of network behavior, their solutions often fall short of detecting the behaviors the Plixer NDR platform is able to identify.

With the Plixer NDR platform, SecOps teams can also fine-tune desired alarm frequencies, thresholds, and patterns that are pushed as alert data into existing solutions, like NAC, firewalls, web application firewalls, and SIEM/SOAR tools.

Many people assume packets are the best method, despite their complexity and resources needs, because they provide access to more data—in the form of the payload. This assumption is challenged, though, when it comes to encrypted traffic. Suppose a hacker has compromised your network and is moving data from one area to another to prepare for exfiltration. A packet's payload should show you what exactly was moved. If the traffic is encrypted, though, then you'll need to account for more overhead in your process to decrypt the traffic. But the problem gets more complicated if the hacker has brought their own encryption. In this case, you will not be able to decrypt the packet, leaving you blind to actual data that was moved. More often we see organizations using encrypted traffic on their networks, and threat actors are increasingly encrypting their traffic as well. If you're unable to decrypt the packet, you wind up with the same data you would get from network flow data—but with more effort and resources.

Features of the Plixer NDR platform

The Plixer NDR platform collects, analyzes, visualizes, and reports on data from every network transaction. By providing insight and historical data, SecOps teams have a source of truth to reduce risks, detect threats, and respond to incidents. The advanced platform uses network infrastructure data to provide real-time, end-to-end visibility for anomaly detection and correlation, network and application performance, and traffic patterns and trends.


Supervised and unsupervised ML
Detects anomalies
Automatic & manual responses
Identifies threats & malware behavior
Comprehensive response
Full network visibility
Based on metadata
No $$ probes
From existing infrastructure
Not based on packets
Not limited to ingress/egress points

Gauge and reduce risk: Reducing risk requires a combination of strong forensic data, detailed context, powerful reporting, and the ability to hold users accountable. Using flow analytics for detection, the Plixer NDR platform provides proactive alerting via programmable thresholds to ensure user accountability.

The platform gauges the risk posed by all network-connected devices, isolates vulnerable devices, and mitigates threats by scoring device risks in real-time and creating risk scores for the entire network—as well as for individual devices. Scores are calculated for each device by examining four risk categories:

- Operating system : To assess the inherent risk associated with a device's underlying OS, a risk value is automatically assigned to each device by determining if the device is running the latest supported OS release, as well as by gauging how susceptible the device is to malware and other threats
- Profile identity: To assign risk that's inherently associated with each device, a score is automatically assigned based on the device profile
- Communications risks: Risks related to communications are assessed by identifying when unsecure protocols that expose the enterprise to data theft are being used
- Integration: Risk management data can be incorporated from external sources, including vulnerability, patch, and antivirus/ malware management solutions, to extend the value of technology investments

Anomaly detection and response: The Plixer NDR platform uses both supervised and unsupervised machine learning (ML) to recognize traffic anomalies, enabling it to dynamically detect previously unknown threats, identify traffic behaviors of malware families, and improve investigation efficiency. Using the network as a sensor, the platform monitors network traffic to identify indicators of compromise in real-time, including whether an attack is volumetric-, application-, or protocol-based. Proactive thresholds, alerting, and open RESTful APIs then enable rapid and dynamic event response.

Leverages DPI and DNS: Deep packet inspection (DPI) is used to monitor internal and cloud-bound critical application traffic, empowering SecOps to monitor critical application traffic in order to find the root cause of problems. Likewise, the Plixer NDR platform observes domain name system (DNS) traffic across the entire network to detect abnormal behavior and security threats.

Contextual forensics: The Plixer NDR platform visualizes every conversation from Layers 2-7 and then provides context and data correlation that make that data useful. Context is derived from the correlation of network-related data with metadata and is gathered from firewalls, IDS/IPS, SIEM, and distributed probes. Better context is achieved by correlating traffic flows and the metadata collected from all corners of the network into a single database. Root cause analysis then instantly identifies the user, device, location, protocol, and application data for every flow on the network.

Comprehensive response for faster time to resolution: Extensive response capabilities include automatic responses (i.e., sending commands to a firewall to drop suspicious traffic) and manual responses (i.e., providing threat hunting and incident response tools). By correlating flows and metadata across the entire network infrastructure, the Plixer NDR platform provides visualization and reporting of forensic details needed for faster time to resolution. Likewise, rich contextual data is used to establish the root cause of issues, while also supporting flexible and rapid reporting, as well as user accountability.

Summary

The Plixer NDR platform enables SecOps teams to identify and stop threats before they cause business disruption – regardless of where vulnerabilities are in the network. By ingesting and analyzing network flow data from existing infrastructure, the Plixer NDR platform avoids the problems associated with packet-based solutions. It bridges cloud and on-premises environments to provide real-time, end-to-end visibility for anomaly detection and correlation, network and application performance, and traffic patterns and trends.

About Plixer

Plixer provides a single platform for network security and monitoring, delivering the insight and analytics needed to manage the immense opportunities and risks of a digital business. As a leader in the Network Detection and Response & the Network Performance Monitoring and Diagnostics markets, Plixer provides the comprehensive intelligence and visibility needed to analyze, evaluate, and visualize the millions of conversations that cross networks every second.

The content in this document is for informational purposes only and is subject to change by Plixer, LLC without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, Plixer, LLC assumes no liability resulting from technical or editorial errors or omissions, or for any damages resulting from the use of this information. Unless specifically included in a written agreement with Plixer, Plixer, LLC has no obligation to develop or deliver any future release or upgrade or any feature, enhancement, or function.