WHITEPAPER

Find and respond to network issues faster with machine learning

How Plixer uses machine learning for network security and performance

Plixer

What is machine learning and why is it important?

Imagine trying to make sense of the millions of data points created by each network device interaction. With the size of today's typical enterprise network, the sheer number of people and hours needed to analyze a single day of interactions only emphasizes the impracticability of the task. Analyzing that amount of data is only efficiently possible with Artificial Intelligence (AI) and the application of Machine Learning (ML)—a subset of AI.

An ML engine can ingest all your network flow data and see the underlying behavior patterns to make sense of the data and refine its understanding over time to provide actionable insights. In short, the ML engine adapts to the unique behaviors on your network to provide alerts about potential issues.

> **For network security**: an ML engine provides intelligent threat detection of even the most sophisticated attacks that try to mimic normal device activity.
>
> **For network performance**: an ML engine predicts capacity issues and enables you to track and maintain compliance with a few clicks.

An ML engine can then apply additional AI logic to dynamically eliminate alarms that can be explained and provide relief to under-resourced teams. These advanced capabilities elevate true versus false positives and provide the contextual information needed to resolve problems quickly. This is a welcome relief to an industry that is seeing a talent shortage and skills gap that continues to intensify. With ML you can more easily identify issues, investigate root-cause, and respond before your business can be disrupted.

Types of machine learning

While most people have a general sense of ML and may even employ tools that use ML, they may be unsure how to tell the sophisticated ML applications from the more simple applications. While it's not really an evaluation of good versus bad ML, some companies are more hype than substance when it comes to how their tools apply ML to achieve the purpose of the tool.

All ML is used to continuously better the performance of a desired function. For example, the desired function of an ML engine could be to trigger network alarms (for either security or performance monitoring) about abnormal device behavior. Or the desired function could be to forecast future network behavior based on current patterns.

To better understand if a prospective vendor is using ML in a way-that will be helpful to you, look for:

- How the ML is used in the tool (i.e., for reporting, alerting, etc.)
- What resources are needed to deploy and manage it
- How long it will take to prime the ML engine
- How flexible it will be at taking in new datasets

Having a basic understanding of ML will help you better understand any answers to the above questions when evaluating a tool. There are three main ways that ML can learn and increase performance accuracy:

- **Supervised learning**: the process of training an ML on specific datasets to achieve a desired result—i.e., identify characteristics of malware
- **Unsupervised learning**: the process of ingesting new datasets and allowing the ML to make its own connections
- **Deep learning**: A progression of supervised and unsupervised learning to create an artificial neural network that can learn and make intelligent decisions on its own

While Plixer uses all three, classic ML engines only employ unsupervised and supervised learning. Deep learning is becoming more prevalent but is not quite as common. For actionable network intelligence, it's important to have ML process flow data from your network. Each network is too unique to be analyzed from a generic dataset. Additionally, for threat detection, having an ML engine that has been trained through supervised learning to recognize common characteristics of malware can greatly reduce mean time to resolution (MTTR) and the risk of a significant data breach. A vendor that uses deep learning can further progress the accuracy and usefulness of the ML being applied to detect network issues.

How Plixer's NDR platform uses machine learning

The Plixer NDR platform leverages ML to help security teams in a few important ways. The ML engine ingests network flow data to set a baseline for expected behavior on the network (who talks to whom, which applications are being used and in what ways, who's present on the network at which times, etc.). After about a week of observing the network, the Plixer ML engine has learned to distinguish normal from abnormal traffic behavior. Additionally, we've accounted for granular configurations, such as subnet activity, custom sensitivity thresholds and seasonality behaviors—to account for behavior on nights and weekends or quarterly activities. ML models are regenerated every 24 hours to maintain accuracy.

By processing network flow data, the Plixer NDR platform provides intelligent threat detection. Rather than hunting for indications of a hack after a breach has occurred, the ML engine detects the tactics, techniques, and procedures a bad actor must take to compromise the network in real-time. Because it continuously establishes a baseline for what normal traffic looks like, the ML engine can quickly detect abnormal behaviors like data accumulation, data exfiltration, brute force, tunneling, worm detection, and lateral movements. Once detected, the Plixer NDR platform can then map these to the MITRE ATT&CK framework. With automated forensics, your team can quickly dig into the detection to follow the metadata trail and gauge the severity of the threat.

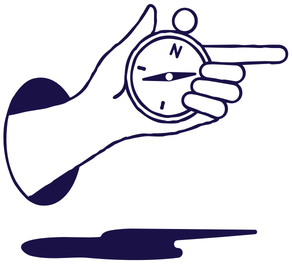
In addition, we've tuned the ML engine to help detect common malware classifications. We trained our ML engine to spot suspicious behaviors by various malware families based on the classification of commonly observed network traffic behaviors. Introducing malware behavioral detections to the ML engine allowed it to more readily find the behavior of devices trying to compromise the network.

The goal of ML is to shorten attacker dwell time. Powerful and intelligent threat detection allows you to remediate compromises on your network before they become disruptive and costly.

How Plixer's NPMD platform uses machine learning

While the Plixer NPMD platform uses the same ML techniques as our NDR platform, rather than monitoring the behavior of devices, the NPMD platform monitors the traffic behavior of network infrastructure interfaces. Plixer's NPMD platform processes all network flow data and uses that as a basis to determine network health and performance. The ML engine analyzes the flow records to create intelligent and actionable insights from that data.

For NPMD, the power of ML comes from two areas – the ability to detect changes in network traffic behavior and the ability to forecast. Changes in observed network traffic behaviors—often challenging to see in complex network environments—are typically an early indicator of network service delivery issues (performance, availability, etc.) before an alarm condition is met. With ML-driven forecasting, you can take any report in the NPMD platform and extend it into the future. For example, say you are looking at a 12-hour report of capacity on one interface. The traffic seems a little heavier than usual but isn't yet alarming. With forecasting, you can project that report into the future to see if it will become an issue or not.



Additionally, you can use forecasting to extract business intelligence via streaming. For example, if your point of sale (POS) system is on the network, you can run a report on traffic from that POS to predict future credit card transactions. This has network implications, but it also has value for general business insight.

As with the NDR platform, the Plixer NPMD platform provides pervasive network visibility and device detection. This enables NetOps teams to thoroughly investigate issues on the network and shorten the time to resolution.

Summary

Using ML to secure and strengthen your network gives your organization a competitive edge. But not all vendors use sophisticated ML for their solutions. Because ML can be used to describe supervised, unsupervised, or deep learning applications, there is a wide variety of ML in the market. Knowing how the vendor you're exploring uses ML can help you make the right decision.

That said, the benefits of sophisticated ML are unmatched. When using a tool that harnesses a combination of supervised, unsupervised, and deep learning, your network security and performance efforts can be greatly augmented for more efficient and effective work.

For SecOps teams, ML ingests network flow data to determine device and application behavior. With a strong baseline, you can be alerted to unusual or suspicious behavior. With ML, you can reduce false positives and shorten the dwell time for threat detection, investigation, and response.

For NetOps teams, you can use ML to process massive amounts of network flow data to see trends and predict outcomes. This type of analysis can be used to precisely predict future network capacity requirements, giving you the information necessary to keep your network performance strong.

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.