WHITE PAPER

The Plixer Advantage

NETWORK SECURITY AT SCALE

Rapid detection. Unrivaled protection.

With the global cost of a data breach estimated at $4.35 million, enterprises are recognizing three important truths: Their networks will be compromised, they can't rely on prevention measures to stop attackers from getting onto their networks, and they need to minimize the impact that compromises will have.

Further complicating the issue are several shifts that have occurred in enterprise network security. The first is a shift in how corporate network resources are controlled. Increasing public cloud adoption coupled with a rise in the number of end-user devices – think Internet of Things (IoT) devices in homes, industrial environments, transportation networks and elsewhere – limits network visibility and the ability to place strong controls. Another shift is that cyberattackers now are finding ways to monetize every attack. This is evidenced by the rise of ransomware, as well as through the theft of personally identifiable information (PII), proprietary information, trade secrets, credit card and financial data.

All of these shifts make it critical for enterprises to quickly pivot from detection to investigation, while gaining access to the historical data necessary to understand the full scope of an incident.

Network Detection and Response (NDR) solutions enable enterprises to address all of these issues. NDR solutions use machine learning and other analytical techniques to process network data in real time and build models to represent normal network behavior. When anomalous behavior is detected, NDR solutions raise alerts and provide manual or automatic actions that network and security operations teams can use to remediate incidents.

While there are many NDR solutions on the market today, it's important to understand that not all of these solutions are created equally. Choosing the right NDR solution requires you to know what to look for, the difference between solutions that are flow-based and packet-based and how such solutions are used by IT and security teams to combat the flood of cyberattacks that are happening every day.

LIMITATIONS OF MOST NDR SOLUTIONS

The majority of NDR solutions in the market rely on full packet capture in order to function. This means you'll need to architect and maintain taps, spans, probes and other packet infrastructure.

Why are packet based solutions a problem? In theory, it's a great way to get rich network data. But in practice it is costly, complex, and lacking the value it promises. Here's a quick look at why:

- **Expense**: It's cost prohibitive to deploy packet capture capabilities everywhere.
- **Extended time-to-value**: Deploying such solutions is a complex process that requires you to physically deploy, monitor and update packet capture capabilities – significantly lengthening time to value.
- **Limited detection of ransomware**: Detecting ransomware largely depends upon seeing lateral movement in the network, which isn't possible with packet-based solutions.

- **Misses traffic**: Packet-based solutions are typically focused on north/south traffic, leaving network blind spots to east/west traffic, the cloud and data centers.
- **Limited value with encrypted traffic**: Most network traffic is encrypted. Decrypting the payload means storing keys, storing the payload for an extended period and risking internal security risks by decrypting your own traffic. But the reality is an attacker will encrypt their traffic and you will not be able to decrypt the packets that actually matter. Packet-based NDR solutions will only be able to process the packet's metadata (essentially the network flow data). So you're paying extra and using more resources to get the same result as a flow-based solution like Plixer.

THE PLIXER ADVANTAGE

Unlike other vendors, Plixer's NDR solution does not require additional infrastructure to operate, giving enterprises a broader view into their network at greater scale and flexibility with faster time to value.

Plixer's platform ingests and analyzes network flow data (metadata) from your existing infrastructure—switches, routers, firewalls, packet brokers, security tools, network monitoring systems and more. It bridges cloud and on-premises environments, providing real-time, end-to-end visibility that enables you to detect and correlate anomalies, understand network and application performance, and interpret traffic patterns and trends.

Full network visibility

Plixer's platform collects and contextualizes network-related data and metadata from network locations in physical, virtual and cloud environments. It monitors north/south traffic that crosses the enterprise perimeter, as well as east/west communications to provide complete network visibility and detection of attackers as they move laterally within the network. The platform lets you monitor single hosts or entire subnets from multiple levels in the network. Using intelligent de-duplication, users see alarm data that's accurate and trimmed down to only what they need to see.

Comprehensive response

Whereas many NDR vendors tack on response as an afterthought, Plixer provides extensive response capabilities. This includes both automatic responses, such as sending commands to a firewall so that it drops suspicious traffic, as well as manual responses through threat hunting and incident response tools. With full network visibility, you can push alert data into existing solutions—network access control (NAC), firewalls, web application firewalls and SIEM/SOAR tools—fine-tuning the desired alarm frequencies, thresholds, and patterns.

Vendor-agnostic, seamless integration

Integration with hundreds of network monitoring tools from third-party vendors gives the Plixer NDR platform the ability to ingest their flow, establishing a baseline of network activity to set appropriate thresholds. A notice of compromise is created whenever traffic deviates from normal behavior. But if something is truly wrong, the platform alerts into the workflow tools you use.

Anomaly detection

The Plixer platform uses supervised and unsupervised machine learning, as well as deep learning to recognize traffic anomalies. By doing so, it dynamically detects previously unknown threats, identifies traffic behaviors of malware families, and improves investigation efficiency.

Cost containment

Plixer's platform leverages data that's already available in the network and can be deployed in distributed environments – providing significant savings over solutions that rely on sensors to collect network data, including packet-based solutions.

NETWORK SECURITY ON YOUR TERMS

For over 20 years, Plixer has been at the forefront of collecting, visualizing, and reporting on telemetry data generated from every conversation that crosses the network, from the end user all the way into the cloud. This context-rich flow data is collected directly from the existing multi-vendor infrastructure.

Unlike competing solutions that require the implementation of expensive and proprietary appliances, Plixer's implementation collects data that is exported directly from the existing infrastructure (switches, routers, firewalls, packet brokers, etc.). This differentiated approach is frictionless. It eases implementation, reduces complexity, and makes scaling your threat detection more cost-effective and less complex. Plixer offers two tiers of a network security solution. Both solutions, however, also include network performance and diagnostic data to help serve both NetOps and SecOps teams.

Plixer Enterprise Platform is a full NDR & NPMD solution. This platform is built upon Plixer Core Platform, which comes native with Endpoint Analytics, and includes an ML engine for ML processing and uses Plixer FlowPro for DNS, application, and other IPFIX data enrichment. This platform offers flexible deployment options and can integrate with the systems present in your environment.

Plixer Core Platform is a network monitoring solution that offers key security and performance analysis. Endpoint Analytics is a native component of the platform. For additional data enrichment on applications, DNS, or other data sources, Plixer FlowPro is recommended. Like Plixer Enterprise, this platform can be offers flexible deployment options and can integrate with the systems present in your environment.

To fully understand the differences between the platforms, we've provide a table below which covers a sample of the differences between Plixer Core and Plixer Enterprise.

SUMMARY

Attack surfaces are widening and cyber threats are increasing in number and sophistication, putting your business's reputation and bottom line at risk. The data deluge and false positives make it a challenge to combat these growing threats.

Plixer helps you rapidly detect and neutralize critical threats in real-time. With advanced AI and machine learning, you can identify, prioritize, and respond with laser precision and accuracy.

With Plixer you get 90% less noise from false positives, an 80% reduction in investigation time, a 47% increase in threat neutralization accuracy, and a 40% cost-efficiency compared to other NDR solutions.

Join the new network defense revolution today and book a demo.

ABOUT PLIXER

Plixer gives you visibility and context of every network transaction so you can better understand what's happening in your IT environment. Our 20+ years of network monitoring and management solutions help us provide innovative solutions that help you secure and optimize your digital enterprise. Supercharge your business defense with AI-powered visibility and insight that goes beyond traditional NDR.

sales@plixer.com

plixer.com

68 Main St Ste 4
Kennebunk, ME 04043

PLIXER