WHITE PAPER

Plixer Network Performance Monitoring and Diagnostic Platform

Plixer

Introduction

The Plixer network performance monitoring and diagnostic (NPMD) platform is a flexible solution for network operations teams to continually monitor network and application performance, while also detecting abnormalities that impact network performance, scalability, and availability.

Digitalization, automation, the Internet of Things (IoT), hybrid, and multi-cloud environments—all of these and more—are creating massive changes in today's enterprise networks, requiring NetOps teams to rethink how they monitor and secure those networks. Plixer's NPMD platform uses network flow data to monitor and secure both perimeter and internal network resources, empowering NetOps with a single solution that meets the challenges of today's enterprise networks.

Why network flow data?

Unlike most network detection solutions that depend upon expensive collection tools like packet capture technology, Plixer's NPMD platform takes advantage of your existing infrastructure to collect network flow data across the entire network.

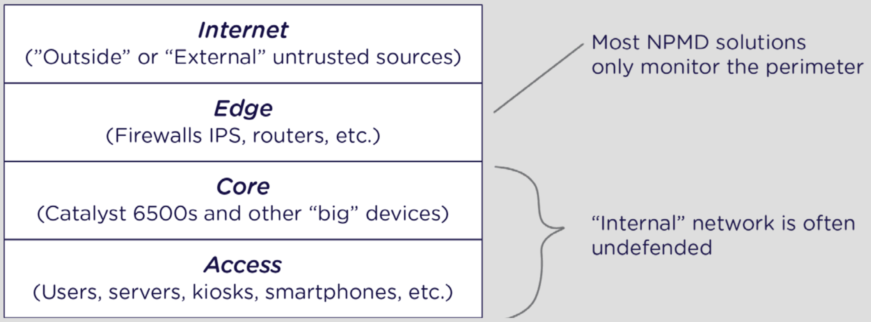
Enterprise network infrastructure is a storehouse of rich metadata that provides insight into every conversation that occurs in the network. Plixer's NPMD platform ingests and analyzes network flow data from that infrastructure—switches, routers, firewalls, packet brokers, security tools, network monitoring systems, and more.

It bridges cloud and on-premises environments to provide real-time, end-to-end visibility, giving you access to every network conversation happening. With that scalable visibility, you can easily understand network and application performance, interpret traffic patterns and trends, and retain logging for historical, root cause analysis.

Monitoring the internal network—not just the perimeter

Plixer's NPMD platform collects and contextualizes network-related data and metadata from locations in physical, virtual, and cloud environments. While most NPMD solutions only monitor north/south traffic that crosses the enterprise perimeter, Plixer also monitors east/west communications to provide complete network visibility and detection.

Monitoring the internal network


Internet
("Outside" or "External" untrusted sources)
Edge
(Firewalls IPS, routers, etc.)
Core
(Catalyst 6500s and other "big" devices)
Access
(Users, servers, kiosks, smartphones, etc.)
Most NPMD solutions only monitor the perimeter
"Internal" network is often undefended

The access layer—made up of smartphones, IP phones, laptops, servers, and virtualized infrastructure—is the most important place on the network to monitor. But it's far too complex to rely on disparate tools that require a manual process.

Most NPMD solutions only monitor the perimeter—firewalls, proxy servers, data loss prevention (DLP) solutions, and other edge technologies. In contrast, Plixer's NPMD platform monitors the entire network, including the access layer.

Features of the Plixer NPMD platform

Plixer's NPMD platform collects and refines data from diverse sources for asset discovery and profiling. The platform also provides proactive thresholding, advanced reporting, and alerting to ensure user accountability. Likewise, it enables real-time insights into device identity, location, and behavioral data to simplify operations and automatically identify and remediate threats. And when a network issue becomes a security issue, your NetOps and SecOps teams can easily collaborate, leveraging the same intelligence.

Device discovery: Organizations need to efficiently track assets scattered across a distributed enterprise to gain a complete and accurate view of all network endpoints, including managed, unmanaged, authorized, and unauthorized devices. The Plixer NPMD platform identifies the types of devices that are connected to the network, including where they are located and how they behave, in real time. By validating enterprise software license agreements against actual device or use counts, the solution ensures contract compliance and audit readiness.

Profiling: The platform collects and analyzes contextual data from a wide variety of sources, including DNS, DHCP, SNMP polling, SNMP traps, NetFlow/J-Flow/sFlow, Active Directory, RADIUS Accounting, and port mirroring. It then categorizes endpoints using thousands of predefined device profiles, reducing dependence upon manually intensive, time-consuming processes, which then frees staff to focus on core business tasks.

Features of the Plixer NPMD platform with the addition of network intelligence

When the Plixer NPMD platform is combined with artificial intelligence (AI) and machine learning (ML), it dynamically predicts network capacity requirements and monitors data volumes. Staff resources are then supplemented through automation and dynamic data sharing.

With advance notice of capacity requirements, operation teams can identify future usage hotspots, forecast multiple classes of data, generate threshold boundaries, identify seasonal variances, and generate data in support of infrastructure planning.

Evaluating endpoint risks: To isolate vulnerable devices and mitigate threats, the platform starts at the endpoint. It does this by providing and individual risk score in real time for each specific endpoint, and then correlates the individual score to provide a collective risk score. At this level, the risks are broken out into distinct categories that enable administrators to isolate high-risk endpoints.

Detailed configuration and operating information are provided for individual devices, and an individual risk score is calculated for each endpoint by examining four risk categories:

- Operating system (OS): To assess the inherent risk associated with an endpoint's underlying OS, a risk value is automatically assigned to each device by determining if the endpoint 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

Application performance monitoring: Many factors can impact application performance, including packet loss, retransmits, round-trip time, and the physical location of an end user. Resolving issues around poor connection times requires more than simply reviewing bandwidth utilization trends to determine if the problem is isolated to a specific end system, end user, subnet, or whether it impacts the entire organization.

To identify the root cause, the platform leverages deep packet inspection (DPI) to monitor internal and cloud-bound critical application traffic. Through DPI, the platform can provide detailed visibility into each connection to ensure optimized end-user experience.

Contextual data identify root cause: Plixer enables the visualization of 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.

Faster time to resolution: By correlating flows and metadata across the entire network infrastructure, Plixer provides visualization and reporting of details needed for faster time to resolution. Likewise, rich contextual data is used to establish the root cause of issues, support flexible and rapid reporting, as well as user accountability.

Summary

Plixer's NPMD platform empowers NetOps teams with real-time, end-to-end network visibility of every network conversation, correlating and contextualizing alerts across your corporate network. Using network metadata, Plixer monitors and reports on both perimeter and internal networks with real-time, end-to-end visibility that understands network and application performance, and interprets traffic patterns and trends. Plus, the ability to retain logging data for extended periods means you'll have it for historical, root cause analysis. With two deployment options, Plixer NPMD enables enterprises of all sizes to continually monitor network and application performance, detect abnormalities that impact network performance, and remediate issues when identified.

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.

©Plixer, LLC. All rights reserved. Plixer and Scrutinizer are trademarks of Plixer. All other brand names are trademarks or registered trademarks of their respective companies.

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.