BlackBerry®
Intelligent Security. Everywhere.

Evaluation Guide

5 Tips for Evaluating AI-Driven Security Solutions

What to ask security vendors when they promote their product's AI capabilities

Artificial intelligence (AI) has become a security industry buzzword so broadly applied as to become almost meaningless. Security decision makers may become cynical, even toward the most exciting innovation shaping cybersecurity today, when every product boasts AI capabilities.

It is important to understand the difference between AI and machine learning in the context of cybersecurity when evaluating AI-based technologies:

- **AI** is a broad concept of machines being able to carry out tasks in a way that humans consider intelligent.
- **Machine learning** is a more specific application of AI. It is based upon the principle that machines can perform assigned tasks intelligently if they are given access to data sets and allowed to learn for themselves. This process is often referred to as "training".

Here are five categories of questions you should ask security vendors when they promote their product's AI capabilities.

1. Why does your security product include AI capabilities?

Vendors generally add capabilities to their solutions when they discover better ways to protect systems or when responding to pressure to meet market demand. The inclusion of AI is no different, so it's important to understand the vendor's motivation behind incorporating AI into their technology.

- Why does the product use AI?
- Is AI a core component of your security product or a feature that was added to an existing product?
- What new capabilities is the AI performing?
- How does including AI improve your product over similar, non-AI offerings?

2. How does your AI benefit my organization?

It is not unheard of for vendors to add capabilities into their product for marketing reasons rather than for customer benefit. It is important to discover the true motivation for including AI by understanding how each vendor's implementation will improve your overall security.

- How will your product's AI specifically benefit my organization?
- Does your AI protect my employees without interfering with their productivity?
- Does your AI protect mobile, OEM, and IoT devices?
- How does the incorporation of AI impact the performance your product and its use of enterprise and endpoint resources?

> It is important to discover the true motivation for including AI by understanding how each vendor's implementation will improve your overall security.

3. How smart is your AI?

AI can be simple or complex. Simple AI is good at making decisions based on known information, like picking chess moves given the current state of a chessboard. It weighs existing data to determine an optimal result and can repeat this behavior through multiple iterations. It has no memory of the past and no great ability to anticipate the future.

Complex AI requires massive training data sets, a neural-net architecture, and considerable time to train appropriately. It excels at pattern matching and predictive tasks. Complex AI does not return quantitative answers (e.g. make chess move X), but instead returns qualitative answers (e.g. 89% chance this object is the same as other objects).

It's important to understand what type of AI the security vendor is using so that you have the right expectations of results. Likewise, the effectiveness of AI is improved by the duration and depth of its training. This makes an AI trained for a decade on a large dataset more effective than newer AI trained on the same data set for a shorter period.

- Is your solution using simple or complex AI?
- How is your AI trained?
- How experienced are your AI models in both test and real-world environments?
- Is your AI capable of working within a Zero Trust architecture or addressing threats in the MITRE ATT&CK framework?
- Can your AI detect changes in the environment and user behavior, and adjust access and permissions accordingly?

Complex AI requires massive training data sets, a neural-net architecture, and considerable time to train appropriately. It excels at pattern matching and predictive tasks.

4. How is the AI maintained?

The maintenance required to keep AI well-trained and relevant depends on how the AI is being used. For instance, if the vendor is using AI to automate signature creation for new threats, the AI is typically maintained by the vendor. This may not actually benefit the organization as it may result in more vendor updates to the endpoints. Alternatively, if the AI is trained in the cloud and then deployed to the endpoints, an organization can benefit from consistent prevention with minimal maintenance.

- Where does your AI reside? Is the AI running in your cloud or running locally on the endpoint?
- How is the AI specifically used? Is the AI used to automate signature creation? Is the AI used to make real-time decisions on threats?
- How much maintenance, including employee training and active attention, does your AI solution require?
- How often is the AI retrained?

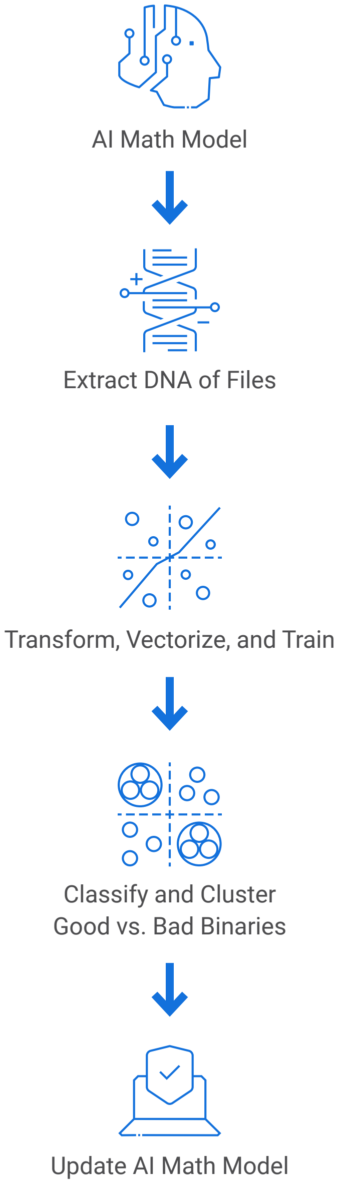
5. Can you provide a demonstration in our environment?

The true test of any security solution should be how well it performs for your organization. Any company selling a security product should be happy to demonstrate its performance within your infrastructure. Be wary of companies who only offer internal test results and bold assurances. The levels of aggressiveness used in testing environments can vary greatly from the needs of real-world enterprises, leaving the end-user to make adjustments. This means internal test results on endpoint protection may represent mathematical models with incomplete training.

- Does the AI provide levels of aggressiveness?
- What cloud dependencies does the AI rely upon to be effective? Can the AI be as effective offline as it can be online?
- Can the AI prevent zero-day malware on the endpoint without connectivity to the cloud?
- Can the AI prevent malware that its training set has never encountered?
- Has the AI been tested by a third party that confirms its ability to detect and/or prevent malware that did not exist when the AI model was trained?

Visit BlackBerry®Spark Suites to learn more about AI-enabled security across all endpoints.

Training an AI/ML Model


AI Math Model
Extract DNA of Files
Transform, Vectorize, and Train
Classify and Cluster Good vs. Bad Binaries
Update AI Math Model

About BlackBerry

BlackBerry (NYSE: BB; TSX: BB) provides intelligent security software and services to enterprises and governments around the world. The company secures more than 500M endpoints including 175M cars on the road today. Based in Waterloo, Ontario, the company leverages AI and machine learning to deliver innovative solutions in the areas of cybersecurity, safety and data privacy solutions, and is a leader in the areas of endpoint security management, encryption, and embedded systems. BlackBerry's vision is clear — to secure a connected future you can trust.

For more information, visit BlackBerry.com and follow @BlackBerry.

BlackBerry®
Intelligent Security. Everywhere.

©2020 BlackBerry Limited Trademarks, including but not limited to BLACKBERRY and EMBLEM Design are the trademarks or registered trademarks of BlackBerry Limited, and the exclusive rights to such trademarks are expressly reserved. All other trademarks are the property of their respective owners. BlackBerry is not responsible for any third-party products or services.