SOLUTION BRIEF

FortiNDR

Helping Overwhelmed Security Operations Teams to Move from Reactive to Proactive

Executive Summary

Relentless growth in the volume, velocity, and sophistication of threats is overwhelming the security operations teams at organizations in every industry. Fortunately, security architects trying to relieve their burdens have a new tool available—next-generation artificial intelligence (AI). An early leader in the use of AI in cybersecurity, Fortinet addresses these challenges with FortiNDR. FortiNDR brings the latest AI-driven breach protection technology on site to analyze incoming threats in less than a second. This gives security teams the opportunity to stop hackers and malware before they penetrate their networks.

61% of enterprises say they cannot detect breach attempts today without the use of AI technologies.[1]

The advanced threat landscape is straining beleaguered security operations teams almost to the breaking point—with no relief in sight. Rapid increases in the volume, velocity, and sophistication of threats have security architects scrambling to find solutions. The sheer number of alerts means a significant number of them are ignored because of a lack of bandwidth. And help in the form of new team members is not forthcoming at many organizations. If anything, the cybersecurity skills shortage is getting even worse.[2]

Not only that, when investigated, cybercriminal activity is difficult to discern from legitimate operations. As the MITRE Center for Informed Threat Defense notes, the most common techniques "abuse legitimate system tools... underscoring the idea that adversaries are attempting to appear as legitimate users."[3]

The Evolution of AI in Cybersecurity

Cybersecurity firms have been using machine learning (ML) in the fight against cybercriminals for several years—most notably in the area of threat detection. Training algorithms use ML to enable increasingly accurate identification of the characteristics of malicious files, and the result is real-time detection of advanced threats, including zero-day attacks.[4] This evolution of security technology is a requisite for organizations today. For example, a recent study finds that more than 60% of organizations would be unable to detect critical threats without it.[5]

But better threat detection alone does little to make security operations teams feel less overwhelmed. If anything, better detection means an even higher volume of alerts that must be addressed manually. Rather, *more* automation is also needed—especially in the area of threat response and security strategy. Fortunately, an emerging next generation of AI promises to relieve the stress on security operations team members while making them more productive overall.

Next-generation AI: Deep Neural Networks

To describe the potential of next-generation AI for cybersecurity, it is helpful to define terms precisely (Figure 1):

- **AI** is a blanket term that refers to the capacity of a machine to imitate intelligent human behavior.
- **ML** is one component of AI and uses data to solve linear problems such as making predictions or performing tasks. Artificial neural networks (ANNs) are one common ML method. ANNs use hardware and software to build a configuration that is patterned after the operation of neurons in the human brain through ML training. Models are fed vast amounts of information on an ongoing basis, and the system analyzes that information and adjusts algorithms based on new tactics and capabilities adopted by malware or an attack vector.
- **Deep neural networks** (DNNs), sometimes known as deep learning, is another ML technique that uses multiple ANNs—with two or more layers between the input and output layers—to model complex, non-linear relationships.

An example can help illustrate the difference between standard ML and DNNs. Standard ML could be used to teach a computer the English alphabet and how letters are placed together to form words. Then, it could provide a dictionary of English words with definitions and images. Using ML, words found in datasets can be identified, such as *bee*, *pollinate*, *flower*, *field*, and *day*. DNNs, on the other hand, can train a computer to describe a new photograph of a bee pollinating a flower in a field during the day, based on images of each of those characteristics presented in the past.

The levels of understanding and analysis made possible by DNNs provide an opportunity to take AI to the next level when it comes to cybersecurity. When AI is used for threat detection only, it can potentially add to the security operations team's stress, as it only adds to the overwhelming volume of alerts that they already receive. It also increases the odds that a specific threat does not receive a timely response.

On the other hand, if AI can be used to make intelligent decisions about threat response—and even provide actionable insights about security strategy—it can begin to provide relief for beleaguered security operations professionals. Staff members can remain focused on security strategy while most threat response is handled on a real-time, automated basis by a virtual security analyst.

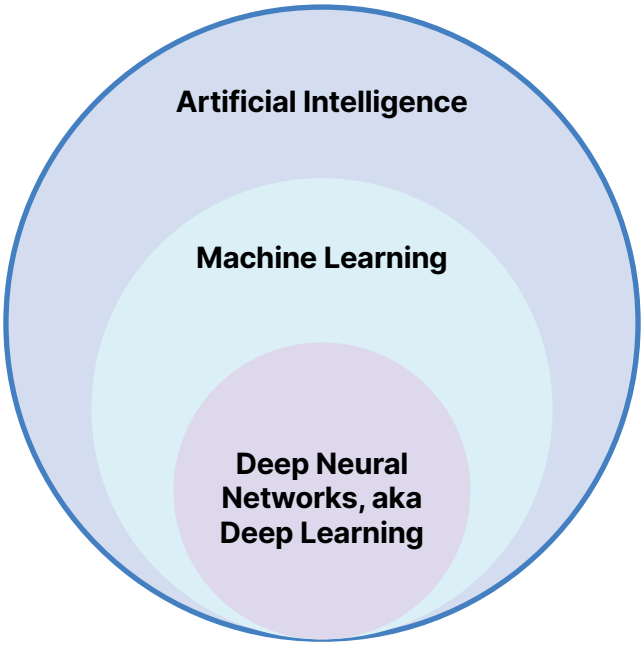

Figure 1: The relationship between AI, ML, and DNNs.

Building Upon Ten Years of AI

Fortinet was an early adopter of AI for threat detection, rolling out a self-evolving detection system (SEDS) based on ANNs in 2016 after four years of prelaunch operational training. The SEDS analyzes millions of objects a day and validates which ones are malicious. It then feeds that information into the products of the Fortinet Security Fabric.

This SEDS managed by FortiGuard Labs has now been trained for a total of 10 years using both supervised and unsupervised ML. The result is extremely accurate, real-time detection of unknown and polymorphic threats based on their characteristics—with almost zero false positives. Since then, Fortinet has added in-line web traffic application analysis to the FortiWeb web application firewall (WAF), introduced AI-powered analysis to FortiSandbox, and included AI-based user and entity behavior analytics (UEBA) through FortiInsight and AI-powered advanced endpoint security with FortiEDR.

"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'."[6]

FortiNDR Virtual Security Analyst: Next-generation AI On-premises

A few years ago, Fortinet was the first to offer an on-premises virtual security analyst based on DNN technology. Like a human security analyst, it adapts to new attacks and gains experience over time. But unlike a human analyst, it does so at machine speed. It uses DNNs to automate incident investigations and create tailored threat intelligence to disrupt targeted attacks at machine speed.

With the FortiNDR AI-capable, unsupervised learning model, the virtual security analyst identifies and analyzes threats with ever-increasing speed and accuracy, augmenting human security staff and enabling their work to be more productive.

Using AI to Learn About Specific Organizations

To accelerate threat intelligence to machine speed and keep pace with the advanced threat landscape, FortiNDR learns and adapts to new attacks on a specific organization over time, continually improving and optimizing the threat protection life cycle. The result is FortiNDR supports security operations staff by identifying and analyzing network anomalies in fileless and file-based malware and identifies compromised systems across the organization with 100% certainty—all in less than a second.

To do so, FortiNDR uses AI technology to make the decisions that a security analyst would make when manually investigating attacks, including:

- **Detecting network anomalies** by processing large amounts of north-south, east-west traffic at the perimeter and in the data center, using ML to profile traffic and detect anomalies and attacks such has encrypted attacks, malicious web campaigns, botnet-based attacks, intrusions, and more. FortiNDR finds the needle in the haystack in terms of malicous activities on your network.
- **Investigation and classification of the attack** by tracking the original source of the infection with a time stamp and providing full visibility of the lateral spread from patient zero to all subsequent compromised systems.
- **Malware analysis** determines the type of malware by features observed by the FortiNDR DNN and provides an event timeline for each infection event. This is akin to a miniature kill-chain model that describes in scientific terms what the threat tried to do in a step-by-step fashion, including technique employed. For example, at “time zero” a download of an HTML file occurred; at “time one” a malicious code exploit took place in a browser; at “time two” a trojan downloaded to a user or temp directory. Here, FortiNDR comes prebuilt with over six million malware features and learns additional ones over time.

As FortiNDR performs these layers of analysis, its full integration with the FortiGate Next-Generation Firewall (NGFW) enables the threats that it identifies to be blocked. Security operations staff can then apply the intelligence to security controls across the network and other elements of the Fortinet Security Fabric.

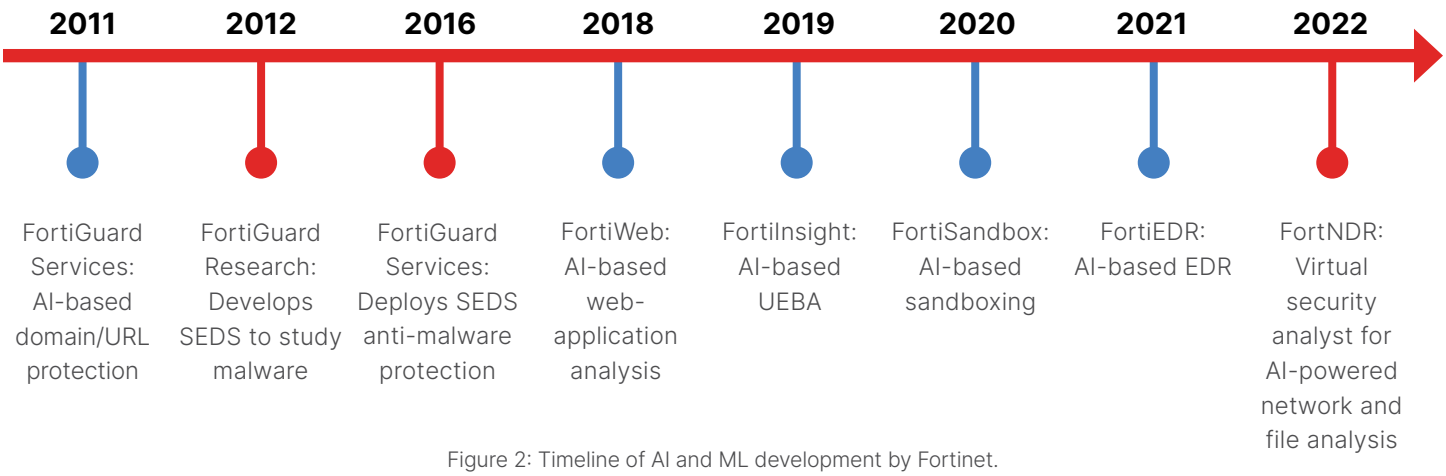

Figure 2: Timeline of AI and ML development by Fortinet.

Benefits of FortiNDR for Cybersecurity Teams

For today's overwhelmed security professionals, FortiNDR can help security operations teams move from a reactive to a proactive security posture, while increasing their operational efficiency. It delivers key benefits that include:

1. **Faster mitigation of attacks.** Real-time, automated investigation of every security incident enables faster response to automated threats that move at machine speed. Since the impact of an intrusion increases as time passes, real-time response is the best way to minimize damage.
2. **Reduced time window for exposure to threats.** With analysis applied in real time, organizations are less vulnerable while waiting for a vendor's application patch or anti-malware signature. Instead, after being alerted in less than a second, the security operations team can block malware in a process that could be termed "virtual patching."
3. **Improved productivity by the virtual elimination of false positives.** Organizations no longer need to apply generic threat feeds to security controls—and manually investigate every false positive.[8]

"The battleground of the future is digital, and AI is the undisputed weapon of choice."[7]

[1] "Reinventing Cybersecurity with Artificial Intelligence: A new frontier in digital security," Capgemini, accessed January 27, 2020.

[2] Sandra Wheatley Smerdon, Cybersecurity training can close skills gap for a safer digital world, World Economic Forum, May 2021.

[3] "MITRE Engenuity CTID. Sightings Ecosystem: A Data-Driven Analysis of ATT&CK in the Wild," 2021.

[4] "Using AI to Address Advanced Threats That Last-Generation Network Security Cannot," Fortinet, June 8, 2019.

[5] "Reinventing Cybersecurity with Artificial Intelligence: A new frontier in digital security," Capgemini, accessed January 27, 2020.

[6] David Strom, "Understanding the Relationship Between AI and Cybersecurity," Security Intelligence, March 22, 2018.

[7] William Dixon and Nicole Eagan, "3 ways AI will change the nature of cyber attacks," World Economic Forum, June 19, 2019.

[8] Chris McDaniels, "Is Threat Intelligence Garbage?" Dark Reading, March 23, 2018.

FORTINET

www.fortinet.com

April 6, 2022 5:25 AM
594577-A-0-EN