HOW TO CHOOSE AN AI-BASED CYBERSECURITY PLATFORM

MixMode AI Guide

Today every cybersecurity vendor is touting their revolutionary machine learning or artificial intelligence. With each stating their AI is the best, someone has to be stretching the truth. Misleading marketing may cause your company to spend millions of dollars on an AI-based cybersecurity deployment that causes more problems than it solves.

This guide covers some of the common misconceptions about AI in cybersecurity and highlights red flags you should look for when buying a new AI-based platform.

MixMode™

MixMode AI Guide

Contents

"As per customer data, rules-based and supervised learning AI systems are 20x less efficient and cause security professionals to run into the same issues and many times make them even worse (e.g., alert fatigue)."

- Industry AI and Automation Analyst

Summary

What does it actually mean when a cybersecurity vendor claims their product is “AI-enhanced” or that it uses machine learning?

Most cybersecurity vendors today tout some form of “Artificial Intelligence” as an underlying mechanism for the differentiation of their product among the market. But if everyone is saying they have AI, and everyone is also claiming theirs is the “best,” how can they all be telling the truth?

Many currently available cybersecurity solutions are based upon off-the-shelf technologies, loosely cobbled together, which require as much, if not more, operator intervention than the legacy systems they are meant to replace. Those interventions do not come cheap. The overall resource cost involved with maintaining and tuning these so-called solutions can far exceed the initial installation fee.

There are several red flags organizations should keep in mind while shopping for a cybersecurity system. This list of questions can help steer you away from inadequate, expensive products and toward more capable, modern AI technology.

DARPA’s Perspective on AI

First Wave AI

Enables reasoning over narrowly defined problems.

No learning capability and poor handling of uncertainty.

Second Wave AI

Nuanced classification and prediction capabilities.

No contextual capability and minimal reasoning ability.

Third Wave AI

Contextual adaptation.

Systems constructs contextual explanatory models for classes of real world phenomena.

https://www.darpa.mil/about-us/darpa-perspective-on-ai

What Resources Does the System Require?

Consider the resource investment required to get the cybersecurity system up and running: time involved with setup, data access and storage fees, labor hours spent on training and the opportunity cost of waiting on a new system while network threats still loom large.

For example, supervised learning models rely on a lengthy data normalization process to monitor networks for anomalous behavior. Cybersecurity vendors seldom mention how much time is required to set up machine learning AI. This process involves several elements that consume a variety of resources:

- Identifying target data
- Developing the right strategy for historical data logging
- Manual intervention and data tuning
- Data labeling
- Creating rules and aggregations
- Hiring and training new systems analysts and other cybersecurity professionals

Red Flag

What does it actually mean when a cybersecurity vendor claims their product is "AI-enhanced" or that it uses machine learning?

Can the System Adapt as Your Network Evolves and Expands?

Data is dynamic. Today's anomalous behavior is tomorrow's norm. The recent shift to telecommuting in the wake of the coronavirus pandemic is an example. Machine learning cybersecurity cannot adjust to evolving network environments without significant manual retooling.

Cybersecurity platforms enhanced by self-supervised or unsupervised AI must be context-aware. When a majority of a company's workforce suddenly begins logging in from offsite locations, context-aware AI can quickly adjust to the new normal. Based on evolving information, it can change its mind about what to flag with a high level of accuracy without manual intervention.

Red Flag

The system needs manual retooling to adjust to changing network environments.

What About Recurring and Additive Costs?

Look out for AI-based Cybersecurity vendors that obfuscate financial details. Sales messaging should take into account the current state of an organization's data management and network status. It's highly unlikely that a company offering a machine learning or AI-based cybersecurity solution would be able to install and launch their platform within a few days. The process can take months or even years.

Problematic, too, are cybersecurity vendors who over-promise results based on bad data science. You are making a significant investment in data security—your vendor should be able to clearly explain the capabilities and limitations of their product and give an estimated overall cost provided in good faith.

Keep looking if the sales pitch focuses on vague, jargon-laden promises that sound complicated, and don't actually give you a clear picture of what you're paying for. Often, what you're paying for are ongoing, recurring, additive costs that keep the platform on life support, but never actually deliver on the promise of artificial intelligence.

Red Flag

The vendor does not mention expected costs beyond the sale.

How Does the System Handle Outside Events?

We can see a glaring difference in cybersecurity outcomes once AI training is complete.

When supervised AI cybersecurity encounters an event outside its trained cluster of information, it ignores the event, leaving the organization vulnerable. The rules-based environment renders the system incapable of examining data that isn't addressed by a specific rule. Supervised AI is not context-aware.

Self-supervised or unsupervised AI can provide more in-depth insight free from rules-based environments. The AI doesn't skip over attacks designed by bad actors who fully understand how these systems operate. Zero-day attacks and "low and slow" attacks happen outside the scope of machine learning AI, but self-supervised AI can intercept these attacks before they are successful.

Red Flag

The system can't handle outside events.

Is the Solution Efficient?

While all cybersecurity requires some level of oversight, your investment in a solution that utilizes AI should not result in a net loss of efficiency. Surprisingly, this is a common outcome when organizations "upgrade" to a machine learning cybersecurity platform.

Some systems require companies to hire additional staff members or to redirect security threat analysts to monotonous data tuning tasks. Legacy approaches to machine learning and AI are inherently prone to inaccuracy and require enormous investments of time, energy, and financial resources.

Even after investing the required resources, organizations have to continue feeding money into the system. These so-called AI solutions require a great deal of very expensive "babysitting".

Legacy machine learning cybersecurity is limited to the quality and quantity of currently labeled data. These systems require constant updates—an entire industry has emerged solely to support machine learning cybersecurity platforms. If the goal for an organization is to create hands-off, efficient solutions, machine learning AI models are not ideal.

Red Flag

Details about system operation and setup are overly complex or incomplete.

Is It Really Unsupervised?

If a vendor claims their cybersecurity solution is unsupervised, dig deeper. What do they mean by "unsupervised?"

An unsupervised cybersecurity solution should not require:
- Continual data tuning
- Extensive, constant data labeling
- A great deal of manual effort
- A dedicated team of analysts

Each of these requirements involves a level of intervention far outside any common-sense definition of the word "unsupervised." The industry standard is a misrepresentation on several fronts.

Truly unsupervised cybersecurity solutions are fundamentally different.

Red Flag

The company glosses over the manual interventions required to keep the system up-to-date and accurate.

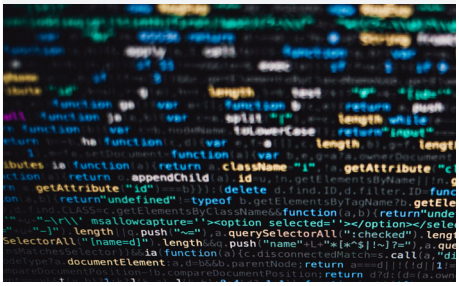
How Is the AI Trained?

Again, the issue here is that security capability correlates directly with accuracy of your data labels. Manual data labeling processes are vulnerable to human error. Manual labeling of data also inherently means that the labels are based on historical data, not real time events. Your team might miss a long-forgotten data store or accidentally misclassify data. When a machine learning cybersecurity platform launches, the AI assumes that everything it finds is clean data.

By contrast, a true self-supervised or unsupervised cybersecurity platform essentially becomes a part of the network. There's no need to clean data before the launch because you can teach the AI as it issues alerts. Context-aware AI evolves alongside the network. This is a more efficient, accurate approach.

Red Flag

Your vendor asks you to clean up your data in order to start training the AI.



Modern Security Threats Require Modern Cybersecurity Solutions

The MixMode third-wave, self-supervised AI platform operates in a fundamentally different way than most cybersecurity options available in the marketplace. Unlike typical supervised, second-wave AI products, MixMode is simple to use, requires less manual labor, and is highly effective against the ever-evolving modern threatscape. Reach out today to learn more about the MixMode solution and sign up for a demo.

MixMode™

www.mixmode.ai

+1 (858) 225-2352 | info@mixmode.ai |