Evolving WisdomTree Cybersecurity for the AI era

Published 26 October 2026

Elvira Kuramshina
Associate Director, Quantitative Research

Key Takeaways

- A new era of cyber risk: Generative AI has already changed the economics of cybercrime, and frontier AI models are now opening a new phase of risk and demand. We have evolved the WisdomTree Team8 Cybersecurity UCITS Index methodology to reflect this change.
- AI is reshaping what needs to be secured: As AI creates new attack surfaces and new categories of security spend, the sources of cybersecurity growth are shifting, and the way companies are selected and weighted needs to follow.
- Three updates to the methodology: an enhanced, multi-signal Focus Score, a forward-looking Growth Score and a transparent, modular weighting formula, all built to capture the cybersecurity opportunity in the AI era.
- Same foundations, sharper tilts: the starting universe, core framework and expert partner, Team8, are unchanged, while portfolio weights shift towards companies with stronger cybersecurity positioning and growth profiles.
- Cybersecurity as a foundational layer: as AI becomes embedded across the digital economy, the index is designed to keep pace with the areas of strongest demand.

Cybersecurity has always been a race between attackers and defenders, and artificial intelligence (AI) is changing the pace of that race. Over the last few years, generative AI has already redefined the economics of cybercrime, making attacks faster and more numerous while giving defenders more powerful tools to detect and respond. Now, advances in frontier AI models are ushering in a new era. As AI spreads across enterprise systems, it is creating new things to protect, from models and training data to autonomous agents and machine identities. The opportunity is still cybersecurity, but the sources of growth and differentiation within it are shifting. Together with our expert partner, Team 8, we explore what these changes mean for the sector.

In recent years, the industry has been shaped by cloud-native, identity-centric and AI-enabled security. Today, it is moving toward an environment increasingly defined by frontier-model capabilities, autonomous agents, machine identities and new attack surfaces, with AI systems themselves needing dedicated

protection. Capturing this transition requires an approach that reacts to where AI is creating the strongest future demand. Our methodology response is updated signals driven by deeper expert insights for selecting and weighting companies, while keeping the same universe and the same core framework.

Why the cyber opportunity is changing

The cyber threat landscape is intensifying on several fronts at once. CrowdStrike's 2026 Global Threat Report found that in the fastest case, an eCrime intruder moved from initial access to lateral movement in only 27 seconds, a reminder of how little room for error defenders can have. The attacker pool is also expanding, with the number of active ransomware groups up 49% year on year. Meanwhile, the bill for failure keeps rising. IBM estimates the global average cost of a data breach at $4.99 million.

AI is now shaping both sides of the contest. On one hand, it has opened up a new attack surface. Check Point's research found that roughly one in 80 generative AI prompts puts sensitive data at risk, while IBM puts the average cost of a breach involving an AI model inversion attack at around $6 million. On the other hand, AI is proving to be a strong asset for defenders. IBM's analysis suggests that organisations using AI and automation extensively in their security operations save an average of $1.93 million per breach. This duality is giving rise to a distinct category of security spending, focused on protecting models, training data, autonomous agents and machine identities. Nothing illustrates this shift better than the recent arrival of frontier models with advanced cyber capabilities.

Figure 1: AI is turning into a new attack surface and a new tool for both cyber criminals and cyber defenders

At >90 organisations	**1 in 80 of GenAI prompts**	**$6 million**
Adversaries exploited legitimate GenAI tools by injecting malicious prompts to generate commands for stealing credentials and cryptocurrency (CrowdStrike)	Expose sensitive data to attackers (Check Point)	The global average breach cost of an AI model inversion attack, reflecting the growing difficulty of protecting training data and sensitive information (IBM)

56%	**7.5% of GenAI prompts**	**$1.93 million**
Increase in AI-driven attacks, led by AI deepfake impersonations and AI-enabled malware (IBM)	Include sensitive or private details (Check Point)	Cost savings from extensive use of AI and automation in security, compared to organizations using none (IBM)

Source: CrowdStrike, "Global Threat Report" published February 2026. IBM, "X-Force Threat Intelligence Index 2026". IBM, "Cost of a Data Breach Report 2026". Check Point, "AI Security Report 2025".

The gated release of Anthropic's Claude Mythos Preview, and the Project Glasswing initiative that followed with around 50 partners, marked a turning point, demonstrating a new level of frontier AI capability in finding vulnerabilities at scale. In just one month, partners uncovered more than 10,000 high- or

critical-severity vulnerabilities. The UK's AI Security Institute, which assessed Mythos Preview in April 2026, described these capabilities as dual use: they create real security challenges but also offer the potential for step-change improvements in defence. With more capable models to come, it argued that investing in cyber defence now is vital.

Introducing the methodology response

The methodology response to the changing cybersecurity opportunity comes down to three updates: an enhanced, multi-signal Focus Score; a forward-looking Growth Score; and a transparent, modular weighting formula. Together, they aim to capture where cybersecurity demand is heading, and which companies are expected to be better positioned to benefit.

An enhanced, multi-signal Focus Score

Focus Score = Cybersecurity Breadth + Product Leadership + Priority Themes

Previously, the Focus Score rested on a single signal: whether a company was classified as Broad or Narrow Focus. It is now driven by three complementary and interpretable signals, which are added together. Each captures a different dimension of a company's cybersecurity positioning:

- **Cybersecurity Breadth (40%)** rewards companies that can participate in demand across many areas of the market, rather than relying on a narrow set of solutions. A company qualifies as Broad Focus when it has high exposure to at least half of the cybersecurity development themes. Narrow Focus companies, which have high exposure to at least one theme, remain eligible, so specialists are still part of the opportunity set.
- **Product Leadership (30%)** recognises depth as well as breadth. Team8 evaluates cybersecurity products within specific solution categories and flags companies whose products lead their field, even where the overall product footprint is narrower. This lets the strategy allocate to companies positioned to capture emerging demand through differentiated capabilities.
- **Priority Themes (20% or 30%)** tilt towards the areas where cybersecurity demand is expected to accelerate. A company earns 20% if at least half of its exposure sits in these themes, and 30% if it is also a product leader. The current Priority Themes are **AI Security**, which covers solutions that protect AI systems themselves; **Smarter Security**, which uses AI and automation to make security responses faster and more adaptive; and **Perimeterless World**, which focuses on identities and access, increasingly critical as AI agents create a growing universe of machine identities. These themes are not fixed and can change as technology and threat vectors evolve.

A forward-looking Growth Score

The updated Growth Score measures how well a company is expected to monetise cybersecurity demand, using estimated revenue growth as the signal. It looks ahead wherever reliable data allows, following a simple order of preference: the estimated two-year revenue compound annual growth rate (CAGR) comes

first, then the one-year estimate if no two-year figure is available, and then actual trailing twelve-month growth if fewer than five analysts are contributing to estimates.

Companies are then ranked against the rest of the eligible cybersecurity universe, not against fixed growth hurdles, so the thresholds adapt to market conditions and to the pace of the cyber cycle. The bottom 20% are excluded, and the remaining companies fall into four groups, each with its own weight factor:

- **Growing Fast & Scale (1.5x):** faster-growing companies with trailing sales within the top 10 of the faster-growing group and above the universe median. The group is capped at 10 companies.
- **Growing Fast (1.2x):** companies with growth above the median of the universe.
- **Growing (1x):** companies with growth at or below the median.
- **Growing & Decelerating (0.8x):** companies in the bottom 40% by growth score whose recent growth is running ahead of what analysts estimate, a sign that momentum is slowing.

One transparent weighting formula

Final weight = equal weight × Focus factor × Growth factor

Every company starts from an equal weight. That starting weight is then multiplied by two factors, one from the Focus Score and one from the Growth Score, and the results are rescaled so the portfolio adds up to 100%:

The **Focus factor** is 1 plus the company's Focus Score. Each of the three signals adds its own bonus: up to 40% for breadth, 30% for product leadership and 20% or 30% for priority theme exposure. A company can therefore be overweighted by up to 100% before the Growth factor is applied.

The **Growth factor** then adjusts the weight according to the company's growth group, from an overweight for Growing Fast & Scale companies to an underweight for Growing & Decelerating ones.

The approach is transparent because each tilt can be traced to a specific signal, and modular because the Focus and Growth factors work independently and can be understood on their own. Weights are also subject to the index's concentration, liquidity and market capitalisation rules, which keep the portfolio diversified and investable.

Portfolio continuity at the core

To demonstrate how the updated methodology looks vs the old portfolio, we compare the target portfolio for the October 2026 rebalance, built under the new rules, with the previous index weights set in March 2026.

The core of the portfolio remains similar. Seven of the ten largest holdings in the new portfolio were also

among the ten largest in March, and the top three, CrowdStrike, Palo Alto Networks and Fortinet, each carry the same weight of 7.68%. The top ten together account for 58.99% of the portfolio.

Figure 2: Top 10 in the enhanced strategy following the October 2026 rebalance

Company name	Weight	Growth Classification	Focus Weight factor
CrowdStrike Holdings, Inc.	7.68%	Growing Fast & Scale	2.00
Palo Alto Networks, Inc.	7.68%	Growing Fast & Scale	2.00
Fortinet, Inc.	7.68%	Growing Fast & Scale	2.00
Zscaler, Inc.	6.15%	Growing Fast & Scale	1.60
Rubrik, Inc.	6.15%	Growing Fast & Scale	1.60
Varonis Systems, Inc.	4.92%	Growing Fast	1.60
Netskope, Inc.	4.92%	Growing Fast	1.60
Cloudflare, Inc.	4.61%	Growing Fast & Scale	1.20
Datadog, Inc.	4.61%	Growing Fast & Scale	1.20
Elastic NV	4.61%	Growing Fast & Scale	1.20
Top 10 total	**58.99%**		

Source: WisdomTree. Based on the target holding prepared for the rebalance of the WisdomTree Team8 Cybersecurity UCITS Index after the Market close on 23 October 2026. **You cannot invest directly in an index. Historical performance is not an indication of future performance and any investments may go down in value.**

The bigger change is in how weight is distributed. The new portfolio gives more weight to companies with stronger cybersecurity positioning, with larger shares in all three Focus Score groups, most notably Product Leadership and Priority Themes. On the growth side, more weight sits in Growing Fast & Scale companies, and no weight remains in the bottom 20% of the universe by Growth Score.

Figure 3: Comparison of the new and the old strategy by Focus and Growth groups

Groups	New WCBR weight	Old WCBR weight
Focus Score		
Cybersecurity Breadth	27.14%	24.33%

Product Leadership	56.54%	49.03%
Priority Themes	84.19%	76.42%
Growth Score		
Growing Fast & Scale	49.16%	41.82%
Growing Fast	25.03%	25.50%
Growing	9.01%	20.54%
Growing & Decelerating	16.80%	7.99%
Bottom 20%	0%	4.15%

Source: WisdomTree. New WCBR weights are based on the target holdings prepared for the rebalance of the WisdomTree Team8 Cybersecurity UCITS Index after the Market close on 23 October 2026. Old WCBR weights represent target weights set for the rebalance in March 2026. **You cannot invest directly in an index. Historical performance is not an indication of future performance and any investments may go down in value.**

Bottom line

Cybersecurity is becoming a foundational layer of the digital and AI economy, and the demand it generates is being reshaped by frontier AI. The updated methodology retains the existing universe, core framework and expert partner, while refining how companies are selected and weighted to follow where the demand is heading.

Team8 Disclaimer: This Article represents the opinions of Team8 Labs Inc. (“Team8”) and is for informational purposes only. You should not treat any opinion expressed by Team8 as a specific inducement to make an investment in any security, but only as an expression of Team8’s opinions. Team8’s statements and opinions are subject to change without notice. Team8 is not registered as an investment adviser under the Investment Advisers Act of 1940, as amended (the “Advisers Act”), and relies upon the “publishers’ exclusion” from the definition of investment adviser under Section 202(a)(11) of the Advisers Act. As such, the information contained in this Article does not take into account any particular investment objectives, financial situation or needs and is not intended to be, and should not be construed in any manner whatsoever as, personalized investment advice. The information in this Article is provided for informational and discussion purposes only and is not intended to be, and shall not be regarded or construed as, a recommendation for a transaction or investment or financial, tax, investment or other advice of any kind by Team8. You should determine on your own whether you agree with the information contained in this Article. Certain of the securities referenced in this Article may currently, or from time to time, be constituents of an index developed and maintained by WisdomTree Investments, Inc. using data provided by Team8, which has been or will be licensed for a fee to one or more investment funds. In addition, certain officers or employees of Team8 or funds or other persons or entities affiliated or associated with Team8 may hold

shares of, be officers or directors of, or otherwise be associated with some or all of the issuers of the securities referenced in this Article or included in such index. Team8 expressly disclaims all liability with respect to any act or omission taken based on, and makes no warranty or representation regarding, any of the information included in this Article.

Important Information

This material is prepared by WisdomTree and its affiliates and is not intended to be relied upon as a forecast, research or investment advice, and is not a recommendation, offer or solicitation to buy or sell any securities or to adopt any investment strategy. The opinions expressed are as of the date of production and may change as subsequent conditions vary. The information and opinions contained in this material are derived from proprietary and non-proprietary sources. As such, no warranty of accuracy or reliability is given and no responsibility arising in any other way for errors and omissions (including responsibility to any person by reason of negligence) is accepted by WisdomTree, nor any affiliate, nor any of their officers, employees or agents. Reliance upon information in this material is at the sole discretion of the reader**. Past performance is not a reliable indicator of future performance.**