Using advanced AI to stay ahead of cyber criminals

By Doros Hadjizenonos

22 Mar 2019

Staying ahead of today's accelerated cybercrime trends requires adding artificial intelligence (AI) to an organisation's network security strategy

Doros Hadjizenonos, Regional Director – SADC at Fortinet

As the threat landscape continues to evolve rapidly, it now includes increasingly sophisticated, zero-day malware that traditional security approaches can no longer keep pace with. As a result, security researchers estimate that the cost of cybercrime will outpace security spend by over 16X, reaching $2.1trn by the end of 2019. Staying ahead of today's accelerated cybercrime trends requires adding artificial intelligence (AI) to an organisation's network security strategy.

The rise of artificial intelligence

The goal of AI is to replicate the analytical processes of human intelligence but to enable decision making at machine speeds. The most effective AI uses a deep-learning model built around an artificial neural network (ANN). This network is comprised of hardware and software configured after the neuron patterns in the human brain. This design not only accelerates data analysis and decision making but also enables the network to adapt and evolve based on new information.

To accomplish this, an ANN goes through a machine learning (ML) training process where implanted learning models are

carefully fed vast and increasingly complex amounts of information on an ongoing basis. Once the system has identified patterns and problem-solving strategies, it is then provided with new information that enables it to adjust its algorithms so that it can adapt to and identify new tactics and capabilities adopted by malware or an attack vector.

Fortinet and AI

As an early adopter of AI, Fortinet began developing a self-evolving threat detection system over six years ago. This system leverages a custom-designed ANN comprised of billions of nodes, and we have been meticulously training it with new threat data every day since, giving us a significant competitive threat intelligence advantage over every other vendor in the security marketplace.

Our FortiGuard Labs team now uses this advanced AI technology to analyse files and URLs and label them as clean or malicious—at machine speeds and with a high degree of accuracy.

Training an AI

The most crucial element of any AI solution is the methodology used to train its analysis and decision-making algorithms.

The ML model used to train FortiGuard AI leverages the three essential learning model strategies endorsed by the AI community:

- ### Supervised learning

  This initial model begins the training of the AI by feeding it a vast amount of labelled data, clearly identifying the characteristics of each labelled data set, and then repeatedly applying those characteristics to unlabelled data.

- ### Unsupervised learning

  In this next phase, the algorithm has no known solution set to follow. Instead, it recognises patterns learned in phase one that enable it to label data without human help. At this point, new data can be slowly introduced to force it to deal with data it hasn't seen before and make new decisions.

- ### Reinforcement learning

  The results of supervised and unsupervised learning are then “tested,” by scoring the system’s performance with unlabelled files and “rewarding” the system for good results. Training then continues to cycle between these three learning strategies on an ongoing basis.

Because of the recursive requirements of machine learning, any AI system that does not use all three of these learning models is incomplete. Each learning model helps refine results and improve accuracy.

Delivering true AI to customers

Many cybersecurity companies claim to have introduced AI capabilities into their solutions. But the reality is, most fall short of true AI because their underlying infrastructure is too small or their learning models are incomplete. Others refuse to divulge the methods that they use, which raises concerns about the reliability of their AI. Fortinet instead opts to be more transparent about its methodology so that customers know the breadth and depth of the analysis involved.

Sharing intelligence across the Security Fabric

Intelligence in isolation is useless. The more it is shared, the more effective your defensive systems can become. This is why every time a threat is identified, FortiGuard AI generates threat intelligence that automatically updates defensive signatures for every solution across the entire Fortinet Security Fabric, enabling security tools to work together to defend customers with advanced threat detection and protection solutions.

And because AI powers it, all of this happens seamlessly and behind the scenes—requiring no staff time from an organisation’s security analysts. This allows the Fortinet Security Fabric to integrate, collaborate, and automate threat detection, prevention, and remediation capabilities through sandboxing by sharing threat intelligence across each security element in real time.

Because Fortinet covers the network from end to end, we have a unique and comprehensive view that includes every component needed to protect an organisation's ecosystem - from the data centre to multiple clouds. This approach, unique in the industry, improves operational efficiencies while dramatically mitigating risks. And because FortiGuard AI threat detection is incorporated into the Security Fabric’s centralised visibility and controls, it also enables the network security team to work proactively based on the most accurate and timely information possible.

ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet
- Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- How to have strong cyber hygiene - 26 May 2020
- How to approach data breaches - 11 May 2020
- Employees must be educated about mobile cyber threats - 13 Feb 2020
- Stay ahead of emerging cyber threats - 8 Jul 2019

View my profile and articles...