Beating broad benchmarks in 2025 with cybersecurity

Published 16 June 2025

Elvira Kuramshina
Associate Director, Quantitative Research

Key Takeaways

- Cybersecurity demand remains resilient in a volatile 2025, supported by digitalisation, geopolitical tensions, and AI risks.
- Despite macro headwinds like tariffs and rates, cybersecurity is still seen as essential infrastructure—reflected in recent index performance rebounds.
- WisdomTree's Team8 Cybersecurity UCITS Index offers targeted, differentiated exposure beyond what traditional benchmarks provide.

2025 has been vigorously testing investors' patience. From tariff-induced uncertainty to rising geopolitical risks and accelerating proliferation of AI, markets have experienced significant turbulence and volatility. Against this challenging backdrop cybersecurity-focused strategies stand out with their year-to-date outperformance vs. broad tech and equity benchmarks highlighting resilience of cybersecurity demand despite a weakening macroeconomic environment and shifting corporate priorities and spending. In this blog, we delve into the resilience of cybersecurity's long-term demand, highlight short-term headwinds from macro uncertainty and, finally, discuss how a satellite allocation to cybersecurity can potentially boost your portfolio's returns beyond the return of broad benchmarks.

Resilience of cybersecurity demand

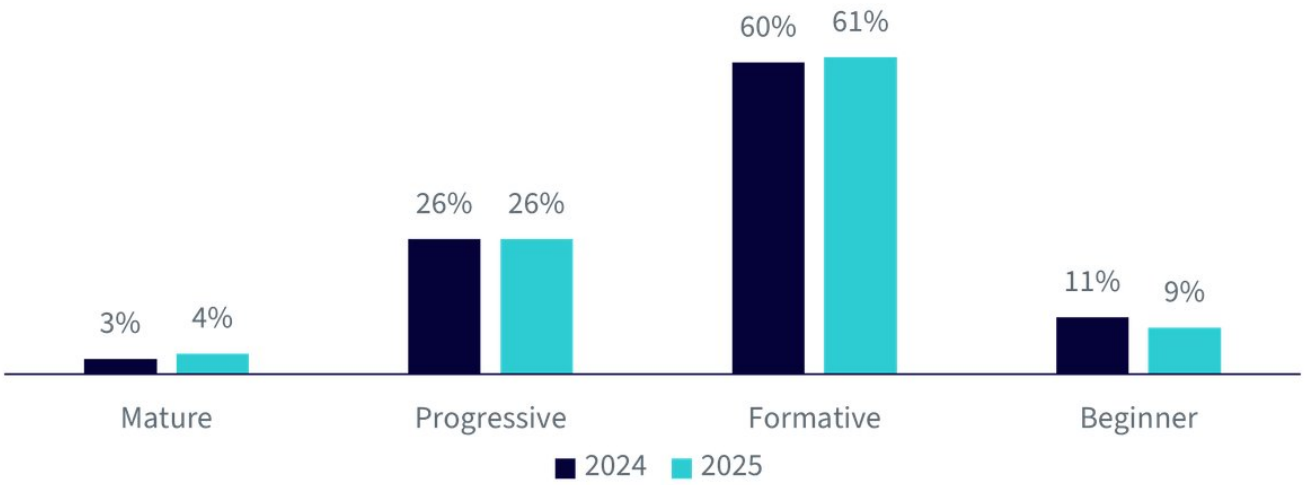
As the world continues to become increasingly digital, cybersecurity is turning into the key megatrend to safeguard our future. But alongside the ongoing wave of digitalisation, cybersecurity's growth potential is being further reinforced by multiple tailwinds:

1. Redefined business and competitive resilience

The digitalisation that was super-charged by the global pandemic received another boost with the unfolding AI revolution. But every new layer of digital infrastructure requires robust security measures, and, in the modern digital age, cybersecurity becomes a matter of business resilience. A recent cyber incident at Marks & Spencer, one of the UK's biggest retailers, is an example of how crippling and costly a cyber-attack can be in modern realities. The company estimates a $300mn hit in its profits and the disruption in its online operations to last until July[1].

This incident highlights the critical nature of adequate cybersecurity solutions for any modern business and explains why demand for cybersecurity solutions is staying robust even during periods of economic turbulence. At the same time, Cisco, in its 2025 Cybersecurity Readiness Index, reports that companies are not keeping up with the evolving threat landscape with only 30% of companies showing a 'mature' or 'progressive' state of readiness to face today's cybersecurity risks and almost flat dynamics from 2024 (see Figure 2). This, in turn, demonstrates future growth potential for cybersecurity companies, as businesses looking to step up their competitive resilience will start ramping up their cybersecurity spending. For example, companies with adequate cybersecurity solutions can create a trust-based competitive moat and safely adopt new technologies for staying ahead competitively.

Figure 1. Global readiness to face cybersecurity risks



Source: 2025 Cisco Cybersecurity Readiness Index. 2025 Cisco Cybersecurity Readiness Index assesses how ready companies are to face today's cybersecurity risks based on 5 pillars: Identity Intelligence, Machine Trustworthiness, Network Resilience, Cloud Reinforcement, and Artificial Intelligence (AI) Fortification. The assessment is based on a double-blind survey of 8,000 businesses and cybersecurity leaders across 30 global markets and a broad range of private sector industries.

2. Geopolitical risks and policy tailwinds

In addition, the concurrent rise in geopolitical tensions and high-profile cyberattacks has kept cybersecurity top of mind not just for businesses, but also for governments. The rapidly evolving threat landscape, that includes state actors, led to a wave of regulatory and strategic responses that are reinforcing long-term demand for cybersecurity solutions. In the US, the National Cybersecurity Strategy (2023) emphasised the urgency of adopting a more intentional and coordinated approach to cyber defence, as well as the realignment of incentives to support long-term strategic investments in cyberspace. In Europe, the EU's Cyber Solidarity Act seeks to bolster collective preparedness, detection and response through funding under the strategic objective 'Cybersecurity' and joint preparedness actions, situational awareness and cross-border cooperation. Meanwhile, NATO is also increasing its focus on collective cyber defence and adapting its defence posture as a response to the rapidly evolving threat landscape.

3. Proliferation of generative AI

From the release of ChatGPT on 30 November 2022, generative AI took the world by storm. While AI technology unlocks innovative capabilities for cybersecurity companies, such as automating threat detection and enhancing data analytics, it also creates new vulnerabilities and fuels innovations in the threat landscape. With rapid proliferation and advancements, the technology has been one of the main catalysts in the surge of cyberattacks. From malicious tools to generate deepfakes for impersonation and social engineering to large language model (LLM) data poisoning and jailbreaking of LLMs to enhance malware creation, threat actors have been leveraging AI to become more efficient, prolific and fast in accomplishing their goals.

At the same time, organisations are experiencing heightened risks of data leakage due to use of AI models. Check Point in its inaugural "AI Security Report 2025" reports that 1 in 13 gen AI prompts contains sensitive or private details and 1 in every 80 prompts exposes sensitive data to attackers. At the same time, Check Point highlighted that companies not using AI might find their employees leveraging AI tools without permission leading to further risks. As a response, a range of cybersecurity companies have already started offering solutions tailored specifically to risks stemming from the business use of LLMs. As AI-powered cyber threats become more and more prevalent, the demand for cybersecurity solutions is poised to increase in lockstep.

Short-term macro headwinds

Despite strong underlying demand and compelling future growth potential, cybersecurity companies are not immune to broader macroeconomic turbulence. In fact, they often represent longer-duration tech equities in terms of sensitivity to interest rate expectations. This is primarily because many leading cybersecurity firms are growing rapidly, with much of their expected cash flows projected into the future. As interest rates rise, these future cash flows are discounted more heavily, making valuations more susceptible to changes in interest rate expectations.

Recent monetary policy developments in the US, amid macroeconomic uncertainty triggered by tariff announcements, have led to increased market volatility and a re-pricing of expectations for future interest rate cuts that kickstarted by the release of January's Federal Open Market Committee (FOMC) meeting minutes. Tariff-related uncertainty has contributed to markets pricing in higher recession risks, especially against the backdrop of a slowing economy and the Fed's preference to hold rates steady rather than risk cutting too soon.

Planned tariffs have contributed to greater volatility and reduced corporate spending confidence. In this climate, cybersecurity might see slower deal closures as companies weigh the near-term outlook. Another way that US tariffs might affect cybersecurity companies is through their hardware appliances, e.g. firewalls, secure routers, intrusion detection/prevention systems (IDS/IPS). Some companies might bundle their software with third party hardware and be affected through their partners. Software-focused cybersecurity companies are better positioned in this environment, but they might be also exposed to tariffs

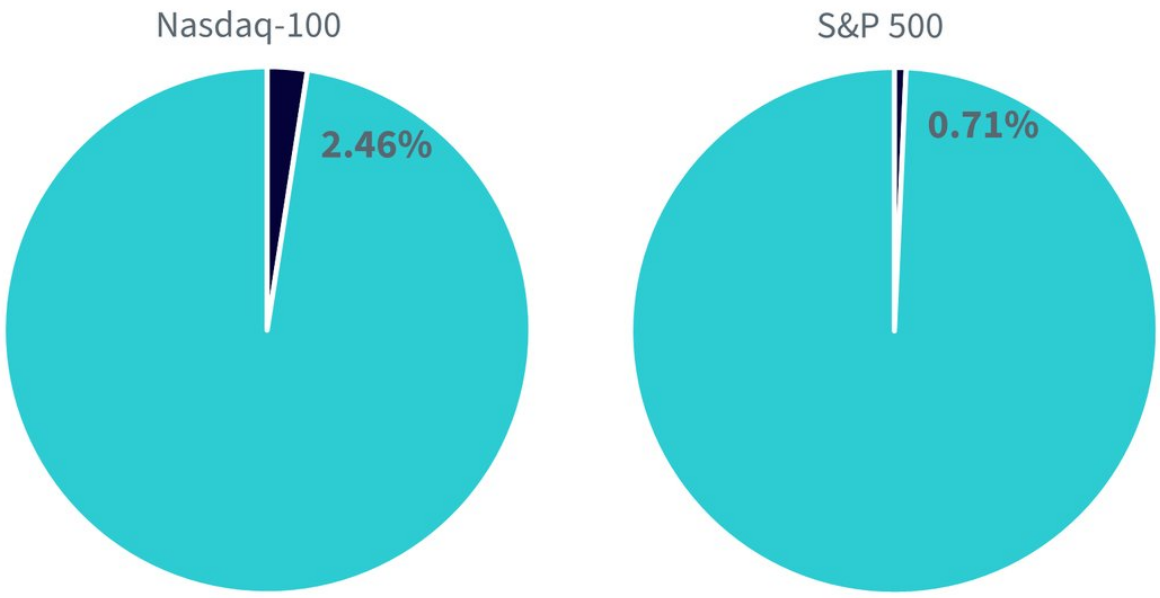
indirectly. Cloud-based services rely on physical data centre hardware and public cloud providers might raise prices if they are affected by increased costs.

While interest rate and tariff concerns could pressure near-term spending, secular tailwinds, from rapid digitalisation and AI proliferation to evolving geopolitical threats, provide a durable foundation for sustained investment in cybersecurity, keeping the long-term growth proposition intact.

A compelling satellite to a long-term core

One of the key value propositions of thematic strategies is differentiation that they offer vs. broad equity exposures. This differentiation potential might vary from theme to theme. When it comes to cybersecurity companies, the exposure that investors can gain to the theme via broad equity or tech benchmarks is minimal especially due to low weight of those companies within broad benchmarks. For example, Palo Alto and CrowdStrike being one of the largest pure-play cybersecurity companies by market capitalisation have only 0.79% and 0.68% weight in the Nasdaq-100 as of 30 May 2025. If we look at the overlap between the WisdomTree Team8 Cybersecurity UCITS Index that currently comprises 25 cybersecurity companies, it has less than 2.5% and less than 1% overlap with the Nasdaq-100 and the S&P 500 respectively (see Figure 3).

Figure 2. Overlap between WisdomTree Team8 Cybersecurity UCITS Index and broad tech and equity benchmarks



Source: WisdomTree, Bloomberg, MSCI. As of 30 May 2025. WisdomTree Cybersecurity is represented by the WisdomTree Team8 Cybersecurity UCITS Index (WTCBRUN). Nasdaq-100 is the NASDAQ 100 Index. S&P 500 is the S&P 500 Index. Overlap of common securities is the sum of all overlapping weights with WTCBRUN within a given index. Overlapping weight is computed as the lower weight of a security that is held both in WTCBRUN and a given index. **You cannot invest directly in an index. Historical performance is not an indication of future performance and any investments may go down in value.**

Low overlap suggests that adding this type of exposure to your core tech or core equity allocation has the potential to enhance returns through diversification benefits. In addition, the resilience of cybersecurity demand further makes a cybersecurity strategy a compelling long-term investment alongside the traditional core exposures.

[1] https://www.bbc.co.uk/news/articles/c93llkg4n51o

Important Risks Related to this Article

Important Information

Marketing communications issued in the European Economic Area ("EEA"): This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

Marketing communications issued in jurisdictions outside of the EEA: This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as "WisdomTree" (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

For professional clients only. The information contained in this document is for your general information only and is neither an offer for sale nor a solicitation of an offer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and affer seeking independent investment, tax and legal advice.

The application of regulations and tax laws can offen lead to a number of different interpretations. Any views or opinions expressed in this communication represent the views of WisdomTree and should not be construed as regulatory, tax or legal advice. WisdomTree makes no warranty or representation as to the accuracy of any of the views or opinions expressed in this communication. Any decision to invest should be based on the information contained in the appropriate prospectus and affer seeking independent investment, tax and legal advice.

This document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public offering of shares or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any affiliate, nor any of their respective officers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.