CHECK POINT™

A CISO'S Guide to AI in 2024

TABLE OF CONTENTS

INTRODUCTION

Advancements in the field of generative AI have led to an explosion of interest and hype around chatbots that can create logical paragraphs, realistic images and that can seemingly mimic the human brain.

Modern chatbots rely on two branches of AI; natural language processing (NLP) and machine learning (ML). In cyber security, advances in the aforementioned branches of AI are driving new human-machine capabilities.

In short, AI is transforming the way that we approach cyber security, solving some of our most challenging problems and keeping us ahead of fast-moving threats. An essential tool in cyber crime prevention, AI can help protect businesses 24/7 in ways that were previously inaccessible.

Cyber security powered by AI is at the top of IT budget priorities. Ninety-two percent of organizations intend to use AI and machine learning to support cyber security and over half of business owners already use artificial intelligence for cyber security and fraud management purposes.[1,2]

As an example of AI's utility in cyber security, blending traditional security mechanisms with AI can result in an almost 100% detection rate, while dramatically reducing false positives.[3]

At the same time, artificial intelligence based cyber security tools can be prohibitively expensive for small businesses and AI tech's overwhelming popularity has transformed it into a target for hackers.

Organizations should carefully assess the advantages and limitations of implementing AI algorithms within cyber security programs. Questions to consider include 'Where is AI beneficial?' 'What are the drawbacks?' 'Which types of artificial intelligence based tools truly add value'?

In this eBook, see what experts have to say and drive stronger cyber security outcomes for your organization.

What is artificial intelligence?

Artificial intelligence is an umbrella term for a variety of different technologies. The researchers who created it can't agree on a singular definition, but artificial intelligence generally mimics human aptitudes and enables problem solving.

It relies on machine learning, the process of 'feeding' on massive amounts of data, in order to evolve capabilities beyond what initially arrives in the box or on the screen.[4]

Eventually, artificial intelligence may approach artificial general intelligence, or AGI. At this point, the technology will definitively match or surpass human capabilities.

CURRENT TRENDS

Every organization now manages tens, hundreds or thousands of connected devices. With 4.6 billion people surfing the web everyday, the amount of data produced each day is beyond imagination and it exceeds our abilities to independently contend with it.[5]

By 2025, connected devices are expected to generate 79 zettabytes of data annually.[6] (A single zettabyte is 2 to the 70th power bytes or 1,000,000,000,000,000,000,000 bytes.) In other words, they'll generate a massive amount of data.

In 2022, organizations that used AI within cyber security programs saved an average of $3 million.[8]

Your security operations center (SOC) team is likely already overwhelmed. Poorly integrated point solutions, fragmented data insights, and a shortage of qualified talent intensifies the challenges.

Due to their abilities to enhance the speed and scale at which organizations can secure digital infrastructure, autonomous cyber threat monitoring, detection and prevention solutions are growing in popularity. ...

Let's discuss speed and scale.

Leveraging AI as a 'co-pilot' can significantly reduce the number of days that it takes to spot trouble. AI-based tools can also lower the total cost of breaches.

Organizations save an average of $1.2 million if breaches are contained within 200 days or fewer, meaning that AI can be game-changing.[7]

Eventually, AI-powered tools may be our only option for keeping up with supremely sophisticated, stealthy and one-in-a-trillion threats.

---

[5] 53 Important Statistics About How Much Data Is Created Every Day, FinancesOnline Reviews for Business
[6] IoT Devices to Generate 70.4 ZB of Data in 2025, Says IDC, Larry Dignan, June 18 2019
[5] AI's Key Role in Cybersecurity and National Security, Brandon Pugh, The Hill, May 23 2023
[6] Ibid

BENEFITS

AI in cyber security can make cyber security management **easier**, more **efficient** and less **expensive**. Here's a snapshot of how AI might be able to enhance outcomes within your organization.

1. **Upgraded threat intelligence.** CISOs and cyber security teams can leverage AI to analyze threat intelligence data from a variety of sources. The AI can identify emerging threats and predict possible attacks, helping leaders stay ahead of evolving challenges and proactively protect their organization.

2. **Reduction of false positives.** Using AI, cyber security teams can reduce false positive rates. This conserves time and resources. While AI isn't perfect, it can prove more accurate than humans in parsing apart genuine threats from facsimiles, limiting false alarms.

3. **Increased efficiency.** AI-supported cyber security programs can automate time consuming and monotonous tasks, from monitoring logs, to scanning for vulnerabilities, to patching systems. In turn, security teams can focus their attention on more strategic activities.

4. **Clear predictive analytics.** AI can review and observe data patterns, predicting potential cyber threats before they become full-blown bombshells.

5. **Resolution of talent gaps.** There is a serious shortage of cyber security professionals. In contrast with humans, AI doesn't get tired, it doesn't go on vacation, and it won't leave for a better opportunity. In subbing for a human, AI can determine root cause analysis and can orchestrate next steps based on accumulated data and intelligence.

6. **Improved malware response.** AI allows for rapid malware family identification and attribution (malware DNA) including first seen malware variants.

BENEFITS

7 **Augmented incident response.** AI can help analysts cycle through a fast, data-driven and comprehensive incident response. It can automate workflow and remediation. Beyond that, it can enable SOC teams to review and refine incident response processes on a continuous basis.

8 **Disruption of bots.** Within cyber security, bots are a growing threat. They're used for malicious purposes, from spreading malware to stealing data. Artificial intelligence tools can observe patterns and block bots. It can then create more secure captchas and honeypots in order to disrupt them.

9 **Improved decision-making.** AI-based tools can present CISOs with real-time insights into the security of an organization, enabling leaders to make better informed decisions. In this way, AI-based tools can help improve resource allocation and assist with structuring the prioritization hierarchy for security initiatives.

10 **Automated threat response.** CISOs can configure AI-based tools so that it can independently respond to security incidents. For instance, in the event that AI detects a potential attack, it can automatically block the attack, quarantine a device as needed, and alert the security team. In turn, this cuts down on response times, prevents large-scale incidents, and enables security teams to tackle tougher problems.

11 **Compliance monitoring.** AI-based tools can prove useful in the context of automating compliance. This can assist CISOs with ensuring that the organization remains compliant with relevant regulations. It also ensures that corresponding compliance failure penalties are not levied against the organization.

The benefits of leveraging AI within cyber security programs can be irrefutably compelling and advantageous. CISOs should keep these benefits in mind when assessing how to improve their organizations' cyber security posture. Nonetheless, AI is not a panacea and cyber security programs must be designed with an eye towards the human factor and a comprehensive approach.

DRAWBACKS

As noted on the previous page, professionals can't simply install AI-based software and presume that all threats will be negated. AI-based tools aren't everything for everyone. In fact, there are valid reasons as to why organizations may hesitate to implement AI-based tools.

1. **Expense.** Incorporating AI into existing systems can be an expensive undertaking, particularly if an organization needs to purchase specialized hardware or software. For smaller organizations with more limited budgets, this is of particular concern.

2. **Algorithmic rigidity.** In the development phase, algorithms require huge training data sets. They are rigid and cannot adapt after initial training and it is sometimes challenging to interpret their decisions, meaning that they are opaque.

3. **Testing and validation.** Ahead of deploying AI-based tools, organizations should pursue rigorous testing and validation. AI model competence is a function of the training data that they've been given – If the data is insufficient or deficient in some way, the model may produce inaccurate results. For example, in the context of security, this could result in false positives, where the AI indicates a threat despite the absence of one. This can sink resources into unnecessary activities and cause undue stress.

New Trend: Microsoft has just developed the AI Security Co-Pilot, a version of ChatGPT-4 with essential knowledge of protocols and encryption algorithms.

The tool can respond to cyber security-related prompts. The AI Security Co-Pilot is designed to process information quickly and to help humans rapidly detect threats.

To combat this issue, CISOs should pursue a **human-in-the-loop** approach, where AI discoveries are validated by human cyber security experts. This will help keep a cyber security program effective, reliable and trustworthy.

DRAWBACKS

4 **Lack of explainability.** AI tools vary. Some AI tools are considered "black boxes." In other words, cyber security professionals will struggle to understand how the AI arrived at certain conclusions. In turn, this makes it tough to understand the root of a problem, can styme efforts to correct errors, or can obfuscate biases in models.

5 **Privacy concerns.** In some cases, AI-based tools may require access to sensitive data in order to operate as intended. This can result in privacy concerns.

6 **Adversarial attacks.** As useful as AI is for us, hackers have also discovered its utility. For hackers, artificial intelligence presents opportunities to launch sophisticated attacks. One type of adversarial attack involves the manipulation of AI-based tool input data, which deceives the AI model into delivering inaccurate results. In putting this into concrete terms, a system that delivers false negatives will prevent cyber security teams from seeing the real threats.

EXPERT INTERVIEW HIGHLIGHT

Yaniv Shechtman | VP Security Engineering, North America, Check Point

There is much discussion in the security community around the delivery of false positives and false negatives on the part of AI. As a CISO, here's what to keep track of...

Yaniv Shechtman has over 15 years of expertise in cyber security, AI, and product management. At Check Point, Yaniv's primary responsibility is to shape Check Point's Threat Prevention strategy and technologies, ensuring their products are always ahead of modern attackers and are able to prevent zero-day threats before anyone else.

Could you share a bit about AI and false positives and false negatives?

As AI is based on statistical algorithms, it is vulnerable to producing false positives or false negatives. Accuracy is crucial in AI because it has a direct impact on an organization's security estate, users' productivity and their ability to work without interruptions, and the workload of security teams who need to review false logs and manually decide on their verdict. To enhance the accuracy of AI, the model must be trained on a highly qualified data set. This approach will enable the AI model to make informed decisions and minimize the chances of false results. Security vendors with large customer bases have an advantage in this regard, as they can obtain a significant amount of data, which will result in a more accurate AI model. By ensuring that precision and recall are balanced, AI decisions will be reliable, trustworthy, and effective in solving problems.

What are your perspectives concerning the current trends around AI in cloud security?

With the increasing adoption of cloud-based services, current trends in AI and cloud security are quite promising. AI-powered predictive security analytics enable security teams to anticipate security threats. For example, 'Cloud Workload Protection' solutions that analyze network traffic and identify suspicious activity, 'Identity Threat Detection and Response' (ITDR) tools to identify users' abnormal behavior, or 'Cloud Identity Entitlement Management' (CIEM) that minimize the risk of unauthorized access to cloud environments and applications. Additionally, DevOps teams who manage cloud software development processes use AI-powered tools to automatically identify and remediate security vulnerabilities in code.2. Better threat intelligence so those engines can provide thorough, accurate prevention without impacting "business as usual" traffic.

Read the full interview here.

DECISION-MAKING: SELECTING SOLUTIONS

In many cases, the benefits derived through AI-based security technologies outweigh the drawbacks. AI-based tools can be a valuable addition for an organization that's looking to build next-generation cyber resilience.

When selecting AI-based technologies to incorporate into your cyber security program, ensure that you select a vendor that has a proven track record of developing artificial intelligence engines and incorporating them into critical decision points across products.

In addition, be sure to select a vendor that uses an extensive quantity of data to train AI models, as a higher quantity of data will enrich the product and likely make it of greater benefice to your organization.

Other considerations include:

- Whether or not a technology has high accuracy rates when it comes to threat prevention and detection. Explore independent evaluations and certifications.
- Compatibility with current security systems and whether or not your organization will be able to continue using existing security infrastructure/investments.
- The level of transparency available through the system. In other words, your new technology should offer clear insights into the decision-making process, enabling your team to evaluate and maintain confidence in the results.
- Availability of vendor support. Will your vendor provide timely patches and support as threats evolve?
- Assess whether or not the technology will still enable you to meet industry regulations and compliance. standards. Does the tool meet industry-specific compliance requirements

IN CONCLUSION

In many cases, the benefits derived through AI-based security technologies outweigh the drawbacks. AI-based tools can be a valuable addition for an organization that's looking to build next-generation cyber resilience.

When selecting AI-based technologies to incorporate into your cyber security program, ensure that you select a vendor that has a proven track record of developing artificial intelligence engines and incorporating them into critical decision points across products.

In addition, be sure to select a vendor that uses an extensive quantity of data to train AI models, as a higher quantity of data will enrich the product and likely make it of greater benefice to your organization.

PROTECT INNOVATION | PROTECT YOUR ENTERPRISE | IGNITE BUSINESS SUCCESS

Lastly, be sure to visit the executive-level thought leadership site CyberTalk.org for the latest artificial intelligence information.

You've got this. Is your organization AI-optimized?

Out-innovate the hackers. Protect what matters most and put security into action. For more insights into AI-based cyber threat prevention and detection tools, please reach out to your local Check Point representative.

Worldwide Headquarters
5 Shlomo Kaplan Street, Tel Aviv 6789159, Israel | Tel: +972-3-753-4599

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 1-800-429-4391

www.checkpoint.com