WHITE PAPER

Use Artificial Intelligence to Combat Cyberthreats

Empower Defenders and Disarm Attackers

Executive Summary

Just a few years ago, much of the discussion on artificial intelligence (AI) was probably more bluster than benefit. But now, the pace of AI innovation and the positive and negative impacts it can have on organizations is changing at unprecedented scale. In cybersecurity, the advent of meaningful and disruptive AI tools and their use by cybercriminals amplifies the complexity and urgency to secure organizations and their digital infrastructures from emerging AI-based cyberthreats. The good news is that cybersecurity vendors have been applying various AI technologies for years. But when it comes to a future full of bad actors using AI-based tactics, it's critical for security and IT leaders and their teams to evolve their security strategies to address these sophisticated new AI-powered threats.

Innovate to Fortify

As organizations continue to pursue digitization initiatives, their attack surfaces inevitably expand. Whether the initiative is cloud adoption, the breaking down of air gaps between information technology (IT) and operational technology (OT), the proliferation of Internet-of-Things (IoT) devices connecting to the network, or the reality of hybrid workforces, many organizations are pushing the limits of their security and IT teams' resources. And now, bad actors' use of AI tools is compounding an already challenging and dynamic situation.

Recently, bad actors used deepfakes of a company CFO and other employees on a video call to successfully convince a worker to make a $25.6 million wire transfer.[1]

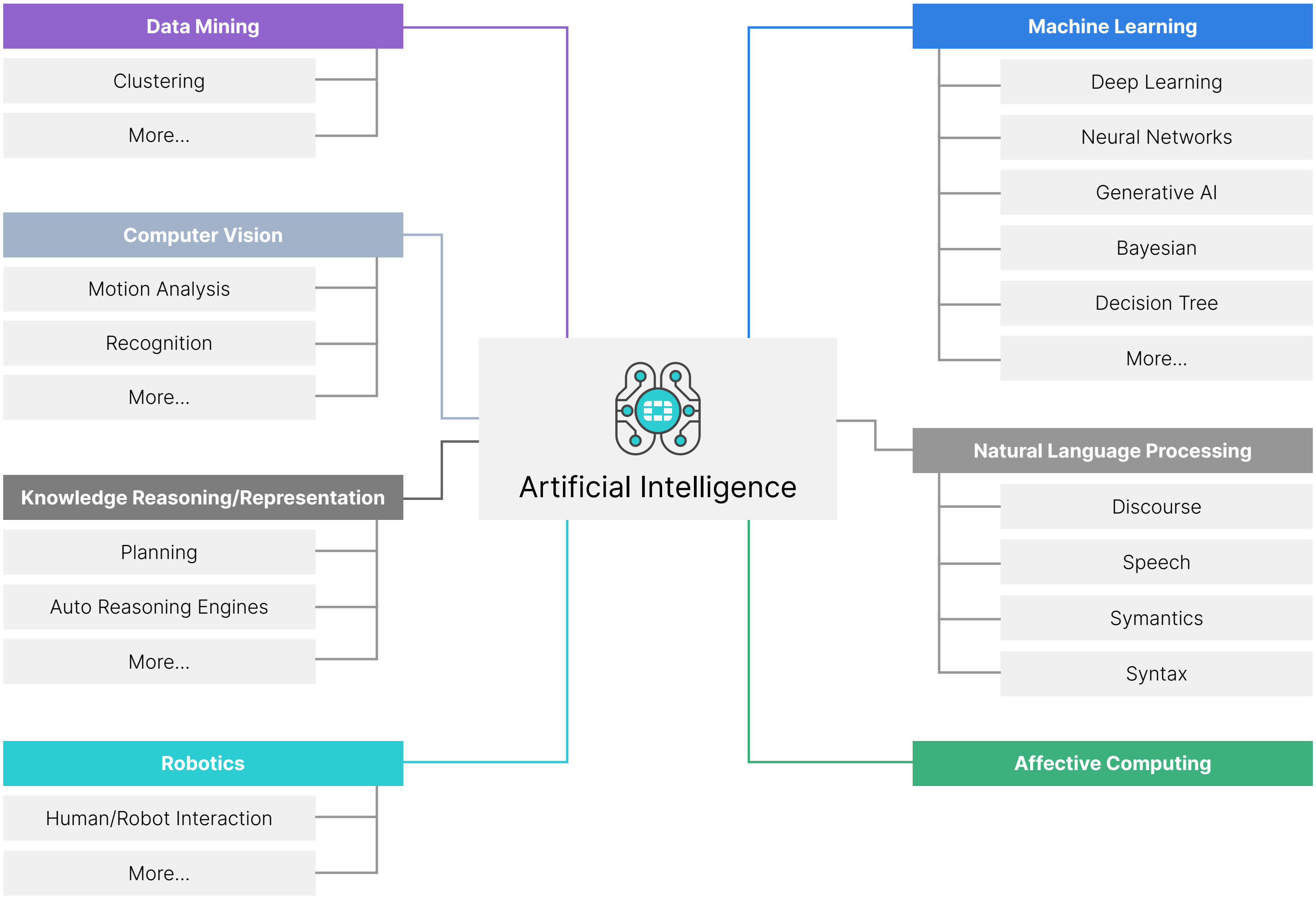

Figure 1: Artificial intelligence sub-fields or application areas

How the Bad Guys Use AI

Bad actors have harnessed AI's power to develop and use new, more capable, and compelling threats, including zero-day threats. With AI, attacks can be more targeted and launched faster than ever before. In the hands of bad actors, AI is having multiple effects:

- AI technologies, such as generative pretrained transformers (GPT) or generative AI (GenAI) are lowering the barriers to entry for new bad actors. Today using this technology, a non-English speaker anywhere in the world can create compelling email phishing and social engineering attacks with native-English syntax.
- AI can be used to create new malicious code and greatly reduce, while simplifying, efforts to develop new malware.
- The use of deepfake technology by bad actors has already inflamed the political class and electorate and has made it feasible to commit large-scale cybercrime.
- AI could be used to detect and exploit application vulnerabilities more quickly, which opens the door to increased supply chain risk for organizations around the globe.
- AI can be used to create adaptive variants of malware and launch swarm and coordinated multi-vector attacks.

Today, malicious AI tactics cover the entire attack life cycle outlined in the MITRE ATT&CK framework. MITRE has developed a knowledge base called ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems) detailing AI-based adversary tactics and techniques.[2]

Computer scientists at the University of Illinois Urbana-Champaign tested using Open-AI's Chat GPT-4 in concert with LangChain and the Playwright web browser as a malicious agent to scan websites for vulnerabilities and compromise those websites without human intervention. Amazingly, the authors cite the tool's ability to execute a 38-step process associated with a SQL Union attack.[3]

Challenges Amplified

The challenges posed by the modern and ever-evolving threat landscape are exacerbated by the use of AI by bad actors, putting added pressure on already taxed IT and security teams. Securing the expanding network environment and attack surface from these new threats is more complicated than ever with challenges related to:

- Siloed visibility across their environments
- A lack of centralized and coordinated policy application and enforcement
- The use of many disparate security tools and consoles that make monitoring, alert triage, and incident investigation and response extremely time-consuming
- Ongoing difficulties in hiring and maintaining security expertise

Effectively dealing with AI will require organizations to reduce complexity and friction and streamline operations.

How the Good Guys Use AI

The convergence of AI and cybersecurity isn't just a technological upgrade. It's a much needed and increasingly urgent evolution that can help organizations elevate their defenses against emerging threats to their modern attack surfaces. Many cybersecurity vendors have been applying various AI technologies for years. For example, Fortinet has been researching and using AI technologies for more than 10 years and continues to adapt and respond to the challenges of the modern attack surface with its AI-powered defenses.

AI-powered threat intelligence

The most significant use for AI in cybersecurity is threat detection and protection. A key element of detection and protection against threats is the creation and continuous enhancement of threat intelligence. The applied use of AI technologies is critical to data collection, analysis, correlation, and, ultimately, the formulation of that data into actionable intelligence. This type of AI-powered threat intelligence can be channeled through integrations to address a wide set of threat vectors and various types of threats, whether AI-enabled or not. How a vendor applies AI and their breadth of data sources and data matter. The more visibility a vendor has into their data, the more AI models can learn from that visibility.

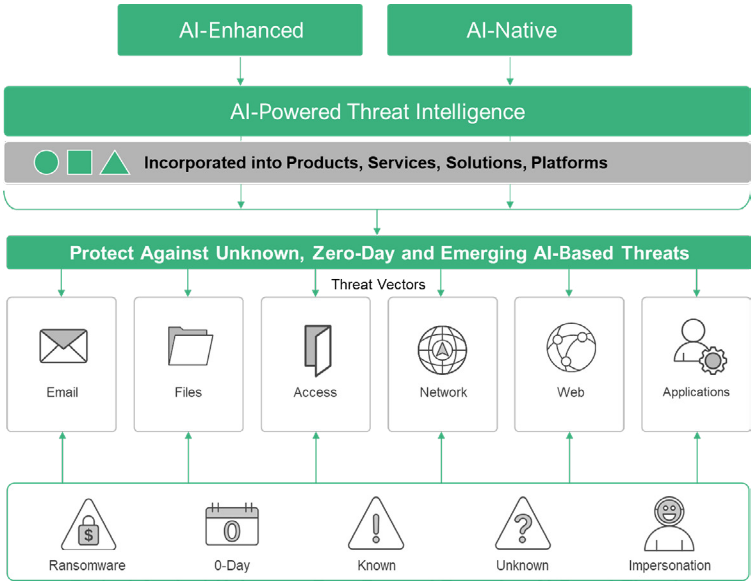
AI-Enhanced
AI-Native
AI-Powered Threat Intelligence
Incorporated into Products, Services, Solutions, Platforms
Protect Against Unknown, Zero-Day and Emerging AI-Based Threats
Threat Vectors
Email
Files
Access
Network
Web
Applications
Ransomware
0-Day
Known
Unknown
Impersonation

Figure 2: AI-enhanced and AI-native capabilities as part of threat intelligence formulation

Understanding the nature of the threat intelligence powering your organization's core security infrastructure is a good starting point to get more clarity into how your vendors are using AI technology. One core area may be your firewall infrastructure, a main line of defense.

Today's next-generation firewalls (NGFWs) represent a collection of capabilities beyond traditional firewalls. For example, your firewall may have built-in intrusion prevention, anti-malware protection including antivirus and sandboxing, and web security capabilities such as DNS and URL filtering. Talk to the vendor about how AI is being applied to enhance the firewall's capabilities, given the breadth of functions it has and the importance of each of those functions.

If the vendor can't provide insights on how AI is being applied, it's time to accelerate your refresh cycle and seek out vendors who are clearly using the latest technologies to enhance the efficacy of their solutions.

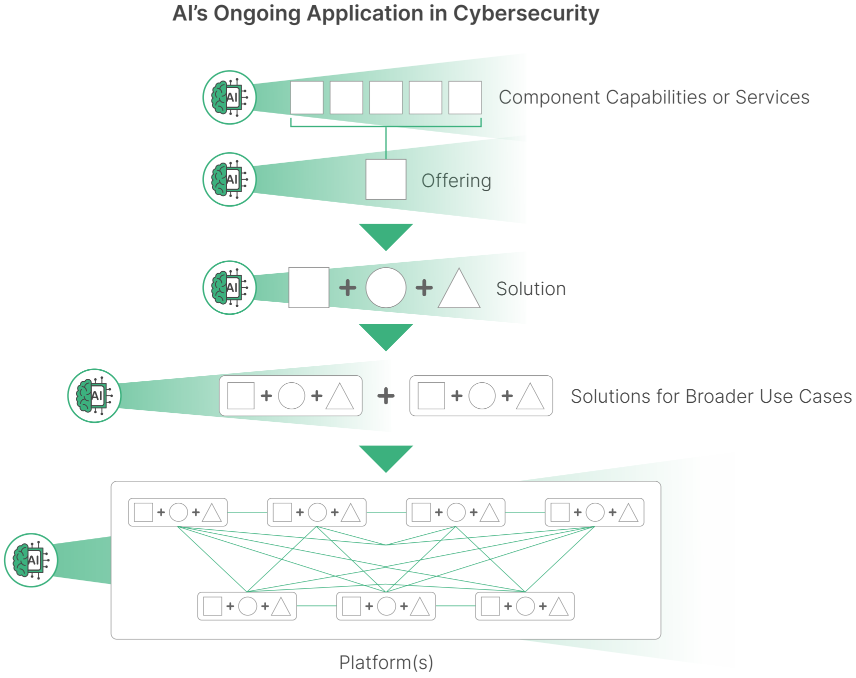
AI's Ongoing Application in Cybersecurity
AI
Component Capabilities or Services
Offering
Solution
Solutions for Broader Use Cases
Platform(s)

Figure 3: The application of AI and threat intelligence from component to platform

Understanding the nature of the threat intelligence powering your organization's core security infrastructure is a good starting point to get more clarity into how your vendors are using AI technology. One core area may be your firewall infrastructure, a main line of defense.

Today's next-generation firewalls (NGFWs) represent a collection of capabilities beyond traditional firewalls. For example, your firewall may have built-in intrusion prevention, anti-malware protection including antivirus and sandboxing, and web security capabilities such as DNS and URL filtering. Talk to the vendor about how AI is being applied to enhance the firewall's capabilities, given the breadth of functions it has and the importance of each of those functions.

If the vendor can't provide insights on how AI is being applied, it's time to accelerate your refresh cycle and seek out vendors who are clearly using the latest technologies to enhance the efficacy of their solutions.

Today, AI-enhanced solutions can help improve outcomes with benefits for both vendors and customers:

- **Firewalls:** NGFWs include security capabilities often powered by various AI models behind the scenes. Capabilities like intrusion prevention, antivirus, web security, and inline sandboxing may be using AI technologies to enhance the individual capabilities integrated into the firewall. When hybrid mesh firewalls are combined with NGFWs, organizations can realize dual benefits from AI-powered threat protection and enhancements in broader firewall visibility and centralized policy and firewall management.
- **Application scanning:** Although bad actors can use AI to create malicious agents, application scanning solutions and penetration testers can use the same capability to find and remediate vulnerabilities in both development and production stages more quickly.
- **Endpoint detection and response (EDR):** An EDR solution uses neural networks for pattern recognition to make sense of all of the event data being captured on an endpoint, including data on activities, processes, registry modifications, and memory accesses.
- **Security information and event management (SIEM):** A SIEM uses supervised and unsupervised machine learning (ML) models to perform sophisticated linear regression, including support vector regression, Gaussian process regression, and decision tree regression. It also uses ML to run various clustering algorithms. This analysis helps the SIEM solution accurately identify threats and vulnerabilities while minimizing false positives. SIEM solutions also utilize GPT technology and natural language processing (NLP) to create a more informed and guided experience for security operations center personnel. Analysts can directly query the AI engine and get insights on threats and guidance on appropriate incident response actions.
- **Image analysis:** Computer vision, image recognition, and neural network technology are combined for image analysis. Nearest-neighbor algorithms may also be used. Incoming images embedded in an email or downloaded from the internet can be scanned to determine if they present any risk or exposure. These images can include QR codes, pornographic imagery, violent and extremist imagery, or images with weapons, alcohol, or drugs.
- **Penetration testing:** OpenAI's Chat GPT4 can be used to advance penetration testing, and online videos show how to use Chat GPT4's large language model to write Python and Bash scripts within minutes for use in penetration testing.

The potential of AI doesn't stop with the formulation and application of AI-powered threat intelligence. For example, at Fortinet, AI technologies are being used to enhance the Fortinet Security Fabric platform to make it even more proactive, unified, and intelligent.

AI-native cybersecurity

The emergence of cybersecurity solutions that use AI capabilities as a starting point is often referred to as AI-native cybersecurity. Although there is no industry-standard definition for the term, AI-native cybersecurity tools do things at machine speed. For example, when analyzing potential threats, rendering a verdict and taking the prescribed actions occur at machine speed. Performing actions more quickly has positive advantages both from a cybersecurity and business standpoint. AI-native cybersecurity tools generally share the following characteristics:

- Utilize purpose-built AI models
- Embed AI at their core or as a foundation
- Are continuously learning and adapting to new threats
- Perform actions at machine speed

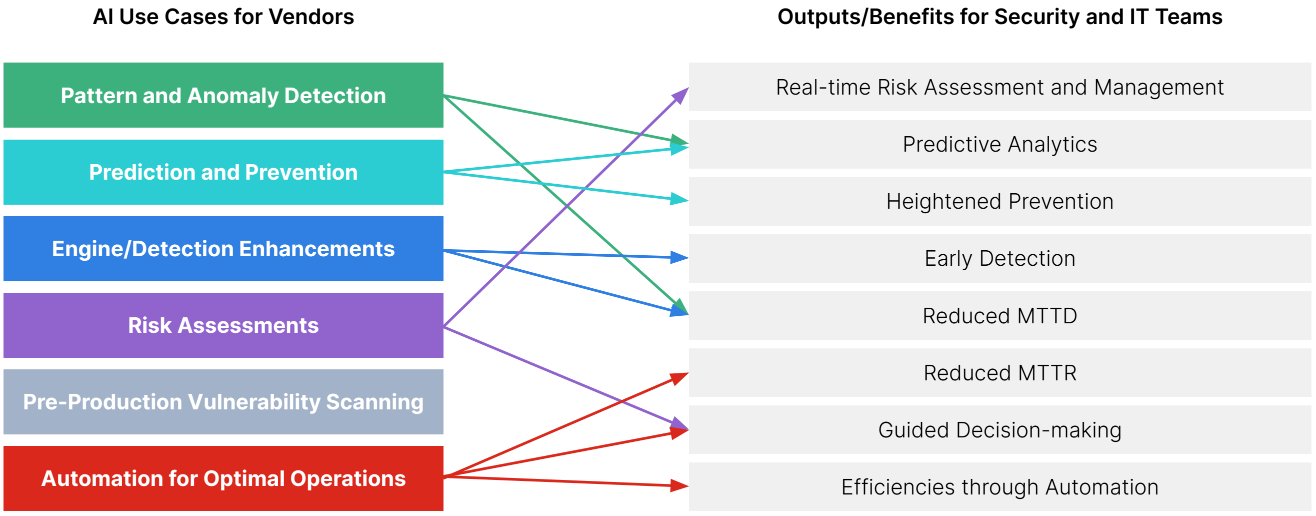
AI Use Cases for Vendors
Outputs/Benefits for Security and IT Teams
Pattern and Anomaly Detection
Prediction and Prevention
Engine/Detection Enhancements
Risk Assessments
Pre-Production Vulnerability Scanning
Automation for Optimal Operations
Real-time Risk Assessment and Management
Predictive Analytics
Heightened Prevention
Early Detection
Reduced MTTD
Reduced MTTR
Guided Decision-making
Efficiencies through Automation

Figure 4: Drivers for the vendor use of AI and resulting customer benefits

- Operate in real time

Use Cases and Recommendations

Security and IT teams outside of the cybersecurity industry need to understand that cybersecurity vendors are applying AI and, more specifically, the type of AI that is being applied, how it is being applied, and most importantly, how that AI benefits the organization directly.

Figure 4 represents the ways cybersecurity vendors might apply AI technologies in their solutions, supporting processes, and the various benefits. You can use the list in Figure 4 as a guide as you ask vendors questions about what their AI does to enhance their customers' security posture, particularly against AI-based threats.

As you move toward incorporating AI into your security strategies, consider the following recommendations.

Make AI a priority

Put AI on your team's radar. Assess your team's current awareness of AI technologies and principles. Establish the adoption of AI as a strategic objective across major areas of your security and IT infrastructure and prioritize those areas for review. Because vendors may use AI to some degree in their solutions, establish a questionnaire and process for evaluating vendors based on the merits of their AI know-how and integration.

Get educated

IT and security leaders should take steps to educate themselves and their teams on AI and how it can be used to improve their efforts and the solutions they purchase. This education will also be important to better understand when your organization is actively experimenting or deploying AI technologies for its purposes. Teams will be better prepared to ask the right questions regarding these use cases. Many online resources exist that provide some level of free education about AI. Once leaders and teams are somewhat educated, it may be worthwhile to consider paid online training content or even attending training by a reputable cybersecurity organization like SANS.

Stay informed

Stay on top of new AI developments in cybersecurity. Innovation is happening quickly, so it's easy to fall behind.

Review your security infrastructure

Assess how you can use AI technology in your security infrastructure. To start, consider reviewing how your organization benefits from AI technologies for your core or main lines of defense. Then, move into other controls that you have. In many respects, the progression of this review can follow existing risk prioritizations for your overall environment (where reviews are prioritized for the greatest areas of risk).

Ask questions

Ask the cybersecurity vendors you work with how they are using AI. Understand the technologies they are applying, how they are being applied, and most importantly, the benefits AI provides for customers. Here are a few questions to start with:

- What visibility into threats and related data sources does your organization use for the formulation of the threat intelligence that powers your product, service, and solutions?
- How is AI used in the formulation of that threat intelligence?
- What is your organization's experience concerning use of AI technologies in your products, services, and solutions?
- Can you tell me what specific AI technology or technologies are being applied to this product, service, or solution, and how they are being applied?
- Can you tell me what data sources the product, service, or solution uses to feed any AI technologies?
- How do you train and retrain your AI model or models?
- Are we able to engage with the AI directly in any capacity?
- How do you protect against data poisoning by bad actors?
- Can you tell me how your application of AI works to:
    - Reduce risk
    - Heighten prevention
    - Reduce mean time to detect
    - Reduce false positives
    - Help with alert triage and incident investigation
    - Reduce mean time to remediate
    - Help security operations analysts in their day-to-day roles

This is not a comprehensive list of AI questions, but rather a guide. Please add or customize your questions based on your organization's unique needs.

Add AI to vendor criteria

Make AI usage part of your request for proposal documents. Use the questions above and others to clarify AI usage across

[1] Heather Chen and Kathleen Magramo, 'Finance worker pays out $25 million after video call with deepfake 'chief financial officer,' CNN, February 4, 2024.

[2] MITRE ATLAS Adversarial Threat Landscape for Artificial-Intelligence Systems.

[3] Richard Fang, et al, "LLM Agents can Autonomously Hack Websites," February 6, 2024.

FORTINET

www.fortinet.com