FORTINET

Using AI to Address Advanced Threats That Last-Generation Network Security Cannot

Executive Overview

In a world of digital transformation (DX), security teams face increased complexity and an expanded attack surface, threatening both security and network performance. Artificial intelligence (AI) can help in both of these areas by automating and speeding up threat detection and remediation. This is essential given the current landscape, as cyber criminals are using AI to create the next generation of threats. But it also enables CISOs and other security leaders to deploy security analysts to more strategic initiatives.

For network security, AI and machine learning (ML) power self-evolving detection systems (SEDS) that keep up with the evolving nature of threats and identify zero-day attacks by their characteristics. ML uses three learning principles to "train" their models: supervised, unsupervised, and reinforcement learning. Using a large amount of data and all three ML training models results in the highest degree of accuracy for SEDS. Those seeking a SEDS solution should consider the amount of data ingested, the use of all three learning models using artificial neural networks (ANNs), and the ability to integrate AI into a comprehensive security architecture that enables centralized visibility, true automation, and real-time intelligence sharing.

"If you know your attacker and can respond quickly, 'the chances you will be hitting back your true adversary are higher if you can react in real time'."[1]

Table of Contents

01 DX Complicates Network Security

DX initiatives are helping companies realize cost efficiencies, exploit new revenue opportunities, and keep one step ahead of the competition. As a result, IT network architecture is evolving at a breakneck pace. This results in business-critical data and applications residing in multiple clouds, internal traffic bypassing the data center via software-defined wide-area network (SD-WAN) technology, and Internet-of-Things (IoT) devices proliferating in virtually every corporate function.[2]

This complexity extends to network security. A growing attack surface and increasingly complex advanced threats mean that the security controls built into "last-generation" networks are unable to address the volume, velocity, and sophistication of the threat landscape.[3] Traditional, signature-based antivirus can no longer keep up, as real-time detection and response is now essential.

Because of these factors, the result of DX is all too often an overwhelmed network security team that is reactive rather than proactive. This presents risk to the organization of downtime or data loss caused by advanced threats that were not caught in time. But it does not need to be that way.

Each day, 28% to 40% of all new malware tracked by FortiGuard Labs is zero day.[4]

02 AI Detects Zero-Day Threats at Machine Speed

AI is reaching a tipping point where ever-increasing CPU power allows machines to perform a wider variety of tasks faster and more accurately than humans. This is evidenced by the rapid growth in investment in AI technology—almost a sixfold increase from 2016 to 2020, according to IDC research.[5]

On the security front, AI is now being deployed in the fight against cyber criminals. Using ML to analyze the characteristics of malicious files, AI provides the fastest detection of advanced threats—including increasingly common zero-day attacks.[6] Automation based on AI-derived intelligence, from automatic signature creation to real-time quarantining and remediation, represents the future of network security.[7]

Unfortunately, cyber criminals are already using AI to build next-generation polymorphic malware that will spontaneously create entirely new, customized attacks.[8] This makes AI a doubly important tool for threat protection.

According to Constellation Research, AI is emerging as the predominant area of technological experimentation.[9]

03 AI Optimizes Network Security Resources

For network security leaders, AI also offers the promise of getting the most out of existing staff while enabling the network operations team to meet or exceed network performance and security benchmarks. Limited budgets, competing priorities, and the current shortage of cybersecurity professionals—projected to reach 3.5 million by 2021—means that hiring more talent may be impossible even if the budget were available.[10]

Unlimited headcount would not solve the problem anyway, as threats are now causing damage at machine speed—faster than an army of humans could remediate.[11] According to FortiGuard Labs, between 28% and 40% of new malware tracked on a given day is previously unknown or zero day.[12]

Using AI to automate detection processes enables management to concentrate an organization's most high-value cybersecurity resources on more strategic tasks. When coupled with an integrated security architecture with centralized visibility and automation of other security processes, the organization assumes a proactive stance, enabling network security staff to plan for future threats rather than responding to past ones.

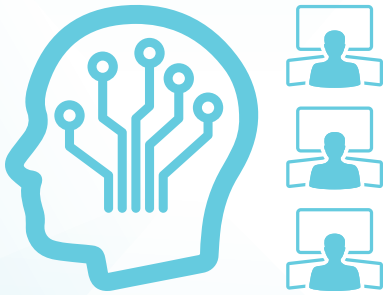
"The idea that the massive security issues facing businesses today can be resolved by putting more people on the job is naïve."[13]

04 How AI Helps Improve Network Security

AI represents the final step in evolving toward real-time detection of known and unknown threats—moving beyond virus signatures and pattern recognition to build SEDS. Providing actionable intelligence for SEDS involves three components:

- **AI:** The capability of a machine to imitate intelligent human thought processes.
- **ML:** Using data to refine how computers make predictions or perform a task, learning to make decisions on its own and respond to new situations.
- **Deep Learning:** An ML technique in which data is filtered through self-adjusting networks loosely inspired by neurons in the human brain.

Since SEDS are continually trained using ML—and in some cases deep learning—the accuracy of their threat detection improves over time. The training process can adjust the weighting of each feature as threats evolve, while adding new features as they are detected.[14] The more data that is fed into the system, the more accurate it gets.



“Teams that are using [AI] to augment their existing analysts … are more effective than their peers and even SOC teams with more than 10 members who are not using AI.”[15]

05 How Machines Learn to Detect Malware

It takes a lot of capacity and data for SEDS to work properly. Large ANNs—systems of hardware and/or software patterned after the operation of neurons in the human brain—are required to collect, analyze, and classify millions of threats every day. "Training" of AI algorithms involves three different types of learning:[16]

1. **Supervised Learning:** Presenting the system with correctly labeled data, which it analyzes and applies to unlabeled data.

2. **Unsupervised Learning:** Providing unknown solution sets, which the system analyzes for patterns from which it can ultimately label the data.

3. **Reinforcement Learning:** Optimizing the system's performance by testing it with unlabeled data and offering grades (rewards) for the results.

This comprehensive training over a period of time results in billions of examples that are subjected to extensive analysis for features and behaviors that suggest whether a file is clean or malicious. The result is instantaneous decisions that reflect a high degree of accuracy—enabling remediation in real time.

"Attempting to label data [manually] would be extremely time-intensive ... it is often much easier to simply have the machine separate data into groups for us."[17]

06 Tips for Choosing an AI-Powered Network Security Solution

A number of security vendors already use different elements of AI as a part of their offerings, but many of them are vague about just how comprehensive their AI efforts are. Here are some things to look for in a solution:

1. **True SEDS.** Does the vendor use a true SEDS that adapts its analysis to real-time changes in the characteristics of threats?

2. **Size of Intelligence Store.** How big is the vendor's Threat Intelligence data store, and how long has it been training the model? The more data and the longer the training history, the more effective the result will be.

3. **Using All Three ML Learning Modes.** Is the vendor training its algorithms using all three learning methods—supervised, unsupervised, and reinforcement learning?

4. **ANN Capabilities.** Does the vendor use ANNs to analyze incoming files? How many processing nodes does the vendor's ANN have? How many security sensors? These capabilities will be crucial as the threat landscape expands.

5. **Packaging and Wrappers.** Does the solution look beyond the files themselves and perform deep inspection of packaging and wrappers used to encrypt malicious code and deliver it into IT environments?

6. **Architectural Integration.** Is the vendor's offering a part of an integrated security architecture that provides transparent visibility and centralized control across the entire network, with real-time threat-intelligence sharing across the organization? Adding another silo to your security infrastructure is not productive.

“Make no mistake: The future of cybersecurity is about embracing and innovating for the partnership of man and machine—both relying on each other in the fight against hackers.”[18]

07 Conclusion

Clearly, AI must be a part of any enterprise's network security strategy today. Cyber criminals are using AI to make their malware less detectable, faster, and more destructive. Only AI can detect zero-day threats based on behavior and other characteristics. Automation enabled by AI also helps make your network security team more effective by enabling them to focus on proactive threat prevention rather than reactive remediation.

As with all aspects of security operations, a strategic approach is best when designing a solution. A comprehensive integrated solution is far preferable to adding another silo to the network security architecture to check off a box. The latter keeps the team in reactive mode; the former enables the team to truly become proactive and strategic in its approach.

Early AI Adoption at Fortinet

Fortinet began using AI beginning in 2012 after years of preparation. Since then, AI and ML have become integral to virtually all of Fortinet's products and services—and to the Security Fabric approach that unifies them into a broad and integrated platform. It drives security functions ranging from malware detection and analysis to end-user behavior analytics and web traffic filtering.

[1] David Strom, "Understanding the Relationship Between AI and Cybersecurity," SecurityIntelligence, March 22, 2018.

[2] Benson Chan, "The evolving role of IT managers in a hyper-converged digital world," Strategy of Things, September 7, 2017.

[3] "2018 Security Implications of Digital Transformation Report," Fortinet, July 26, 2018.

[4] Based on internal data from FortiGuard Labs.

[5] Margaret de Silva, "2017 was just the tipping point for AI," Vision Critical, April 14, 2019.

[6] Rick M. Robinson, "Zero-Day Malware Poses a Growing Threat," SecurityIntelligence, May 1, 2017.

[7] Zeljka Zorz, "AI is key to speeding up threat detection and response," Help Net Security, August 14, 2017.

[8] Derek Manky, "The Evolving Threat Landscape—Swarmbots, Hivenets, Automation in Malware," CSO, August 29, 2018; Kevin Townsend, "The Malicious Use of Artificial Intelligence in Cybersecurity," SecurityWeek, March 28, 2018.

[9] Courtney Sato, "AI and Internet of Things will drive digital transformation through 2020," ZDNet, October 25, 2017.

[10] Ryan Kh, "How AI is the Future of Cybersecurity," Infosecurity, December 1, 2017.

[11] Laurent Gil, "The Debate is Over: Artificial Intelligence is the Future for Cybersecurity," SC Magazine, March 22, 2018.

[12] Based on internal data from FortiGuard Labs.

[13] Laurent Gil, "The Debate is Over: Artificial Intelligence is the Future for Cybersecurity," SC Magazine, March 22, 2018.

[14] Nick Ismail, "How artificial intelligence can stop the malware threats of the future," Information Age, November 14, 2017.

[15] Zeljka Zorz, "AI is key to speeding up threat detection and response," Help Net Security, August 14, 2017.

[16] "Machine Learning 101: Supervised, Unsupervised, Reinforcement & Beyond," Towards Data Science, August 28, 2017.

[17] Eliezer Kanal, "Machine Learning in Cybersecurity," SEI Blog, Carnegie Mellon University, June 5, 2017.

[18] Laurent Gil, "The Debate is Over: Artificial Intelligence is the Future for Cybersecurity," SC Magazine, March 22, 2018.

FORTINET

www.fortinet.com

429866-0-0-EN

June 8, 2019 2:32 PM

eb-ai-advanced-threats