‘AI Security’ Emerges as the Next Cybersecurity Theme

Published April 6, 2026

Christopher Gannatti, CFA
Global Head of Research

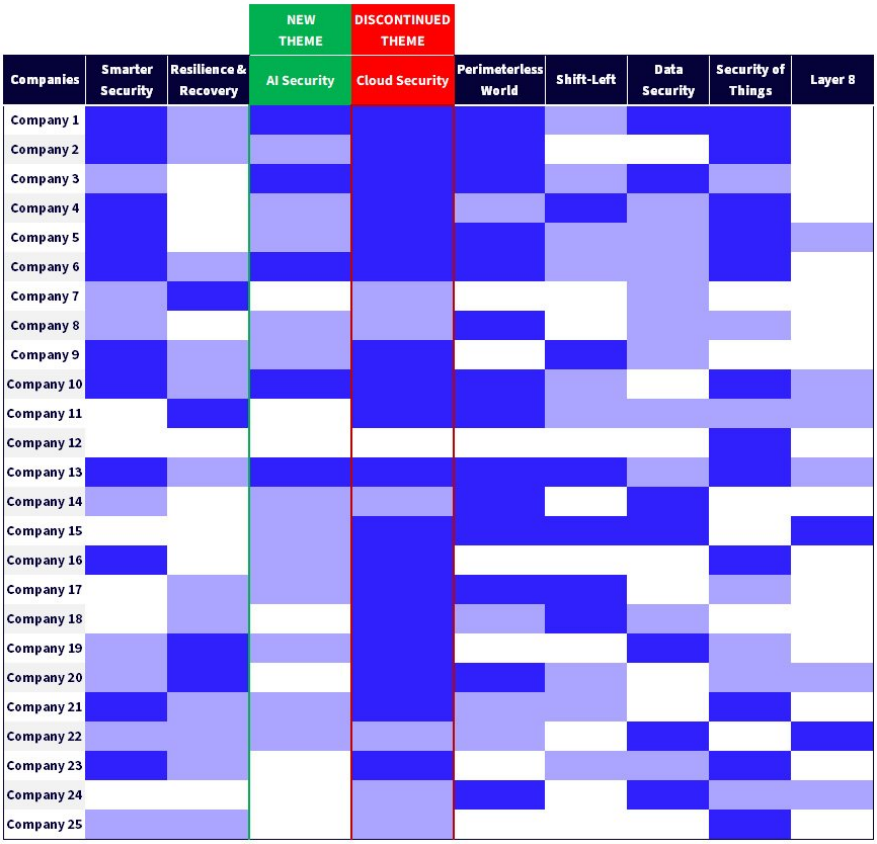
Elvira Kuramshina
Associate Director, Quantitative Research

Key Takeaways

- The WisdomTree Team8 Cybersecurity Index dynamically evolves its key cyber themes to remain aligned with structural shifts in the cybersecurity landscape.
- Cloud security is no longer a differentiator, as capabilities are now embedded across most cybersecurity platforms.
- The Cloud Security theme is retired to better reflect the maturity and ubiquity of cloud protection.
- AI adoption is creating new attack surfaces, including model manipulation, data poisoning, and sensitive data leakage.
- AI Security is emerging as a distinct, high-growth category, driven by new risks and specialized solutions.

This is not the first time we have made adjustments; for example, in 2023 we introduced the Layer 8 theme focused on human risk. Today, to reflect the latest developments in the cybersecurity landscape – particularly the maturation of cloud security and the rapid rise of artificial intelligence—we have once again made updates to the index’s key cybersecurity themes (Figure 1a and Figure 1b).

Figure 1a: Exposure of Companies across Cyber Themes in the WisdomTree Team8 Cybersecurity Index



Source: WisdomTree, Team8. Exposure to each theme is presented from darker blue (high exposure) to white (no product in the space). The presented classification became effective after the close on March 20, 2026.

Figure 1b: Description of Cyber Themes in the WisdomTree Team8 Cybersecurity Index

Cyber Theme	Rationale
Smarter Security	Response capacity is stretched to its limits as organizations face immense security complexity – dozens of products that aren't integrated, an expanding enterprise network, a cyber talent shortage, and an adversary leveraging increasingly sophisticated capabilities. Smarter security can plug the gaps.
Resilience & Recovery	Digital infrastructure is now business critical, and therefore recovery from cyberattacks is now a core tenet of risk mitigation and business continuity. Any sound security strategy necessitates capabilities that enable rapid recovery and reconstitution of assets and capabilities.
Cloud Security	**DISCONTINUED THEME**
AI Security	**NEW THEME**
Perimeterless World	The enterprise perimeter is nearly extinct and the shift to remote work during the pandemic is accelerating its demise. Identity and zero trust architectures will become increasingly important in governing access management.
Shift-Left	Developing and managing software is becoming more agile and faster than ever. Security can't come after the fact, but needs to be shifted-left to the developers, embedding security considerations from the start in a DevSecOps model.
Data Security	Globalization and growth of the digital economy are colliding with emerging privacy regulations and consumer preferences, providing users with more control over their data. Architectural design and business processes must accommodate new privacy- and zero trust-driven strategies.
Security of Things	IoT device connectivity unlocks new business value in the industrial economy. But as IT networks and operational technology (OT) networks converge, the attack surface expands, and adversaries can move from stealing data to threatening health and safety.
Layer 8	No matter how much money a company invests in security controls, humans will always defeat them. Layer 8 is all about how we train humans, how we empower them, how we monitor them, or in certain instances, how we take them out of the loop.

Source: Team8, WisdomTree.

Retiring the Cloud Security Theme

The Cloud Security theme was originally designed to capture companies focused on protecting cloud infrastructure and environments. This included technologies such as Cloud Workload Protection Platforms (CWPP), Cloud Infrastructure Entitlement Management (CIEM), Cloud Security Posture Management (CSPM), SaaS Security Posture Management (SSPM), Cloud-Native Application Protection Platforms (CNAPP), Container Security, and Cloud Access Security Brokers (CASB).

However, as cloud adoption has become universal across enterprises, cloud security capabilities have also become widely embedded across the cybersecurity landscape. Today, most cybersecurity vendors offer products that address cloud environments in some capacity. As a result, in our view, cloud security is no longer a meaningful differentiator between cybersecurity vendors, nor does it serve as a strong proxy for identifying companies aligned with emerging cybersecurity growth themes. Reflecting this shift, the Cloud Security theme is being retired as a distinct category within the index.

While the Cloud Security theme is being discontinued, the index introduces AI Security as the next cybersecurity theme, driven by the rapid adoption of AI systems, the expansion of the AI attack surface, and the emergence of specialized AI security solutions.

Introducing AI Security as a Distinct Cybersecurity Theme

Artificial intelligence is rapidly becoming embedded across enterprise software, infrastructure, and workflows. While AI is transforming productivity and enabling new capabilities spanning industries, it is also introducing new security risks and attack surfaces that create unique opportunities for attackers. Several major drivers are accelerating the evolution of the AI security market:

Explosion in the Adoption of AI Systems

Enterprises are rapidly deploying AI tools across software development, knowledge management, customer support, and internal workflows. What began as experimentation with generative AI is increasingly moving into production environments and becoming embedded in core enterprise software systems. Organizations are also beginning to deploy AI agents capable of autonomously interacting with applications, data sources, and external systems, further expanding the operational role of AI within enterprise environments.

New Attack Surfaces in AI Infrastructure

Since AI systems rely on data pipelines, training environments, model repositories and inference infrastructure, each component represents a potential entry point for attackers. Moreover, the growing use of AI agents introduces new security considerations that make them attractive targets. As a result, security teams are increasingly confronting risks that did not exist until recently. These risks include manipulation attacks, where adversaries craft malicious inputs to bypass safeguards or produce unintended outputs; infection attacks, where attackers poison training data or manipulate model behavior to influence system outputs; and exfiltration attacks, which attempt to extract sensitive information such as training data, model parameters, or proprietary algorithms from AI systems.

Rapid Emergence of Specialized AI Security Solutions

Over the past year, a new generation of security companies has emerged focused specifically on the unique security needs of AI systems and AI-native environments. These solutions are designed to secure AI models and training environments, protect data pipelines and model supply chains, monitor and control AI system behavior, detect vulnerabilities and misuse in AI applications, and enforce governance, compliance, and security controls for enterprise AI deployments.

As these risks and technologies continue to evolve, the cybersecurity market is beginning to recognize AI Security as a distinct category within the broader cybersecurity ecosystem, and for these reasons, the WisdomTree Team8 Cybersecurity Index will now formally recognize AI Security as its own dedicated theme.

Positioning the Index for the Future

The WisdomTree Team8 Cybersecurity Index was designed to track key cybersecurity themes emerging across the industry, and as the industry evolves, so do the key themes shaping its future. By retiring the Cloud Security theme and introducing the AI Security theme, the index continues to reflect key structural

developments in the cybersecurity market, helping ensure it remains aligned with the technologies and themes shaping the future of cybersecurity.

Conclusion: How Are Cybersecurity Software Companies Performing in 2026 Relative to the Broader Software Group?

Those investors interested in the strategy defined by the WisdomTree Team8 Cybersecurity Index need to look to the WisdomTree Cybersecurity Fund (WCBR) as the investable vehicle designed to track it. From there, we can look to Figures 2a and 2b to examine what we believe is an important performance-oriented question:

How are cybersecurity software companies, broadly speaking, performing relative to the broader landscape of overall software companies so far in 2026?

Like many others, we are aware of the difficult performance in the software space starting 2026 as the business model is facing challenges from artificial intelligence. Even if we believe that 'cybersecurity may be different from broader software' it's important to look at what is happening in the market to see if the returns are bearing this out.

In Figures 2a and 2b, the iShares Expanded Tech-Software Sector ETF (IGV), which is designed to track the total return performance before fees and expenses of the S&P North America Expanded Technology Software Index, is used to showcase the performance of 'broader software.' IGV has gotten significant attention in 2026 as people have been looking at software specifically and, as of March 26, 2026, it had more than $9.7 billion in assets under management.

In Figure 2a, which is through March 26, 2026, we see that IGV is down roughly 24.5% to start 2026, whereas WCBR is down roughly 9.6%. The story that 'cybersecurity software may be different' appears to be playing out. We do understand there is a difference between 'going down less' and 'delivering a positive return', but we believe this significant performance difference is telling us something, and we'll have to monitor to see if this difference continues.

Figure 2a: Cybersecurity Software vs. Broad Software so far in 2026

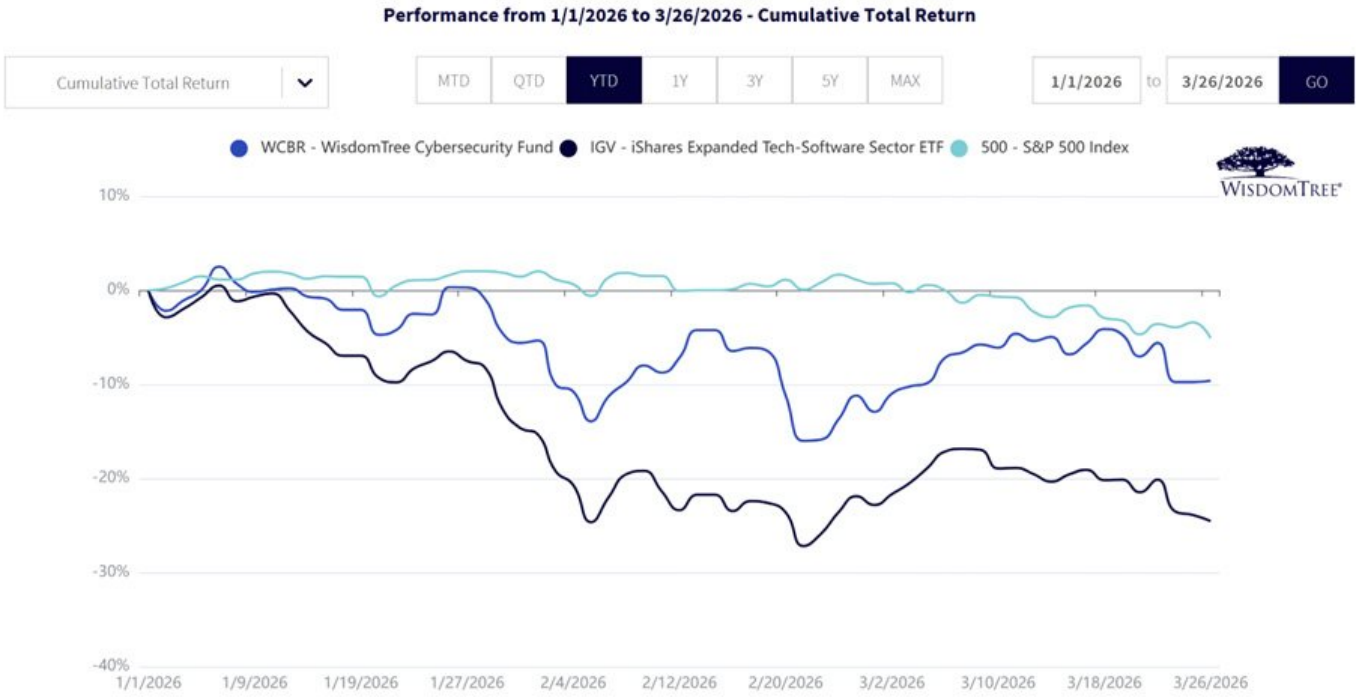


Figure 2b: Standardized Performance

Fund/Index Name	Fund Ticker Symbol	Fund Inception Date	Fund Expense Ratio	Year-to-Date	1-Year	3-Year	5-Year	10-Year	Since Fund Inception
WisdomTree Cybersecurity Fund (NAV)	WCBR	1/28/21	0.45%	-1.73%	-1.73%	22.28%	N/A	N/A	3.03%
WisdomTree Cybersecurity Fund (MP)	WCBR	1/28/21	0.45%	-1.63%	-1.63%	22.28%	N/A	N/A	3.01%
iShares Expanded Tech-Software Sector ETF (NAV)	IGV	7/10/01	0.39%	5.62%	5.62%	27.35%	8.35%	17.90%	10.35%
iShares Expanded Tech-Software Sector ETF (MP)	IGV	7/10/01	0.39%	5.56%	5.56%	27.36%	8.34%	17.89%	10.35%
S&P 500 Index				17.88%	17.88%	23.01%	14.42%	14.82%	N/A

Sources: Morningstar, FactSet and WisdomTree, specifically, data are from the PATH Fund Comparison Tool, accessed as of March 18, 2026, but showing returns for the period ended March 17, 2026 for Figures 2a and December 31, 2025 for 2b. NAV denotes total return performance at net asset value. MP denotes market price performance. **Past performance is not indicative of future results. Investment return and principal value of an investment will fluctuate so that an investor's shares, when redeemed, may be worth more or less than their original cost. Current performance may be lower or higher than the performance data quoted. For the most recent month-end and standardized performance, click the relevant ticker: WCBR, IGV.**

We believe that what we are seeing in AI so far in 2026 ultimately could create more demands for different cybersecurity solutions—many of which come through software—and we look forward to continuing to see how this picture plays out.

Figure 3: Additional Information

Fundamentals	WisdomTree Cybersecurity Fund (WCBR)	iShares Expanded Tech-Software Sector ETF (IGV)
Objective	The WisdomTree Cybersecurity Fund is designed to track, before fees and expenses, the total return performance of the WisdomTree Team8 Cybersecurity Index. The strategy benefits from the expertise of Team8 in analyzing the specific cybersecurity solutions that constituent companies provide, and companies providing more solutions and growing revenues faster tend toward greater exposure in the Index.	The iShares Expanded Tech-Software Sector ETF is designed to track, before fees and expenses, the total return performance of the S&P North American Expanded Technology Software Index. This index is designed to measure U.S. traded securities in the GICS Application Software, Systems Software and Home Entertainment Software sub-industries, as well as applicable supplementary stocks. Weighting is on a modified market capitalization basis.
Total Expense Ratio	0.45%	0.39%
Total Assets Under Management (millions)	$74.79	$9,788.22

Sources: WisdomTree, iShares, with assets under management data as of March 26, 2026. **Subject to change**.

Important Risks Related to this Article

All funds are managed differently and do not react the same to economic or market events. The investment objectives, strategies, policies or restrictions of other funds may differ and more information can be found in their respective prospectuses. Therefore, we generally do not believe it is possible to make direct fund to fund comparisons in an effort to highlight the benefits of a fund versus another similarly managed fund.

WCBR: There are risks associated with investing, including possible loss of principal. The Fund invests in cybersecurity companies, which generate a meaningful part of their revenue from security protocols that prevent intrusion and attacks to systems, networks, applications, computers, and mobile devices. Cybersecurity companies are particularly vulnerable to rapid changes in technology, rapid obsolescence of products and services, the loss of patent, copyright and trademark protections, government regulation and competition, both domestically and internationally. Cybersecurity company stocks, especially those which are internet related, have experienced extreme price and volume fluctuations in the past that have often been unrelated to their operating performance. These companies may also be smaller and less experienced companies, with limited product or service lines, markets or financial resources and fewer experienced management or marketing personnel. The Fund invests in the securities included in, or representative of, its Index regardless of their investment merit and the Fund does not attempt to outperform its Index. Please read the Fund's prospectus for specific details regarding the Fund's risk profile.

For IGV's risk disclosures, click here.

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.