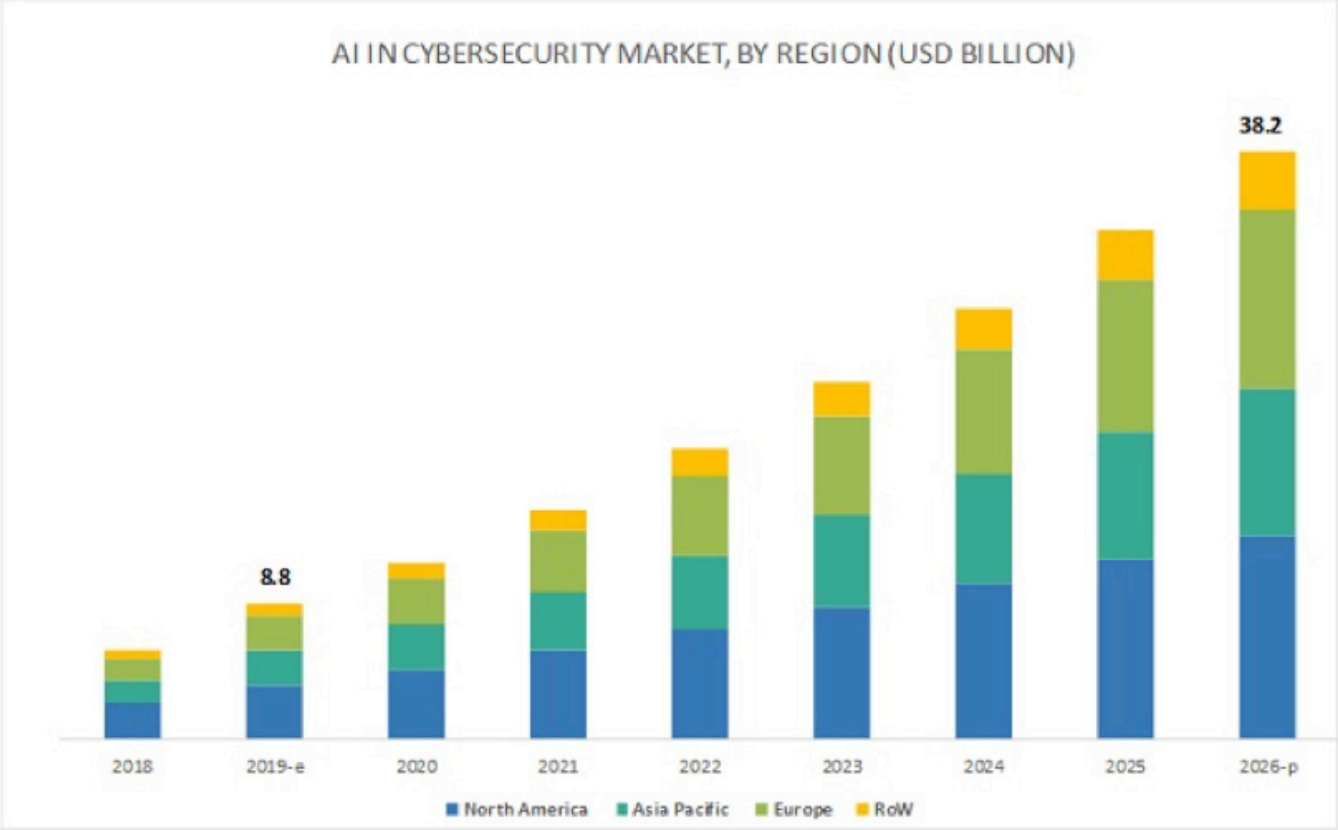
ROBOGLOBAL®
INVESTING IN INNOVATION

ARTIFICIAL INTELLIGENCE: THE BEST WEAPON IN THE WAR AGAINST CYBER ATTACKS

By Lisa Chai, Senior Research Analyst, ROBO Global

Cybersecurity threats have steadily increased in recent years, with 3,800 breaches so far in 2019 alone—an increase of more than 50% over the last four years. In response, businesses around the world are seeking trusted solutions to address this fast-growing problem. At the same time, companies everywhere are finding it more and more difficult to hire and retain skilled security talent. Solution providers are rushing to the rescue, including both established cybersecurity leaders and startups that are harnessing the potential of AI algorithms to deliver next-generation solutions that are able to identify and prevent cybercrimes with minimal human input. Using machine learning and AI neural networks, engineers are finding ways to adapt to new criminal techniques—or **attack vectors**—and to better anticipate the next steps of the hackers behind the major breaches that are happening in the world today. The result: according to recent reports, **AI in cybersecurity** is projected to grow at a 23% CAGR to reach $38B by 2026, with the majority of that growth coming from the US and Europe.



Source: MarketsandMarkets

This rise in cybersecurity spending is imminent. An increasing number of C-suite executives now consider digital security and advanced threat detection the top reasons for adopting machine learning and AI within their organizations. The attraction to AI is rooted in its use of pattern recognition and other powerful algorithms to detect threats early on, reduce response time, and minimize the manual tasks required by automating the inspection process—all more accurately than humans. AI-enabled cybersecurity is currently the most effective method of combating stealth attacks, insider threats, distributed denial-of-service (DDoS) attacks, and more.

THE VAST AND GROWING THREAT OF CYBERCRIME

Safeguarding our passwords and controlling access to networks and confidential information remains a high priority for businesses and consumers alike. But despite efforts to thwart attacks before they start, the threat landscape has expanded, and new attack vectors targeting social media, smart devices, cloud computing, and virtualization have created the need for improved security. The most recent report by **Kaspersky** states that the number of DDoS attacks increased by 84% in the first quarter of 2019 compared to 4Q 2018, and that these attacks are also reaching record lengths.

Case in point: earlier this month, **Wikipedia** and Blizzard's **World of Warcraft** were both downed by DDoS attacks in the same weekend in targeted, connected attacks. The first major attack on Wikipedia's servers, September's incident prevented millions of users globally from accessing one of the world's most popular websites for three days. The series of attacks on Blizzard's servers also resulted in failures, timeouts, players being disconnected, and exceedingly long wait times in the US and Europe for two consecutive days.

Source: Activision

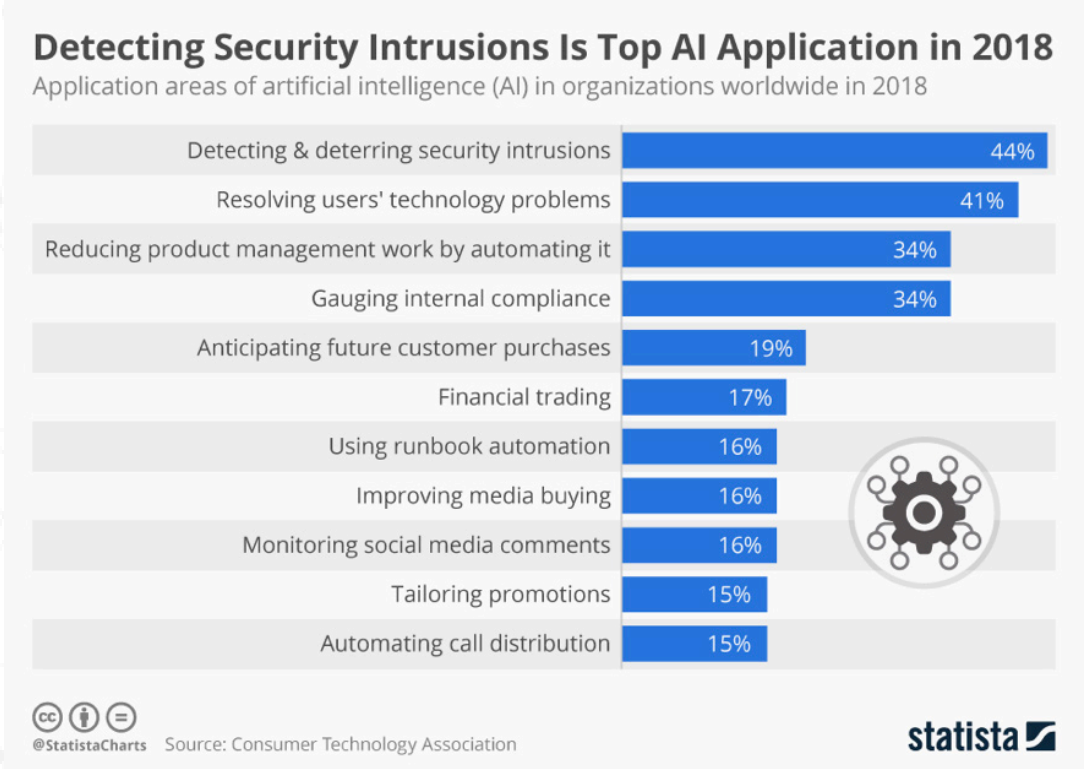
Of course, cyber attacks are by no means limited to the world of gaming and online content. In July, a hacker gained access to the personal information of as many as 100 million Americans and 6 million Canadians in a **Capital One breach**. In May, poor website security was blamed when real estate giant **First American** exposed more than 885 million documents related to real estate closings over the past 16 years, including bank account numbers and statements, mortgage and tax records, Social Security numbers, wire transaction receipts, and driver's license images.

The risk cannot be understated. Over 4.3 billion people are **active internet users** as of July 2019, encompassing about 56% of the world population. Various types of cyber attacks such as unauthorized access, ransomware, malware, and Phishing are causing a huge loss to the global economy. Recent reports from **ForgeRock** indicate that cybercriminals exposed 2.8 billion consumer data records in 2018 alone, costing US organizations over $654B. In 2017, the **Equifax breach** impacted 147 million people and the company was fined $700M as a part of a settlement. The global cost of cybercrime has now reached as much as $600B—about 0.8 percent of the global GDP[1]—and is expected to exceed $6T annually by 2021[2].

THE USE OF AI IN CYBERSECURITY

Luckily, AI is coming to the rescue. The cybersecurity industry has been using **machine-learning** algorithms for decades, but in recent years, AI experts have developed sophisticated data protection techniques using deep-learning algorithms to take security to a new level. End-point security, data encryption, vulnerability assessment, and threat detection are just some of the areas in which AI is being applied today. AI uses deep-learning algorithms to find patterns in data, detect user behaviors and intrusions, and predict security threats. And once a threat is detected, AI speeds up the incident response to give companies the ability to proactively thwart an actual attack. Some AI bots even block access to certain websites completely, stopping threats in their tracks. Security firms that have embraced and incorporated AI into their solutions are already helping companies around the globe to improve security of their on-premise, virtualized, and cloud networks.

[1] Economic Impact of Cybercrime— No Slowing Down, McAfee, February 2018
[2] Cybersecurity Ventures, 2017.



THE FUTURE OF CYBER DEFENSE

One of the biggest cybersecurity challenges has been the nearly universal migration to the cloud. The move to cloud-based infrastructures has been rapid, largely because these networks are much easier to manage and automate than traditional machine architectures. The downside is that applications, data, and other assets stored in the cloud can be more vulnerable to attack than assets stored behind a traditional firewall. The shift has created opportunities for cyber attackers to identify vulnerabilities in cloud containers and server-less functions, and the resulting breaches that occur in microseconds can be virtually impossible to detect.

Luckily, there are many cloud security companies actively tackling the challenge:

- **Rapid7** offers solutions that are tackling the cloud cybersecurity landscape by adding an extra layer of security. Rather than simply automating security operations tasks, these solutions use algorithms to learn from previous actions. Like any AI, the more data the solutions receive, the more accurate they can be in identifying and responding to threats.
- **Prisma**, developed by **ROBO Global Artificial Intelligence Index** (THNQ) member and global cybersecurity leader **Palo Alto Networks**, is among the most complete cloud security suites, offering data protection, governance, compliance, and application traffic control in one platform. At its most recent investor day event, Palo Alto Networks outlined that there were over 925 million new malicious programs registered this year alone, and that it has released several significant advancements in the past few months that use the power of advanced AI and machine learning with the goal of transforming how the security industry tackles these newest threats.

- In February, Palo Alto Networks introduced another new solution for the cloud. **Cortex** is the industry's first open and integrated security platform using AI, enabling enterprise customers to securely and privately store and analyze large amounts of data to find threats and orchestrate responses quickly. Cortex uses the company's Trap 6.0 solution to accelerate threat investigation and incident response.
- **Varonis**, another member of the ROBO Global THNQ Index, offers solutions that focus on enterprise cloud data and file analytics. Varonis uses an AI-powered permissions recommendation engine to fuel its cloud security platform that maps and monitors data to reduce risk, detect threats, and prove regulatory compliance.
- **Crowdstrike** is a pioneer in the space, offering a cloud-based architecture for endpoint technology at the device level. Its solution has a significant advantage in terms of scale and the ability to leverage real-time threat intelligence using AI and machine learning.
- **Darktrace** is an AI platform company offering solutions that help prevent threats before they cause damage. Its algorithms are designed to understand and analyze normal patterns of behavior of each individual user and every device connected to a corporate network in order to predict and protect against emerging threats in real time.
- ROBO Global THNQ Index member **ServiceNow** provides digital workflow solutions to address another need: the global shortfall of an estimated 3.5 million unfilled cybersecurity positions by 2021.[3] To mitigate the need for in-house data scientists, the company's solutions automate back-office and front-office tasks and are aligned with cloud providers to streamline cloud workloads through tight security and IT integration that aggregates, organizes, and prioritizes security alerts from multiple cloud services.

These companies comprise only a part of the fast-growing cybersecurity market. Recent estimates predict the global cloud security market to reach $27.2B by 2025, growing at a CAGR of 25.86% from 2017 to 2025.[4] This is good news for users of AI-enabled cybersecurity solutions, for consumers, and for investors in these much-needed technologies. While the providers listed above are each delivering valuable solutions to help prevent cyber attacks today, we predict that the future will bring an evolving mix of best-of-breed companies, and that these companies are likely to introduce a new generation of autonomous AI-powered solutions that will draw market share from legacy vendors. We expect the market to evolve rapidly, making it mandatory for investors to seek broad exposure based on the most current research and information.

[3] Cybersecurity Jobs Report 2018-2021
[4] Verified Market Research, September 2019