



WHITE PAPER

**How to Use Machine Learning to Improve
Network Performance**

WHAT IS MACHINE LEARNING

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 impracticality of the task.

Luckily, you do not have to rely on the human eye to understand network traffic patterns or a spreadsheet to process all your network data. You can easily understand how your network is used and prepare for future changes with advanced machine learning (ML) engines.

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. This allows ML to provide intelligent insight for network capacity planning and forecasting for future growth.

An ML engine then applies 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. 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 simpler applications. While there is not really a battle of good versus bad ML, some solutions rely on basic ML, while others use more sophisticated applications of AI to detect, investigate, and respond to network problems.

In general, 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.

There are three main ways that ML can learn and increase detection 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



HOW PLIXER'S SOLUTIONS USE MACHINE LEARNING

The Plixer's platforms leverage ML to help network teams in a few important ways. The ML engine ingests network flow data to establish a visualization of 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. To improve the dynamic model of what's considered normal, we also account for granular configurations, such as subnet activity, custom sensitivity thresholds, and seasonality behaviors— to account for different behaviors on workdays, nights, and weekends. Customers can also create custom ML definitions to fit their specific needs and further refine alarm accuracy. The ML models are then regenerated every 24 hours to maintain accuracy.

By processing network flow data, the Plixer platform provides intelligent network behavior and resource allocation details that make future capacity planning and forecasting substantially easier than by using basic network data and spreadsheets to properly allocate resources to every part of the network.

The goal of ML is to shorten the amount of time it takes to properly provide resources to the network, so network teams can work on improving user experience instead of fixing capacity issues.

WHAT ARE CAPACITY PLANNING AND FORECASTING

Capacity Planning

Capacity planning is the process of determining the resources required to meet future demand. In the context of networking, this means predicting the amount of traffic that will flow through the network and ensuring that there is enough bandwidth and other resources to handle it. The traditional approach to capacity planning involves collecting historical data, extrapolating trends, and making projections based on assumptions about future growth. However, this approach is often flawed as it is based on historical data that may not reflect future changes in demand.

Forecasting

Forecasting is the process of predicting future events or trends. In networking, forecasting is used to predict the future behavior of the network based on current trends and changes. The goal of forecasting is to predict future network capacity requirements accurately, so that network teams can adjust network resources accordingly to prevent performance degradation.

HOW TO USE ML FOR CAPACITY PLANNING AND FORECASTING

Capacity planning and forecasting are essential tasks for network teams to ensure that their networks can meet the increasing demands of users and applications.



Traditional methods often rely on historical data and assumptions about future growth trends. However, the increasing complexity of modern networks and the unpredictability of user behavior require more sophisticated methods of capacity planning and forecasting. Machine learning (ML) provides network teams with the tools they need to analyze large amounts of data and make more accurate predictions about network capacity needs than manual calculations are likely to provide.

performance, allowing network teams to quickly identify and address capacity issues before they impact users. When unexpected growth happens in segmented portions of the network, and resources are used to the max, network teams can reallocate resources to these network segments before users start to complain about slowness or other network issues. .

Benefits of using machine learning for capacity planning and forecasting:

Improved accuracy

ML can analyze large amounts of data and identify patterns that may not be apparent to human analysts. This can lead to more accurate predictions of network capacity needs, which can help network teams make better decisions about infrastructure investments and resource allocation. Improved accuracy reduces the amount of time that network teams are wasting on false information or anomalous traffic usage, such as when large spikes of bandwidth are consumed before DDoS mitigation systems stop the bandwidth waste.

Better scalability

ML can handle large volumes of data, making it easier for network teams to scale their processes as their networks grow. This means that as networks grow, forecasts can be updated automatically to reflect the increased usage of network resources, which gives network teams the information they need to allocate for future growth before budgets become constrained.

Faster insights

ML can provide real-time insights into network



SUMMARY

Capacity planning and forecasting are critical components of network management. ML can assist network teams with these tasks by analyzing vast amounts of data and identifying patterns that can help to optimize network performance and avoid potential issues.


The use of ML in capacity planning and forecasting offers several benefits, including improved accuracy, real-time analysis, and proactive planning. As businesses continue to expand their digital footprint, the use of ML in network management will become increasingly important, and network teams that embrace this technology will be better positioned to provide seamless and efficient network experiences.

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, 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.