GLOBAL X
by Mirae Asset

GLOBAL X INSIGHTS

Cybersecurity Faces Transformation from Generative AI

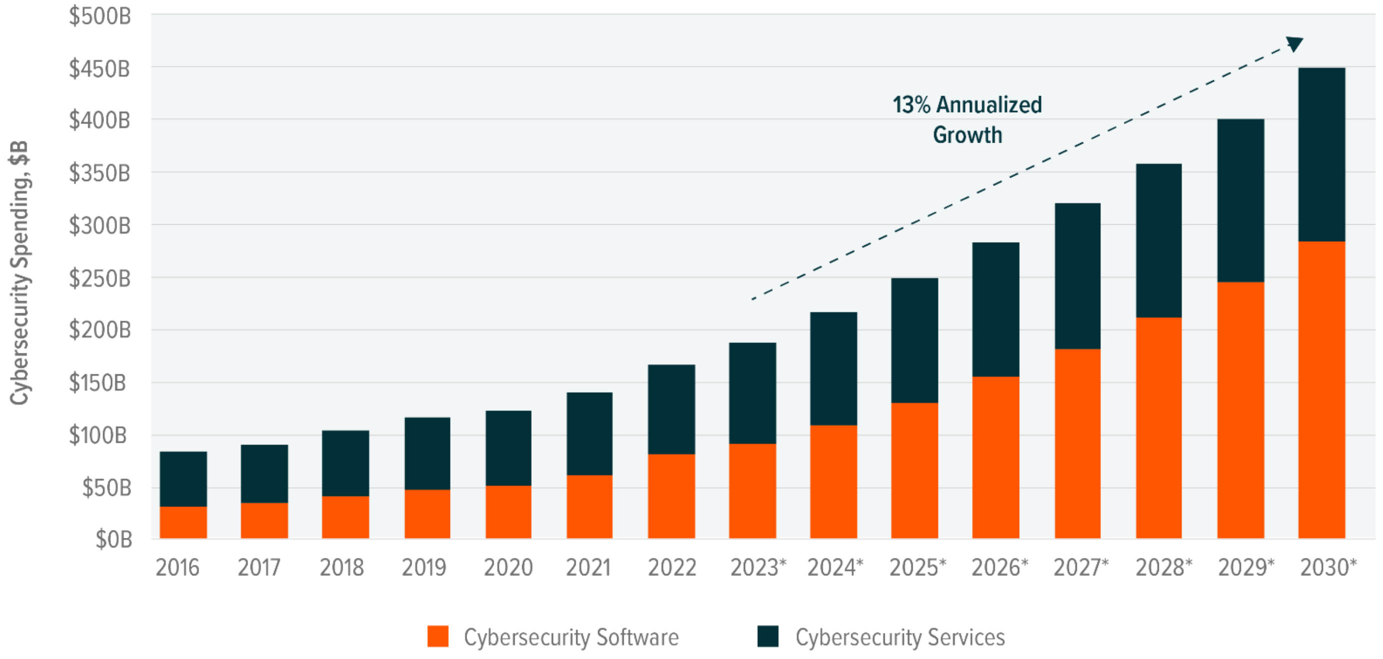
Tejas Dessai
tdessai@globalxetfs.com

Date: April 2, 2024
Topic: Thematic

We believe that Cybersecurity is a compelling theme in 2024 for multiple reasons. First, an evolving attack landscape requires corporations to keep their guard up and security spending elevated. Second is the growing relevance of generative AI, which is a double-edged sword. Generative AI enables malicious actors to discover vulnerabilities and improve attack methods, but it also enables security teams to build better defenses, detect threats, and manage operations more efficiently. The cybersecurity industry is on the verge of yet another transformation amid AI's proliferation, and we expect it to create numerous opportunities for share wins, including through consolidation. For investors seeking exposure to AI outside of the obvious beneficiaries, cybersecurity may have appeal.

GLOBAL CYBERSECURITY SPENDING FORECASTED TO GROW TO $450 BILLION BY 2030

Sources: Global X estimates with data from Gartner (2023, Sep 28) Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024.



*Indicates Forecast

Key Takeaways

- High-profile cyberattacks continue to cripple organizations despite growing cybersecurity investments. The emergence of generative AI presents new threats.
- Generative AI also helps cyber professionals build effective defenses. Major cybersecurity vendors are rapidly developing AI-powered tools to augment human analysts, automate security operations, and detect anomalies.
- Despite economic headwinds, global cybersecurity spending is projected to grow over 14% in 2024 to $215 billion, driven by growing attacks and the urgency to strengthen defenses against AI-enabled threats.[1]

Generative AI Complicates an Already Complex Cyber Attack Landscape

Even the most technologically sophisticated organizations aren't immune to cyberattacks. In 2023, Microsoft was hit with a nation-state sponsored attack, perpetuated by Russian hacking organization Midnight Blizzard that wanted to use information harvested from corporate email systems to breach Microsoft's source code repositories and internal systems.[2] Johnson Controls, a leading electrical equipment supplier, received a $51 million ransomware demand from the Dark Angels after they claimed access to the company's private drives with over 27 terabytes of data.[3] At MGM Resorts, hackers stole personal data of over 10 million customers.[4]

Government assets are also a growing target. China-based hackers managed to get access to email accounts of employees of nearly two dozen organizations starting in May 2023, including the U.S. State and Commerce Departments. The breach was not discovered for three months.[5]

By 2025, cyberattacks are expected to cause $10.5 trillion worth of annual damage to enterprises and governments, a nearly 300% increase since 2015.[6] Annual global cybersecurity spending of $225 billion is insufficient to defend against these attacks and keep up with what will be dynamic changes in the technology landscape.[7]

One such change is the growing prominence of sophisticated generative AI models, which are particularly consequential to phishing and social engineering-based attacks. Large language models can take in information, whether real-time news and updates or personally identifiable information, and generate malicious links, emails, and spurious websites that appear increasingly realistic. As nearly 88% of all security breaches happen because of human error, generative AI can help hackers exploit human vulnerabilities to access broader systems.[8] In 2022, cloud security leader Zscaler reported a 47% surge in phishing attacks enabled by AI.[9]

Moreover, unlike human hackers, AI agents are available 24x7, and they can be designed to monitor digital assets such as websites, tools, and systems for vulnerabilities. Due to their high uptime, AI agents that can attack and overwhelm websites is also a growing threat.[10] Another threat is the rising unmonitored access to online digital assistants, which could result in corporate employees sharing private information. Many large corporations have restricted access to these models until guardrails are in place.[11]

AI Can Also Help Fortify Cybersecurity

Primarily, AI can help with anomaly detection by scanning mundane enterprise traffic for deviations from the norm and surface those patterns quickly to human decision makers. These tools could be particularly effective for technologically less sophisticated businesses and businesses with small teams. AI can also help summarize cybersecurity alerts, breaches, and log data in simple language so engineers can get up to speed on IT issues. With understaffing in cyber jobs high, these simple systems can significantly boost productivity. Organizations can also use AI to perform penetration testing and craft scenarios that attempt to breach enterprise systems to determine weaknesses in networks.

The industry is responding swiftly to this dynamic AI-induced demand. In 2023, CrowdStrike, the leader in end-point security, launched Charlotte AI, which is designed to act as a low-level security analyst that can perform mundane operations.[12] The system features a tight feedback loop that includes insights from human operators, intrusion detectors, and incident response teams. The system also improves the intelligence that CrowdStrike tracks across more than 200 adversaries, learning their increasingly sophisticated tactics and breach techniques.

Similarly, Check Point launched a generative AI support and automation assistant called Infinity AI Copilot that automates operations, potentially being a solution for the global shortage of cybersecurity professionals.[13] Identity management services provider Okta launched a series of AI-specific tools to help with workforce and customer identity.[14] Palo Alto Networks, Zscaler, Fortinet, and nearly all other major cybersecurity vendors have plans to launch similar products.[15]

Large cloud vendors are also looking to expand their market share in cybersecurity by using AI. Available in April 2024, Microsoft Security for CoPilot will allow security and IT professionals to ask questions, assess threats, write code, and help with security and defense operations.[16] The model powering Security for CoPilot has been improved on over 78 trillion security signals that Microsoft processes each day.[17] The platform is expected to make experienced security professionals 22% faster and nearly 7% more accurate across analysis. Ninety-seven percent of security professionals who have used the platform cited interest in using it again.[18]

Last year, Google integrated generative AI across its threat intelligence and cybersecurity operations platform. Google will combine its Mandiant cyber intelligence offerings and its Chronicle security operations platform with its Vertex AI infrastructure solutions to create an AI system called Sec-PaLM, which will form the core of its AI-based security offerings.[19] Core to this system is software from Mandiant, which Google acquired in 2022.

AI Can Benefit Security Spending

Cybersecurity spending was forecasted to grow 10.6% in 2022 and 14.2% in 2023, despite the broader IT industry entering a slowdown.[20] We believe this resilience signals the urgency and commitment to continue to build comprehensive defenses, particularly with new threats likely to emerge with AI's proliferation. According to Global X forecast, annual security spending could top $450 billion by 2030.[21] Spending on artificial intelligence solutions for cybersecurity is expected to grow to $61 billion by 2028.[22]

Software-based spending is likely to show unique resilience, given the predictable nature of the recurring revenue models that are common in cybersecurity. The industry is also migrating towards a consumption-based pricing model, which favors unit economics significantly. Areas such as identity security, application security, penetration testing, end point security, zero-trust solutions, are expected to show tremendous momentum.

Also, we believe that industrywide M&A (mergers and acquisitions) is poised for a comeback this year and likely to remain a trend, as large players continue to favor buying solutions from diversified vendors in an increasingly fragmented market. Already in 2024, Zscaler acquired Avalor and CrowdStrike has announced it will acquire Flow Security, both of which were deals targeted at adding AI-first solutions in their portfolios.[23,24]

Conclusion: AI Can Be Fuel for Cybersecurity's Continued Growth

Generative AI poses new cybersecurity threats, but it's also helping companies create dynamic solutions that can thwart attacks. Major cybersecurity vendors are rapidly developing AI-powered tools to augment human analysts and automate security operations, and cloud providers are integrating generative AI into their cybersecurity stack. Despite economic headwinds, cybersecurity spending is projected to grow robustly, and industry consolidation is expected to continue as companies seek AI capabilities to enhance their product portfolios. In our view, these growth-oriented moves signal that there's an urgency to cybersecurity growth that investors may want to consider.

Related ETFs

BUG – Global X Cybersecurity ETFs

CLOU– Global X Cloud Computing ETF

AIQ – Global X Artificial Intelligence & Technology ETF

Click the fund name above to view current performance and holdings. Holdings are subject to change. Current and future holdings are subject to risk.

Footnotes

1. Gartner. (2023. September 28). Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024
2. Microsoft Security. (2024, March 08). Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard.
3. MSSPAlert. (2024, January 08). Top 10 Cyberattacks of 2023.
4. Ibid.
5. Ibid.
6. McKinsey. (2023, April 3). What is cybersecurity?
7. Gartner. (2023. September 28). Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024.
8. CISOMAG. (2020, September 12). “Psychology of Human Error” Could Help Businesses Prevent Security Breaches.
9. Okta Blog. (2023, September 15). What the GenAI paradigm shift means for Identity.
10. New Scientist. (2024, February 24). GPT-4 developer tool can hack websites without human help.
11. CBS News. (2023, February 23). JPMorgan Chase bars employees from using ChatGPT.
12. CrowdStrike Blog. (2023, May 30). Introducing Charlotte AI, CrowdStrike's Generative AI Security Analyst: Ushering in the Future of AI-Powered Cybersecurity.
13. Check Point Press Releases. (2024, Jan 30). Check Point Software Unveils Infinity AI Copilot: Transforming Cyber security with Intelligent GenAI Automation and Support.
14. Okta Blog. (2023, September 15). What the GenAI paradigm shift means for Identity.
15. Cybersecurity Dive. (2023, May 31). Palo Alto Networks teases plans for generative AI across security services.
16. Microsoft. (2024, March 13). Microsoft Copilot for Security is generally available on April 1, 2024, with new capabilities.
17. Ibid.
18. Ibid.
19. Google Cloud. (2023, August 29). New AI capabilities that can help address your security challenges.
20. Gartner. (2023. September 28). Gartner Forecasts Global Security and Risk Management Spending to Grow 14% in 2024.
21. Global X Estimates.
22. Markets and Markets. (2024, January 11). Artificial Intelligence in Cybersecurity.
23. Zscaler Blog. (2024, March 14). Zscaler acquires Avalor to unleash the power of enterprise security data with Avalor's Data Fabric for Security™ to bring real-time AI-driven security insights and threat prevention.
24. CrowdStrike. (2024, March 5). CrowdStrike to Acquire Flow Security to Expand Its Cloud Security Leadership with Data Security Posture Management (DSPM).

This material represents an assessment of the market environment at a specific point in time and is not intended to be a forecast of future events, or a guarantee of future results. This information is not intended to be individual or personalized investment advice and should not be used for trading purposes.

Shares of ETFs are bought and sold at market price (not NAV) and are not individually redeemed from the Fund. Brokerage commissions will reduce returns.

Investing involves risk, including the possible loss of principal. Cybersecurity Companies are subject to risks associated with additional regulatory oversight with regard to privacy/cybersecurity concerns. Declining or fluctuating subscription renewal rates for products/services or the loss or impairment of intellectual property rights could adversely affect profits. The investable universe of companies in which the Funds may invest may be limited. The companies in which the Funds invest may be subject to rapid changes in technology, intense competition, rapid obsolescence of products and services, loss of intellectual property protections, evolving industry standards and frequent new product productions, and changes in business cycles and government regulation.

International investments may involve the risk of capital loss from unfavorable fluctuation in currency values, from differences in generally accepted principles or from social, economic, or political instability in other nations. Emerging markets involve heightened risks related to the same factors as well as increased volatility and lower trading volume. The Funds are non-diversified.

Carefully consider the funds' investment objectives, risks, and charges and expenses before investing. This and other information can be found in the funds' full or summary prospectuses, which may be obtained at globalxetfs.com. Please read the prospectus carefully before investing.

Global X Management Company LLC serves as an advisor to Global X Funds. The Funds are distributed by SEI Investments Distribution Co. (SIDCO), which is not affiliated with Global X Management Company LLC or Mirae Asset Global Investments. Global X Funds are not sponsored, endorsed, issued, sold, or promoted by Indxx, nor does Indxx make any representation regarding the advisability of investing in the Global X Funds. Neither SIDCO, Global X nor Mirae Asset Global Investments are affiliated with Indxx.