aruba
a Hewlett Packard Enterprise company

SOLUTION OVERVIEW

THE ARUBA AI ADVANTAGE

Experienced data scientists will tell you that the key to a successful application of Artificial Intelligence (AI) is not the math, but the knowledge of the environment and access to the right data to feed the algorithms. Much like an aspiring chef who is wandering around a grocery store with a list of ingredients in hand without the knowledge of how the dish is prepared, products that plug random data into poorly-understood machine learning models soon discover that the results are not particularly useful.

Without the experience and maturity to pinpoint where AI is helpful in solving meaningful network and security problems, the output leads to incorrect conclusions. This is particularly problematic as the results of machine learning models are now being used to automate the changes made to network settings and access in mission critical environments.

Aruba's customers benefit from our extensive domain expertise. With over 17 years of Wi-Fi leadership and thousands of installations with millions of access points and switches, our depth of knowledge and data gathered are critical for secure, autonomous network operations. This is extremely useful in delivering the user experience and performance expected for today's highly mobile workplaces and organizations.

THE BASICS OF AI AND MACHINE LEARNING

Aruba's data science teams use a very specific set of AI techniques called Machine Learning to deliver secure and optimized wired and wireless experiences amidst the complexity and diversity of today's mobile and IoT environments.

Models and algorithms fall into two broad categories: supervised and unsupervised machine learning. Here is a quick overview of each:

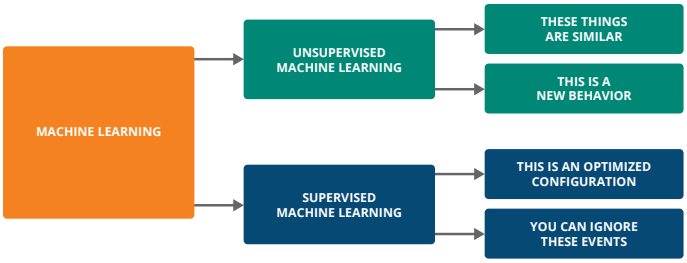
WHAT IS MACHINE LEARNING?

Machine learning (ML) is an advanced branch of artificial intelligence that uses mathematical algorithms (models) to learn and make informed judgements from data, without being explicitly programmed for every situation. When presented with new inputs, ML then uses this data to provide intelligent insights or predict a specific outcome.

Properly applied, ML is particularly well-suited to deal with complex problems such as Wi-Fi optimization, IoT visibility or attack detection inside of an organization.

Supervised Machine Learning. These models are built in collaboration between data scientists and domain experts. The goal is to develop a model that will make predictions based on data the model has never seen before. For example, a model is designed to look at photos of small four-legged animals to decide whether or not the image is a dog. This requires providing training data which is typically millions of examples of right and wrong answers. In this example, the model is shown photos labelled with whether or not the image is a dog. Over time, the model learns which images are dogs and, when presented with a new image, will identify images of dogs with a high degree of accuracy.

Unsupervised Machine Learning. These models are used in situations where the goal is to discover patterns or structures in large data sets. Unlike supervised machine learning, there is no data labeling and the models undergo no training. Data is simply presented to the model and the algorithm determines relevant patterns. Unsupervised machine learning is used to find previously unseen similarities in data (clustering) or associations between two data elements. For example, unsupervised machine learning can be used to identify unclassified IoT devices based on similarities in their IT behavior.



Supervised versus unsupervised learning.

Given this technology framework, here are the keys to effective AI/machine learning:

- **Understand the domain.** Successful data science starts with a clear understanding of the desired outcome, knowing what data is available and then selecting the model(s) that can deliver the results.
- **Deliver relevant data in large quantities.** AI models learn from a vast amount of use case-specific data—the more relevant data, the more accurate the models are.
- **Choose the right machine learning model.** Depending on desired outcomes, experienced data scientists will choose a specific model from a toolbox of available techniques and algorithms.
- **Maturity.** AI is not a "one and done" process. The accuracy of machine learning improves over time as the models encounter real-life situations and adjust their understanding of the data.

For products that lack any of these technical attributes, AI is just a marketing slogan. Questions should be asked about the types of models being used, the number of attributes being monitored, the amount of training data used and how often the models are being updated.

KNOWING THE NETWORK

The science in data science starts with data. There are thousands of potentially relevant data points that can be generated from monitoring the network – such as wireless radio frequency (RF) readings, upload/download traffic volumes, and connection performance – but only a relative few are useful for machine learning applications. For example, the information in a DNS request is relevant if it is encrypted – which is often an indication of a data exfiltration attempt. Similarly, uplink/downlink volumes are not significant for tuning network settings, but the ratio is. These insights require both deep domain and machine learning model expertise.

In the Aruba corporate wireless lab, there are thousands of access points and switches where a complete range of customer configurations are tested – a process that generates huge amounts of AI-relevant data. As a result, Aruba can combine lab data with customer data to develop a range of ML models and techniques that deliver reliable, secure autonomous networking based on a well-tuned arsenal of relevant data. Here are some examples of how these models are used.

ARUBA APPLIES AI/ML ACROSS A WIDE VARIETY OF NETWORKING AND SECURITY USE CASES

Challenge	AI Technique	Benefit
Determining root cause of performance issues	Supervised ML	Reduction in time to investigate and repair
Identifying performance issues before they cause user problems	Unsupervised ML	Proactively adjusting Wi-Fi settings ahead of user-reported issues
Optimizing RF settings	Unsupervised ML	Automated, continuous setting of optimal Wi-Fi radio configurations
Detecting insider attacks such as Ransomware	Unsupervised and Supervised ML	Find attacks that have evaded traditional defenses before they do damage
Profiling never-before-seen IoT devices.	Unsupervised ML	Secure IoT begins with device visibility

BUYER-BEWARE OF AI WASHING

Like many of the latest marketing schemes, AI is used to describe a wide range of products and technologies, many of which do not fit the definition. By industry estimates, over a thousand software vendors describe themselves as providing artificial intelligence solutions, or claim that their products involve AI. In order to understand if it really is AI and is being used properly, here some telltale signs that what is advertised may not be what it claims. This is especially true for machine learning.

- **Pre-programmed rules.** Words like "percentages", "correlation", "averages", and "thresholds" are used to describe the approach. While these techniques may have a use, they all require that both the input and the outcome are known ahead of time. True machine learning draws conclusions from data that has never been seen before, without any pre-programmed rules.
- **Training bias.** The data science term for this is "over-fitting" and it occurs when ML models are presented the wrong data or too little data to train the models. For example, if a network management model has only seen data from small offices, it will fail in larger, more complex environments. Given the diversity of mobile-centric installations, this is an especially significant issue.
- **Faux ML.** Many products claim ML-based behavioral modeling, but under the covers they simply track a few pre-determined variables and look for statistical changes (for example, 50% over the average of the last three days) to flag an anomaly. That might be anomalous; however, by relying on selected pieces of data and pre-programming the condition, other meaningful changes will be completely overlooked.

ARUBA AI IN ACTION

When the San Francisco 49ers take the field at Levi's Stadium, it's not just footballs that fly through the air. Using Aruba's Wi-Fi knowledgebase, a network that sees relatively little traffic for most of the week can instantaneously spring to life – supporting tens of thousands of fans who can simultaneously connect to the network – transferring gigabytes of data for everything from instant replays to food orders.

A global system integrator uses IntroSpect User and Behavior Analytics (UEBA) to monitor IoT devices that could compromise the network. By developing baselines of normal activity through unsupervised machine learning models, IntroSpect is able to see small changes in device behavior typical of an inside attack – and alerts the security team before it can do damage.

SUMMARY

The Aruba AI advantage starts with a deep understanding of Wi-Fi and switching technologies and a long history of data science success – commanded by a strong bench of data scientists. This is supported by insights gained from thousands of installations ranging from buildings to campuses to stadiums, across all verticals and geographies, from global deployments to small business environments.

Aruba applies machine learning to a broad range of networking and security challenges including RF optimization, network assurance, IoT visibility and advanced attack detection. By selecting the right problems to address, having access to sufficient data and knowing what data is most relevant – then curating the results in the most demanding of real-world environments – Aruba sets the standard in delivering AI-powered secure, autonomous networks.

SO_AIAdvantage_SK_030419 a00067207enw