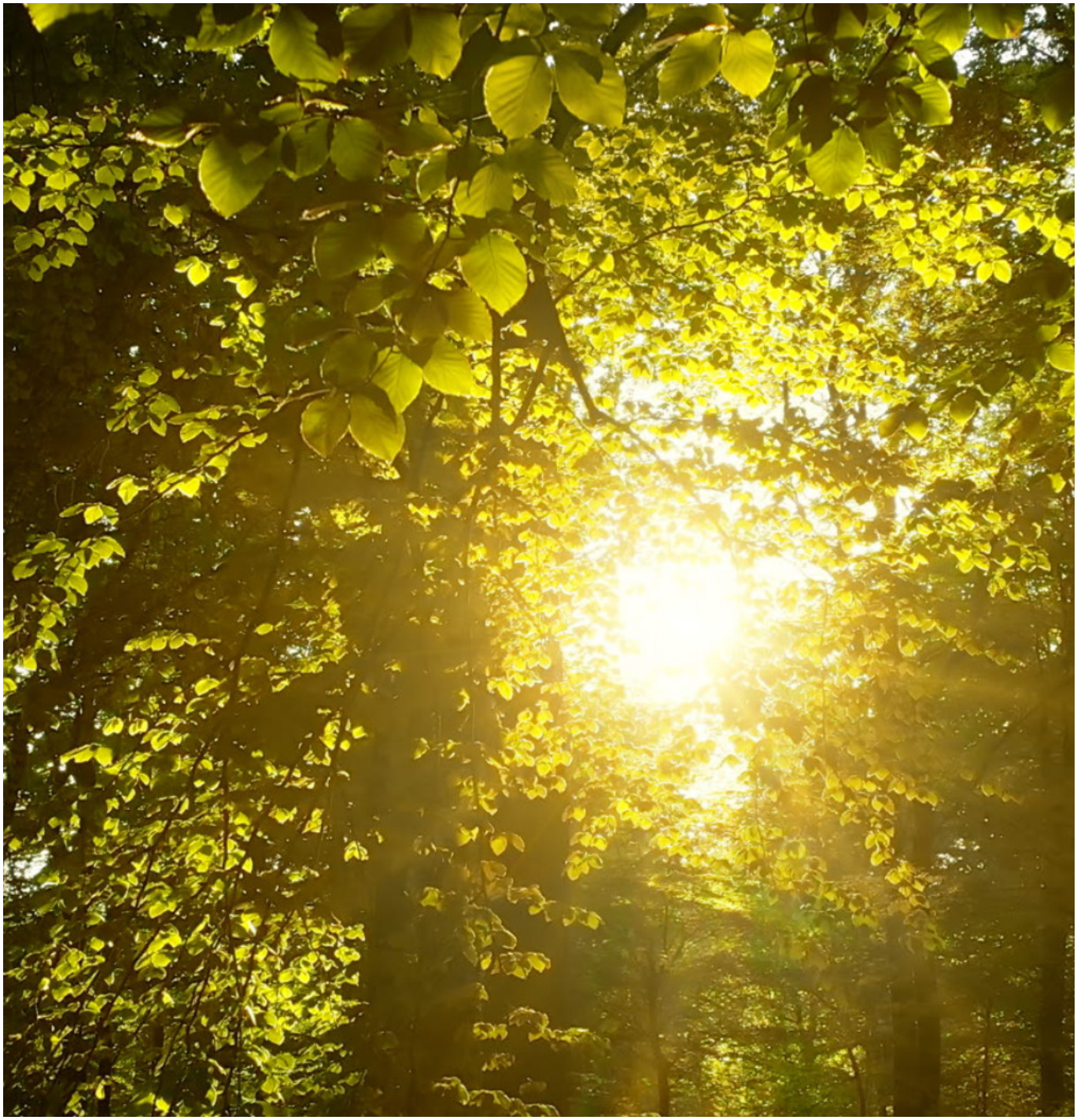
EVIDEN

Digital Security Magazine - 12th edition
November 2023

Artificial intelligence and machine learning: The future of cybersecurity

By Dwayne Natwick



Generative AI, ChatGPT, Bedrock, and the list goes on...

Over the past months, it seems that everyone is speaking about Artificial Intelligence (AI) and Machine Learning (ML). But what really is it? What can it do? What are the dangers? How can it be used for good? In this article, you will find possible answers to these questions and hopefully some helpful ways that AI/ML can benefit you.

What is AI and ML?

In many cases, AI and ML are used synonymously. The truth is that although they tend to work together in many ways, they are two different uses and technologies. AI is the aspect that a device or software could replicate a human capability. This could be accomplished through information that is gathered through data collected, such as known languages. An example of AI software would be text to speech translation. Within technology, AI can be used to complete data analysis or recognize a threat on a device and shut that device down.

Machine learning, ML, is considered a subset of AI. ML has the capability to replicate human tasks through training algorithms on data at a much faster rate than possible by humans. ML is trained with data to understand typical versus non-typical activity. The information and knowledge that ML gains can then be used to initiate other AI interactions and provide analysis of data.

What can it do?

As stated in the previous section, AI can replicate human activities through robotics and language translation. Personal assistants, such as Amazon Echo, has AI software built in to interact with you to perform an activity, like turning on lights or providing the weather forecast. You probably interact with something utilizing AI daily, including a customer service chat bot.

ML models can be trained to support decision making through mathematical data analytics. The ability of ML and the high-performance computers that are utilized, can evaluate peta-bytes of data and find the data that is seen to be an outlier from the primary datasets.

What are the dangers?

There are multiple concerns and dangers when using AI and ML. One of the primary concerns are those that relate to ethical use. As more consumer uses are applied to AI, you must be able to draw the line between how this information is used. For example, having ChatGPT write your school or work assignment crosses that line. Using information that has been heard by your phone or personal assistant to market products to you is another potential ethical breach of privacy, especially if you were not asking for this information directly.

In the world of IT and security, attackers use AI and ML in multiple ways to gain information, identify vulnerabilities, and perform attacks. These include the following:

- **Distributed Denial of Service (DDoS) attacks.** This type of attack succeeds in blocking users from accessing resources through flooding the Internet service provider with request information that is not valid. Systems are unable to respond to the volume of requests and this blocks legitimate users from having access. To have the ability to create the volume of requests, systems must have bots running to make these requests. In some cases, attackers take over control of other systems to run these bots and create the disturbance.

- **IoT botnet attacks.** Like DDoS, AI bots are used to take over IoT devices. IoT devices have access to and gather a large volume of data about performance of these devices and the systems that are interacting with the devices. The AI bots taking control of these devices can steal the data and provide it to the attacker, or they could manipulate that data to provide false information.

- **Social engineering.** You learned in what can AI and ML do section that ML can be used in identify deviations from common behavior. In contrast, certain attacks using AI and ML, such as site redirects or man-in-the-middle can gather information that can help an attacker gain access to systems.

- **Vulnerability identification.** Like social engineering attacks, AI and ML tools can be used to look at systems and networks for vulnerabilities. AI bots can scan thousands of network IP addresses and ports at one time. Since public IP schemas are all know patterns, these patterns can be programmed into AI to scan for vulnerabilities, including open ports that can provide access. Most commonly these are ports 3389 and 22 for remote access.

- **Brute force dictionary attacks.** AI bots can be used to send thousands of requests to systems using common usernames and passwords to gain system access. This takes advantage of the vulnerabilities found on ports 3389 and 22.

- Malware and viruses have been around about as long as Windows operating systems. Malware is mutating software that causes damage to an operating system and can also be used to gather sensitive information on that system. ML allows this software to work smarter and mutate to avoid system protections that are in place.

- **Data manipulation.** In addition to using AI and ML to gather information and perform theft on systems, an attacker may also use these tools to manipulate data that damages systems and could do reputational and financial harm to a company. One form of this data manipulation is ransomware.

As you can see, AI and ML is being used throughout these examples to increase the efficiency and effectiveness of an attack. AI and ML has positive uses as well, let's look at these now.

How can it be used for good?

As stated in the challenges and concerns, AI and ML can have some negative and potential ethical uses. However, there are many good uses for these tools. ML has been used in the healthcare field to accelerate understanding of new diseases to bring vaccines to the market faster. It has also been used to identify indicators that someone could develop diseases such as diabetes and heart disease.

It also can be used to support Security and Governance within IT and data protection. Some of these capabilities are:

- **Analyze mobile endpoints.** AI and ML tools can analyze the locations of endpoints and perform hardening on these endpoints that include geo-tracking to protect and block access to sensitive information in certain situations, or conditions.
- **Detect malicious activity and stop attacks.** ML algorithms are built within managed detection and response solutions to hunt for malicious activity on systems and identify activity proactively that could be the early stages of an attack. AI can then be triggered to automate the response to this information.
- **Human behavior analysis.** ML algorithms can be run against user behavior and activities. The information gathered will look for activity that is non-typical and can trigger AI activities that could block access to certain resources or data until this is cleared.
- **Detect and close zero-day vulnerabilities.** As stated previously, attackers are always looking for vulnerabilities on systems and networks. Most notably, are vulnerabilities caused by firmware and software updates. This is where mutating malware can take advantage of a system. AI and ML within endpoint protection can be proactive in identifying these vulnerabilities and taking proper countermeasures to protect against this from becoming an incident.
- **Automate repetitive tasks for remediation and recovery.** When responding to a threat, human interaction may not always be the most effective. Attacks may be carried out when operations are closed. AI can be used to automate security patching, malware scans, and even shutting down compromised systems to minimize an incident.

AI and ML can be used to counteract some of the challenges and concerns that AI and ML are used for in attacks. However, AI and ML cannot replace a good planning and education program. Human social engineering, email phishing and spear-phishing, and identity man-in-the-middle attacks can still be carried out by attackers without AI and ML even knowing.

The capabilities of AI and ML for security operations only keep getting stronger. The ability to utilized AI and ML within the cloud at a much larger scale creates possibilities to protect, monitor, manage, and control the protection of identities, data, and endpoints. If you continue to make users aware of the potential dangers and ethical concerns with AI and ML, while embracing the evolving security uses of the technology, the future looks bright for security operations.