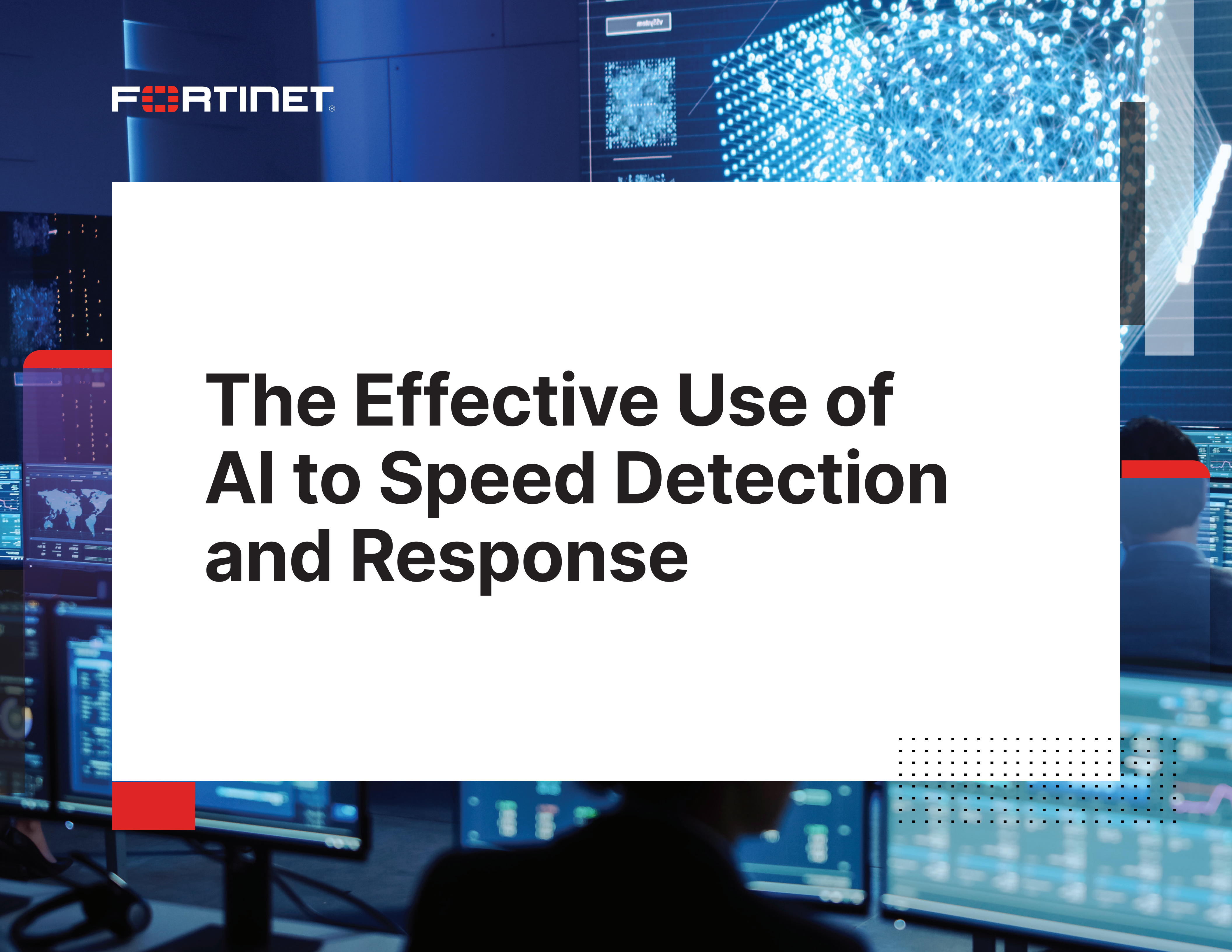

The Effective Use of AI to Speed Detection and Response

Table of Contents

Executive Summary

In many ways, cybersecurity is becoming a big data problem, given the volume and sophistication of cybercampaigns. Fortunately, the application of artificial intelligence (AI) for cyberattack detection is a rapidly expanding and maturing field. Whether it is applied to analyze code (in delivery or at installation), model behavior (on the device or throughout the network), or to thwart ransomware specifically or cybercrime in general, AI is proving its value to detect security incidents in progress all along the cyber kill chain. However, organizations need to look beyond the buzzwords to understand the scope, usability, and complementary capabilities of AI in order to benefit from the advanced technology.

> **"After a 10.7x increase over the prior 12 months, ransomware prevalence across our sensors remained at an elevated level over the latter half of 2021."**[1]

“According to Gartner’s Case-Based Research, the three most pervasive challenges that AI addresses are lack of detection capability, inadequate security posture, and poor operational efficiency.”[2]

Introduction

Focusing on the first one, lack of detection capability: “This category captures organizations’ inability to detect security attacks because of the scale of the attack (frequency of attack) or the sophistication of attack techniques that can bypass the detection of traditional security measures. For example, even with firewalls and antivirus software, malware can sometimes bypass those protections into the organization’s network. The malware evolves, thus conventional blocking techniques or signature-based algorithms cannot provide sufficient protection. Most organizations have the same number of people dealing with a growing number of threats, making it challenging for organizations to stay ahead of attackers. The use of AI/ML for this particular challenge is to help organizations scale in order to combat the frequency of attacks and the evolving techniques of attacks.”[3]

However, AI is frequently used casually by security vendors, without providing accompanying detail about the exact security challenge it is addressing and certainly without explaining the way it works in layman’s terms or the quantifiable benefit that it provides. Using the cyber kill chain stages, and most relevant type of AI as outlined in Gartner®, *Emerging Technologies: Emergence Cycle for AI in Security for Malware Detection*, we will explore specific challenges to which AI can be applied, ways those challenges can be addressed, and the types of benefit organizations should expect.

Using AI to Detect Malware Delivery

In order to gain a foothold within an organization, cybercriminals will attempt to deliver malicious code to target systems. Further, this code will often be designed as small, multicomponent code so that it can be frequently changed in order to bypass traditional malware protection technologies, such as signatures (exact matching), heuristics (generic matching), and similar pattern matching approaches. While these are worthy approaches for the time in which they were developed, the amount and frequency of change in ransomware (200,000 detections per week[4]) requires something more.

Gartner calls out AI in malware detection for code analysis as one of the emerging applications of artificial intelligence in security. They note that "rather than analyzing the behavior of files or objects, this group examines the actual code, scripts or memory calls of files and objects."[5] This is a promising area, as static analysis is much faster than behavior and other forms of analysis, making it perfect for prevention, rather than just detection and response use cases. Especially as we look at real-time delivery via the internet (as opposed to the store and forward method of email), AI-based code analysis is a critical capability to reduce organizational risk.

That said, as such models typically return a probability score (high, medium, low, or similar), it can be challenging to know what to do with the results when they are not 100% malicious or legitimate, especially when deployed in-line. Accordingly, it is important to look at the accuracy of the AI model, its customizability for your organization, and the intuitiveness of the result. When selecting a security control that includes AI for code analysis, assess the method by which the model retains its accuracy over time within your environment. Is it updated periodically from global labs, or does it also self-train and adjust dynamically? Finally, look at the additional insight it provides beyond just a mathematical score or risk rating. Can you understand how the score or rating was arrived at? And do you know what each object was intended to do, in addition to the fact that it has a degree of maliciousness?

Using AI to Detect Malware Installation and Execution

Of course, just because malware reaches the intended endpoint does not mean that it is able to install and run. AI in malware detection for code analysis should also be used on the target device itself before installation. Most modern endpoint security products will include “next-generation antivirus” (NGAV) as a preventive security control on corporate-managed devices. For sure, look for products that provide more than traditional signature-based technology.

Perhaps more importantly, since FortiGuard reports that only 20% of malicious code was dependent on user execution (and 80% run by API, scripting, and other automated methods),[6] ensure that AI models are applied to more than just code analysis. Another approach described by Gartner is AI in malware detection through modeling. “This group of malware detection assumes that models, developed and refined by AI analysis, will determine the presence of malware. Currently, vendors use unsupervised and supervised machine learning (ML) for this task. The models should directly predict malware from stronger signals. It is also possible that models could indirectly predict malware as well, potentially picking up weaker signals. Models based on behavioral observations could be set up to predict normal behavior. Then, the weaker signal of a deviation from normal could be deemed suspicious and lead to the detection of malware.”

This behavior-based approach is highly relevant for use on endpoint devices, which run the code and provide a robust data set of system activity on the host for analysis. But the variation in signal strength (confidence) lends itself more appropriately to detection and response products like endpoint detection and response (EDR), extended detection and response (XDR), or user and entity behavior analytics (UEBA). Given that additional investigation will be required, be sure to look carefully at the amount of effort required of your security team. How much associated information is served up to analysts along with the initial detection alert? Is it only enriched with threat intelligence, or has the AI also conducted routine investigation steps for the team? How much confidence does your team have in the ultimate detection? And for high confidence detections, how much of the mitigating response can be predefined and automated?

The reality is that while AI in malware analysis through modeling is a powerful capability, it can also be labor-intensive if AI and automation are not applied beyond the initial detection trigger. Be sure your organization is properly staffed and skilled for this capability.

Artificial intelligence can be effectively applied from the delivery and installation all the way through action on objective stages of the cyber kill chain. Look closely at the technology in EDR, NDR, and XDR in particular.

Using AI to Detect Malware Communications and Lateral Movement

This holds true beyond device-level activity. Even as cybercriminals co-opt legitimate applications, services, and actions on the endpoint (often referred to as living off the land), so too do they leverage them to explore the organization's network and move beyond the initial compromised device. Fortunately, their use in unexpected ways can also be identified by AI malware detection through modeling, once an initial baseline is established.

Network detection and response (NDR) products in particular apply such modeling to profile network traffic patterns in order to flag anomalies in the patterns, even as legitimate applications and services, ports, and protocols are utilized. In this instance, it's the local, self-learning models that are most important given the diversity of organizations, users, and their network traffic. Be sure to ask about the self-training methods of the AI in such products, but also the scope of the model. Which layers of the OSI stack are considered in building the baselines? Certainly, network, ports, and protocols are covered, but to what degree and with how much granularity?

That said, given the ambiguity in many cases, to what degree are more pragmatic analytics—cipher strength, protocol vulnerability, encrypted traffic profiling, IoC enrichment, and more—also applied? And what is the response process after detection? Highly manual or largely automatable? Given that cybercampaigns will often reach out after initial insertion to confirm entry, receive instructions, exfiltrate data, and other action on objectives, analysis of network traffic (both inside and outside the organization) often provides multiple opportunities to identify and interrupt attacks in progress.

Key Takeaways

The volume and sophistication of malware, the sophistication of its evasion techniques (often living off the land), and diversity of network activity are ideal for the application of artificial intelligence to detect threats that would go otherwise unnoticed by the human eyes of even experienced security professionals.

By using AI for malware detection in code analysis, through behavior modeling and more, organizations can regain critical advantage in thwarting multistage cybercampaigns before their end goal is achieved. But only if the sophisticated detection is fast enough, accurate enough, and understandable enough for organizations to take swift, often automated action to mitigate its impacts.

[1] Global Threat Landscape Report 2H 2021, Fortinet, February 2022.

[2] Ibid.

[3] Ibid.

[4] Global Threat Landscape Report 2H 2021, Fortinet, February 2022.

[5] Emerging Technologies: Emergence Cycle for AI in Security for Malware Detection, Gartner, October 27, 2020.

[6] Global Threat Landscape Report 2H 2021, Fortinet, February 2022.

FORTINET®

www.fortinet.com

March 9, 2022 2:03 PM

1475864-0-0-EN