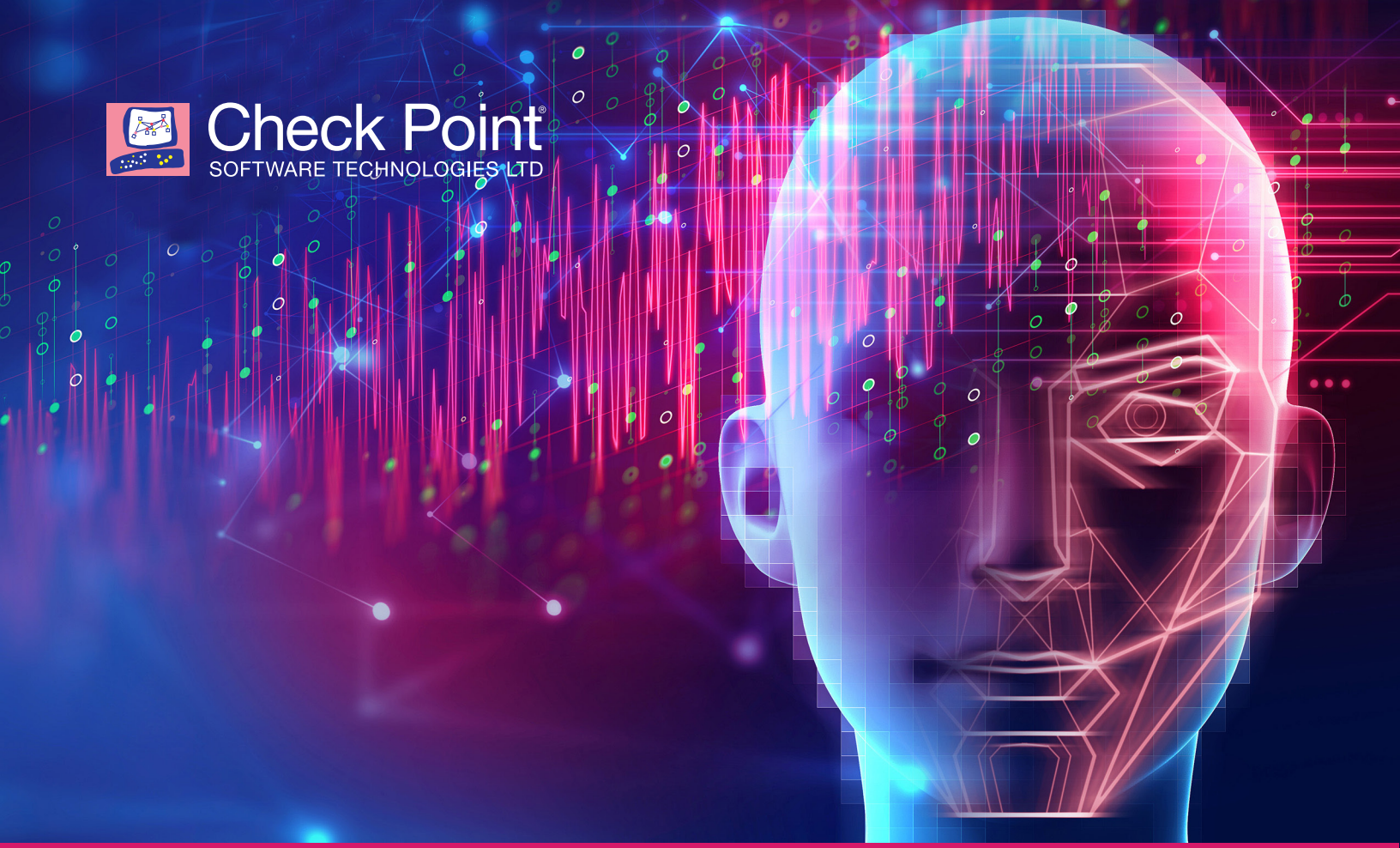

ARTIFICIAL INTELLIGENCE:

An Emerging Catalyst for Cyber Security

Introduction

Artificial intelligence (AI) technology has come of age in elevating cyber security. In 2018, global development of AI within the cyber security market reached $7.1 billion, and it's projected to reach nearly $30.9 billion by 2025.[1]

It's a market segment that's reaching C-suite executives.

A Cap Gemini Institute survey of 850 senior information security executives found 61% of enterprises can no longer detect breach attempts without AI technology.[2] Another 48% claim they'll be increasing AI budgets by an average of 29% in FY 2020. Seventy-five percent of these executives say they are currently testing AI cyber security use cases.[3]

The further along you are in your digital transformation, the greater your exposure to cyberattacks. Digitalization means more entry points beyond the conventional network perimeter, including cloud deployments and connected mobile and IoT devices. Add increased vulnerabilities to an intensified cyberattack environment and it's clear; modern cyber security can't be anything less than smart, agile, and manageable.

> AI offers huge opportunities for cyber security. This is because you move from detection, manual reaction, and remediation towards an automated remediation, which organizations would like to achieve in the next three or five years.
>
> *– Oliver Scherer, CISO, MediaMarktSaturn Retail Group* [4]

In this paper, we'll explore how artificial intelligence and machine learning (ML) can bolster your cyber security practices. We'll discuss how increased intelligence is helping to forge a more proactive cybersecurity approach that allows you to prevent threats before they unleash destructive payloads.

---

[1] "Artificial Intelligence (AI) in Cyber Security Market Will Reach to USD 30.9 Billion by 2025," Zion Market Research, August 28, 2019

[2] "Why AI is the Future of Cybersecurity," by Louis Columbus, Forbes, July 14, 2019

[3] Ibid.

[3] Ibid.

Reinventing Cyber Security with AI

Incorporating AI into cyber security is a global, cross-industry endeavor. The chart below shows how virtually all industries are looking to AI for improved security. Telecommunication, manufacturing, and banking rank highest.[5]

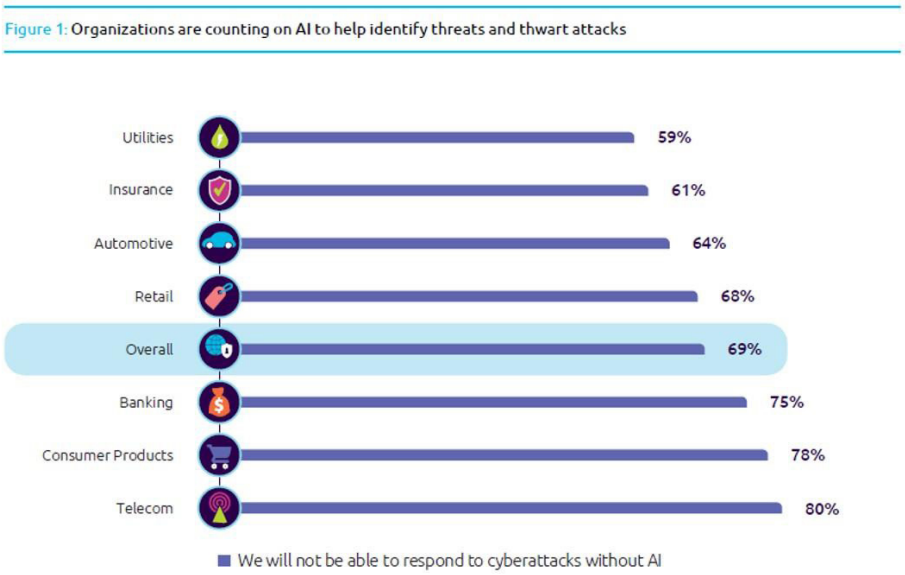

Figure 1. Source: Cap Gemini - Industries and AI cyber security

Telecommunication companies use machine learning algorithms to detect fraudulent activity such as theft or fake profiles, and illegal access, among other activities. Algorithms learn "normal" activity, which allows IT security to spot anomalies with huge data sets. Organizations gain near real-time response to suspicious behaviors.[6] Similarly, banks are upgrading and overhauling traditional fraud and cyber security threat detection with AI-based technology. Improved anomaly detection that identifies abnormalities in a dataset can speed up fraud detection and prove more cost effective.[7]

For decades, traditional firewalls with packet filtering, stateful inspection, VPN support, among other capabilities have defended perimeter-based networks. Next generation firewalls include network device filtering capabilities such as advanced threat prevention, anti-virus, URL filtering, intrusion prevention, and other functions. Protecting beyond conventional networks that can include dynamic, multi-cloud environments, and network-connected endpoint and mobile devices offers new challenges.

[5] "Why AI is the Future of Cybersecurity," by Louis Columbus, Forbes, July 14, 2019

[6] "The Amazing Ways Telecom Companies Use Artificial Intelligence and Machine Learning," by Bernard Marr, Forbes, September 2, 2019

[7] "How artificial intelligence is helping banks," by Raghav Bharadwaj, Fintech News, August 30, 2019

Making a Case for AI-based Cyber Security

AI can help organizations identify and respond to breaches faster. Smart algorithms are key to helping software do its job at a rapid clip while simultaneously increasing accuracy. Here are several reasons why AI-based cyber security is growing:

- Computing power for specialized AI chipsets has increased
- Data lakes and connected Internet of Things (IoT) have increased the amount of training data for AI algorithms, expanding AI domains and decreasing costs
- Accuracy and applicability of existing algorithms have been increased by overcoming previous technology bottlenecks
- Decreased costs for cloud storage and computing have made combining highly specialized knowledge easier than ever before

The infusion of AI and machine learning into cyber security is proving to be a competitive differentiator. It can allow you to adopt cyber security that's effective in preventing unknown, zero-day threats.

The graphic below shows that AI can play a role across many attack vectors:

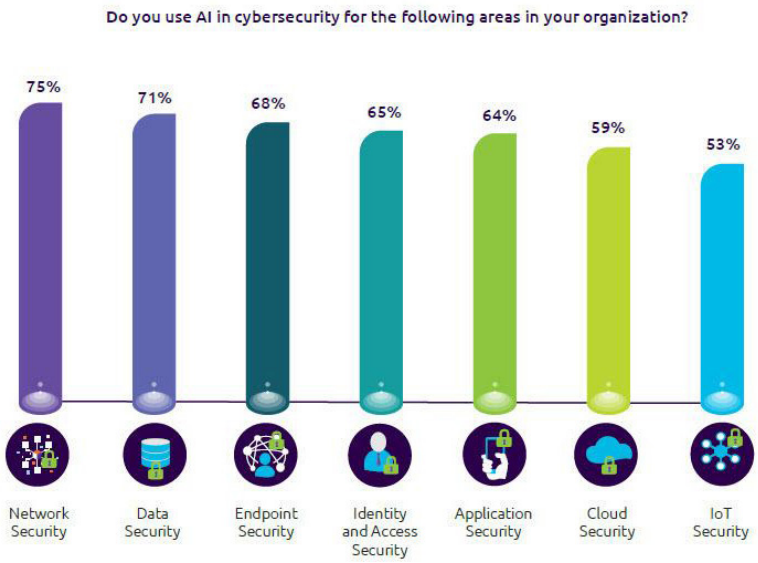

Figure 2. Source: Capgemini Research Institute - Ai in Cybersecurity executive survey, N = 850 executives

[8] "Software at the World, Now AI is Eating Software," by Tarry Singh, Forbes, August 29, 2018. https://www.forbes.com/sites/cognitiveworld/2019/08/29/software-ate-the-world-now-ai-is-eating-software/#16d66c395810h

[9] "Why AI is the Future of Cybersecurity," by Louis Columbus, Forbes, July 14, 2019

Practical Uses Cases for AI and Machine Learning in Cyber Security

The machine learning piece of AI enables computers to use and adapt algorithms based on the data that's collected. Computers can then learn from it, and understand what security improvements are needed. With advanced cyber security platforms, computers can predict threats and observe anomalies faster and with greater accuracy than humans. Here is a list of practical uses for AI/ML as seen from a CISO and security researcher perspective:[10]

- **Password protection and authentication:** AI is being used to enhance biometric authentication, remove imperfection, and develop a more reliable system. Apple's Face ID is an example.
- **Phishing detection and prevention control:** AI-ML can detect and track active phishing threats and respond and remediate more quickly than humans. AI is used to rapidly differentiate between fake and legitimate websites.
- **Vulnerability management:** AI-based systems can proactively look for potential vulnerabilities in information systems by analyzing important factors such as discussions on the dark web, hacker reputation, and patterns used, among others. An analysis of these factors can help determine when and how a threat might be launched at vulnerable targets.
- **Network security:** AI can be used to expedite several processes, including the creation of security policy, and to figure out an organization's network topography. Observing and learning network traffic patterns can help suggest security protocols.
- **Behavioral analytics:** ML algorithms learn and create behavior patterns based on how a device and online platform are used. Unusual activities are flagged as suspicious, triggering the blocking of a user action.

[10] "How Artificial Intelligence is Changing Cyber Security Landscape and Preventing Cyber Attacks," by Remesh Ramachandran, Entrepreneur, September 14, 2019

Conclusion

When it comes to keeping your people and their data safe from cyberattacks, AI has emerged as a key technology to elevate cyber security for the digital age. It's already demonstrating its ability to improve the accuracy, detection, and prevention of cyberthreats. AI-driven cyber security offers business benefits, including reduced costs and improved user productivity time.

It needs mentioning, however, that AI technology is available to all who want or need it. Adversaries could use AI to automate cyberattacks and hack a system's vulnerability even faster than it's done today. AI might be used to disguise attacks so that you do not know that your network or device has been exploited. Cyberattacks are an ugly reality for organizations around the globe, and the threats grow more challenging with each passing day. The emergence of AI technology that integrates into your cyber security is an important trend worth your investigation.

Check Point has adopted AI-capabilities into its solutions for many years. SandBlast Network and SandBlast Agent (for endpoint protection) are examples of improved threat prevention combining AI, machine learning, and behavioral analysis. Our AI-based malware code decomposition explores malware DNA and ancestry to help protect against unknown malware and understand its contents.

For further information, visit Check Point Zero-Day Protection.

[11] "How Artificial Intelligence is Changing Cyber Security Landscape and Preventing Cyber Attacks," by Remesh Ramachandran, Entrepreneur, September 14, 2019

Worldwide Headquarters
5 Ha'Solelim Street, Tel Aviv 67897, Israel | Tel: 972-3-753-4555 | Fax: 972-3-624-1100 | Email: info@checkpoint.com

U.S. Headquarters
959 Skyway Road, Suite 300, San Carlos, CA 94070 | Tel: 800-429-4391; 650-628-2000 | Fax: 650-654-4233

www.checkpoint.com