GLOBAL X INSIGHTS

AI Does Not Kill Cybersecurity, It Enhances the Opportunity

Ido Caspi
icaspi@globalxetfs.com

Date: May 15, 2026
Topic: Thematic, Disruptive Technology

Recent advances in AI models have shown real potential to streamline cybersecurity functions like vulnerability discovery, attack triage, and automated response, raising concerns about sector-wide disruption. The concern is not unfounded, but we think the market is extrapolating too far. The functions AI could potentially disrupt account for only a fraction of the estimated $215 billion global cybersecurity market.[1] Meanwhile, AI is compounding the cybersecurity problem — expanding the attack surface enterprises must defend as copilots, agents, and model integrations introduce new data flows, access points, and surfaces for exposure.[2] At the same time, threat actors are harnessing the same AI capabilities, dramatically increasing the speed and scale of their attacks.

In our view, the choppiness and pullback in the cybersecurity theme so far in 2026 looks less like a structural breakdown and more like a mispriced narrative that may create opportunities for long-term investors.

Key Takeaways

- We believe the market is misreading AI as a threat to cybersecurity when, in our view, it is primarily a tailwind.
- Growing AI usage means more IT surface area that needs to be protected, more complexity to manage, and faster-moving attackers, which can help boost cybersecurity spending.
- Sentiment has driven the selloff more than fundamentals. Low valuations could mean a compelling entry point for long-term investors.

Why Cybersecurity Works in an AI World

AI has emerged as a new source of volatility for cybersecurity stocks, as investors increasingly question whether advancing capabilities could pressure parts of the security stack and erode long-standing business models. In Q1 2026, the Global X Cybersecurity ETF (BUG) returned -17.56%.[3]Volatility intensified following the April 2026 launch of Anthropic's Claude Mythos Preview, which was described as highly capable in computer security applications, and was only released to a select group of organizations to prevent broad misuse.[4]

The market reaction was swift and, we believe, imprecise. Here's why:

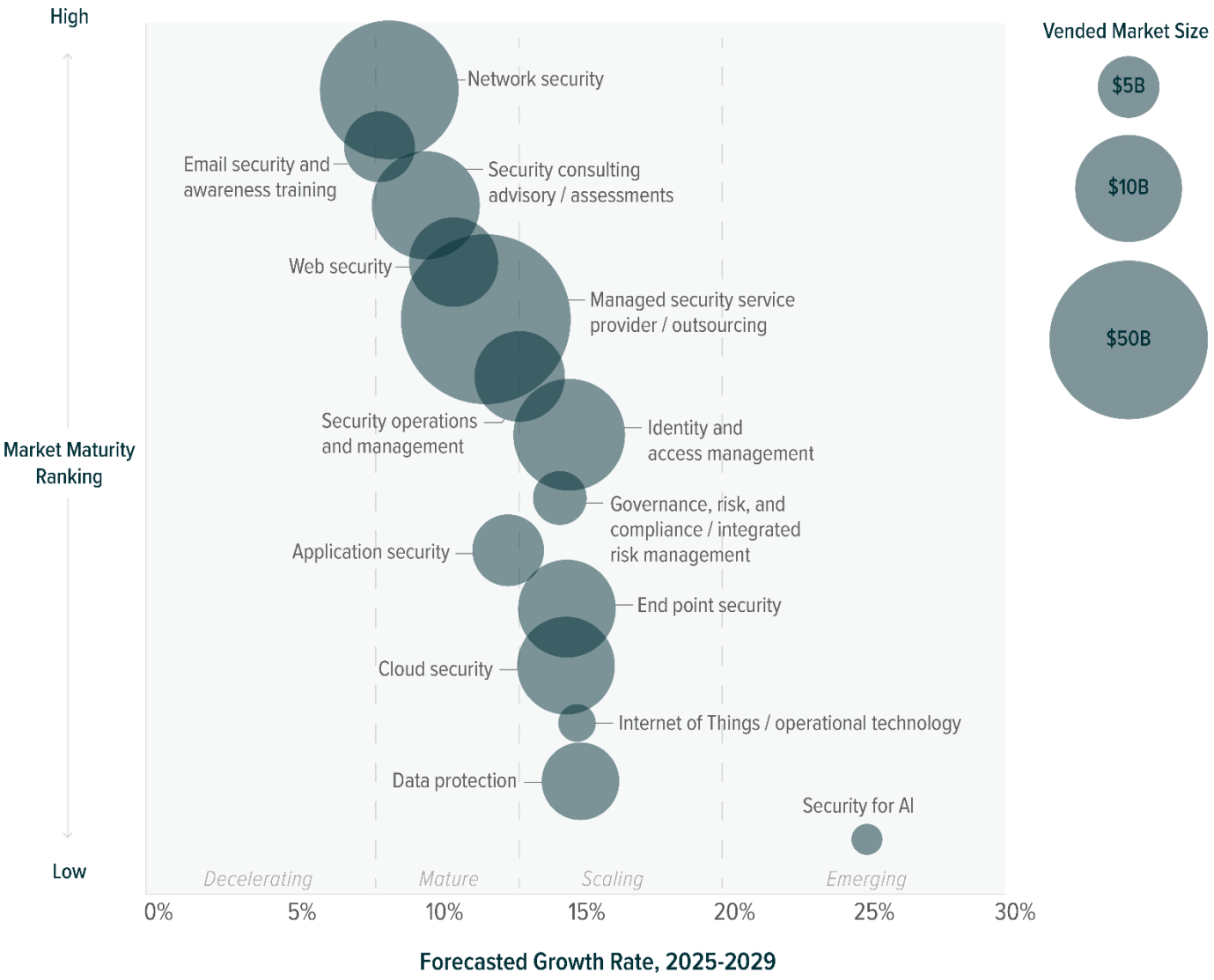
1. **AI does not replace cybersecurity**: Investor conclusion that the entire cybersecurity stack is at risk from AI is overly simplistic and premature. AI is best used today to improve and automate areas like vulnerability discovery, which is only a small part of the cyber market, roughly 7–8% in 2025 by our estimate.[5] Automated response, another automation-prone category, is even smaller at ~1%.[6] The fragmented and extensive core cyber stack, covering identity, endpoint, cloud, data, and network security, represents the bulk of modern security spending and is becoming more critical, not less, as AI increases complexity and accelerates threats. Moreover, parts of the cybersecurity market, such as firewalls, networking appliances, and data-center security infrastructure are physically anchored to enterprise and cloud buildouts and are set to grow alongside the rise of AI data centers.

2. **AI multiplies cybersecurity needs**: Cybersecurity spending has expanded alongside every major layer of technological complexity in the past: the shift to cloud, mobile, and the Software-as-a-Service (SaaS) proliferation. In our view, AI raises complexity faster than any of those transitions as it brings autonomous agency into the technology stack. Enterprises are deploying copilots, agents, and model APIs into environments that are already difficult to secure. As that happens, sensitive data moves across more systems, development cycles accelerate, and the security perimeter becomes more fluid, which is all likely to compel enterprises to keep security investments on the offensive. By 2029, agentic AI is expected to drive 15% of global cybersecurity budgets, nearly three times higher from current levels.[7] Threat actors are gaining the same AI capabilities, raising the speed and quality of attacks. The environment is getting harder, not easier, and spending will follow.

Performance quoted represents past performance. Past performance does not guarantee future results. The investment return and principal value of an investment will fluctuate so that an investor's shares, when sold or redeemed, may be worth more or less than their original cost and current performance may be lower or higher than the performance quoted. Click here for performance current to the most recent month-and quarter-end."

MARKET FRAGMENTATION: AI LIKELY COMPOUNDS CYBERSECURITY GROWTH ACROSS SEGMENTS

Cybersecurity Segment Market Maturity, Growth Rate, and Market Size



Source: McKinsey. (2026, March 24). Securing the agentic enterprise: Opportunities for cybersecurity providers.

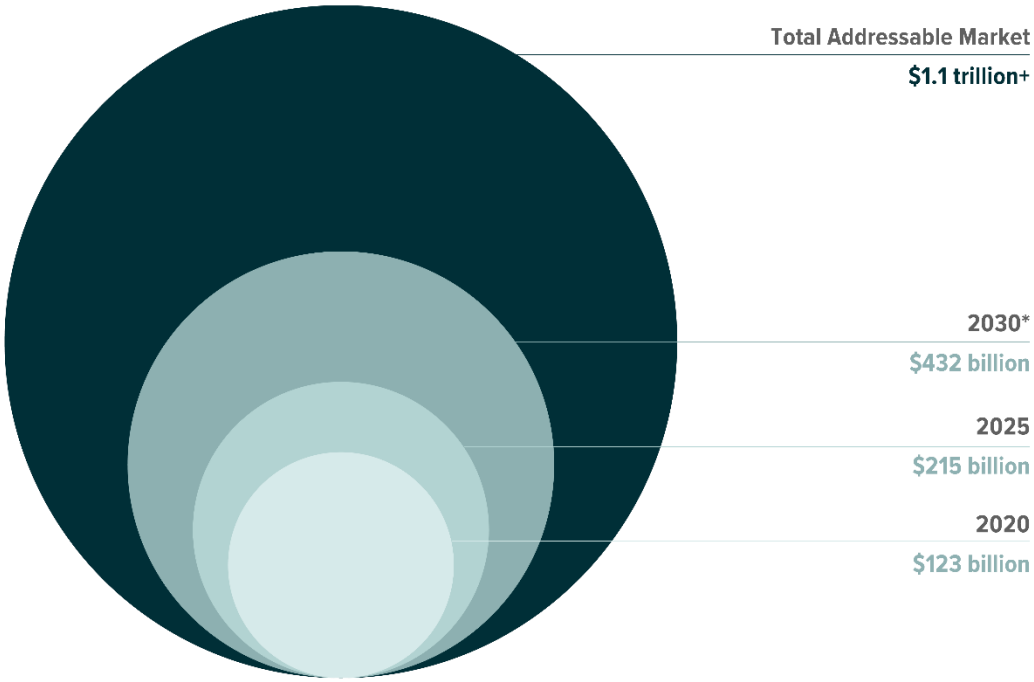
3. **Cybersecurity market is still early and compounding:** In 2026, the global cybersecurity market is projected to grow over 12.5% year-over-year to reach $240 billion, outpacing global IT spending growth by roughly two percentage points.[8,9] Yet cybersecurity still represents only ~4% of total IT spend, and a tiny fraction of the $18 trillion global digital economy, leaving substantial runway ahead.[10,11] At the same time, the weaponization of AI and explosion in data creation make cybersecurity increasingly non-discretionary. Reflecting this shift, CIOs ranked cybersecurity and risk management as the top priority for the next year.[12]

4. **Pure-play cybersecurity platforms should gain share as AI reshapes the market**: Contrary to market's fear, AI is more likely to strengthen scaled cybersecurity platforms than displace them. These leaders such as Palo Alto Networks or CrowdStrike have deep distribution, implementation capabilities, and product breadth to embed AI into existing workflows. They're also well placed to serve as channels for model developers to bring AI into enterprise use cases. In our view, that is likely why Anthropic works with cybersecurity firms to test Mythos, instead of seeking to replace them.[13] While AI may pressure narrow point solutions, the risk of replacing core security platforms with untested new solutions is simply untenable in today's environment.

5. **Current valuation creates attractive entry point:** Cybersecurity fundamentals appear stronger than recent share price action suggests. Earnings have continued to grow, while the actual revenue impact from AI disruption remains limited so far. At ~21.1x forward earnings, the Global X Cybersecurity ETF (BUG) trades at one of its lowest multiples relative to the S&P 500 since the fund's inception, creating an attractive set up for seeking a theme with durable growth.[14]

TOTAL ADDRESSABLE MARKET FOR CYBERSECURITY

Global Cybersecurity Market



*Forecast
Source: Global X ETFs forecast as of November 2025, with information derived from Gartner. (2025, July 29). Gartner Forecasts Worldwide End-User Spending on Information Security to Total $213 Billion in 2025.

Conclusion: Cybersecurity Becomes More Important as AI Scales

We believe the market is overestimating AI's disruptive impact on cybersecurity while underappreciating its role as a long-term demand driver. Rather than displacing the sector, AI is increasing broad technological complexity, expanding the attack surface, and reinforcing the need for comprehensive, platform-based security solutions. Against this backdrop, we believe recent volatility has created a more attractive entry point into a sector where the long-term demand drivers remain intact.

Related ETFs

BUG - Global X Cybersecurity 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.

Glossary:

Forward Earnings: A company's expected future profits (usually over the next 12 months) based on analyst estimates.

Footnotes

1. Global X ETFs forecast with info derived from: Gartner. (2025, July 29). Gartner Forecasts Worldwide End-User Spending on Information Security to Total $213 Billion in 2025.
2. McKinsey. (2026, March 24). Securing the agentic enterprise: Opportunities for cybersecurity providers.
3. FactSet Research Systems. (n.d.). Data accessed on May 4, 2026. Returns represent market price returns.
4. Anthropic. (2026, April 7). Project Glasswing.
5. Global X ETFs estimates with info derived from: MarketsandMarkets. (2026, April 3). Cybersecurity Market Surges to $351.92 billion by 2030 | CAGR 9.1%.
6. Mordor Intelligence. (n.d.). 2025 SOAR Market Share and Analysis. Accessed on May 4, 2026.
7. McKinsey. (2026, March 24). Securing the agentic enterprise: Opportunities for cybersecurity providers.
8. Gartner. (2025, July 29). Gartner Forecasts Worldwide End-User Spending on Information Security to Total $213 Billion in 2025.
9. Gartner. (2026, February 3). Gartner Forecasts Worldwide IT Spending to Grow 10.8% in 2026, Totaling $6.15 Trillion.
10. Ibid.
11. Global X ETFs with information derived from: IDCA.Org. (2025). Global Digital Economy Report (2025).
12. Gartner. 2026 CIO Leadership Perspectives.
13. Palo Alto Networks. (2026, April 17). Defender's Guide to the Frontier AI Impact on Cybersecurity.
14. ETFAction. Data as of May 1st, 2026. BUG's inception date was October 25th, 2019.

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. Please consult a financial advisor for more information regarding your investment situation.

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 BUG may invest may be limited. The Fund invests in securities of companies engaged in Information Technology, which can be affected by rapid product obsolescence and intense industry competition. 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. BUG is non-diversified.

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.

Carefully consider the fund's investment objectives, risks, and charges and expenses before investing. This and other information can be found in the fund's 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.