WisdomTree Cybersecurity Fund

WCBR

In 2021, WisdomTree launched the **WisdomTree Cybersecurity Fund (WCBR)**, which is designed to track the total return performance of the WisdomTree Team8 Cybersecurity Index. Each year, we believe it is clear that with all the advances in technology, cybersecurity is only becoming more important. In what follows, we seek to bring clarity both to the landscape of cybersecurity, our expert partner in the space, Team8, and ultimately how our strategy is focused on the future of this important megatrend.

The Most Critical of all Megatrends?

Security and privacy are no longer background considerations—they are now core infrastructure for the global economy. As digital systems become deeply embedded across financial markets, energy grids, supply chains and defense networks, the attack surface has expanded in both scale and consequence. What was once an IT function is now a board-level and, increasingly, a national security priority.

Cybersecurity today is best understood not simply as protection, but as resilience: the ability of systems to continue operating under persistent attack. This includes safeguarding confidentiality, integrity and availability—but also ensuring continuity in environments where disruption is no longer hypothetical, but expected.

The geopolitical backdrop has reinforced this shift. The Russia–Ukraine conflict has demonstrated that cyber warfare is not a precursor to kinetic conflict—it is embedded within it. Attacks on infrastructure, communications and financial systems have become standard tools of statecraft. Similarly, escalating conflict in the Middle East has highlighted the growing role of cyber capabilities alongside traditional military operations. The boundary between cyber and physical domains is dissolving.

At the same time, artificial intelligence is transforming both sides of the equation. Generative AI has lowered the barrier to entry for sophisticated cyberattacks—enabling faster phishing campaigns, automated vulnerability discovery and more convincing social engineering. The next phase, agentic AI, introduces systems that can autonomously probe, adapt and exploit weaknesses in real time.

But this is not a one-sided dynamic.

The same technologies are being deployed defensively—powering real-time threat detection, automated incident response and predictive security architectures. Cybersecurity is becoming an AI-driven arms race, where speed, data and model quality are emerging as decisive advantages.

Recent breaches—ranging from critical infrastructure intrusions to supply chain compromises—underscore a simple reality: organizations are not defending against isolated attacks, but against continuous, adaptive adversaries. This is driving a structural shift toward higher, more persistent cybersecurity spending across both public and private sectors.

Against this backdrop, cybersecurity companies are no longer selling point solutions—they are building integrated, AI-enabled platforms that sit at the center of enterprise and national security architectures. The **WisdomTree Cybersecurity Fund (WCBR)** is designed to provide targeted exposure to these businesses at the forefront of securing the digital economy. By tracking the WisdomTree Team8 Cybersecurity Index

(WTCBR), the strategy captures companies driving innovation across cloud security, identity management, endpoint protection and AI-native defense systems—areas that we believe are becoming increasingly indispensable in a more contested and interconnected world.

Introducing the Cybersecurity Specialist Partner: Team8

To construct the WisdomTree Team8 Cybersecurity Index we leverage data from specialists in cybersecurity, Team8.

Team8 is a Global Venture Group driven by research, relationships and market validation at the intersection of cyber, data, artificial intelligence and fintech. Leveraging an in-house, multi-disciplinary team of company-builders integrated with a dedicated community of C-level executives and thought leaders, Team8's model is designed to identify big problems, ideate solutions, and accelerate success and impact through technology innovation.

WisdomTree and Team8 share a view about the evolution of the cybersecurity market, the products and solutions that will meet the demand of this evolving need, and about the right approach to track the market that intersects with these ideas.

The cybersecurity market is broad and fast-changing due to the rapid evolution of technology and threats. We believe the best way to capture and keep pace with changes in the market is to understand the underlying trends and to identify the products and services that are positioned to provide creative and effective solutions.

Team8 defines the cyber themes they believe will be critical to the cybersecurity industry today and in the coming years.

Team8's Cyber Themes

- **Security of Things**
  - The growth of the Internet of Things (IoT) is driving digitization and unlocking business value. But Security of Things requires that every connected device or network - each with its own identifier and ability to transfer or process data - must be protected. Each of these devices acts as a potential breach-point into an organization or to private data, which increases overall risk exponentially.
- **Perimeterless World**
  - The enterprise perimeter is nearly obsolete, and the dramatic shift to remote work during the pandemic is accelerating its demise. This requires enhanced processes for identity and access management (IAM), with a growing use of zero trust architectures that provide better control.
- **Data Security**
  - Data is at the heart of everything in the modern corporation, with concerns focused on confidentiality, data integrity, and data availability. While the focus has previously been on confidentiality, there is now an increased focus on availability. Integrity of data will be the last frontier for data security considerations.
- **Resilience & Recovery**
  - In a world where digital infrastructure is now synonymous with business-critical infrastructure, cybersecurity cannot afford to stop at protect, defend and respond. Recovery is no longer a nice to have or an afterthought but a core tenant of risk mitigation and business continuity. Any sound security strategy necessitates capabilities that enable rapid recovery from degradation, disruption, or denial of access to enterprise systems or data, and swift reconstitution of assets and capabilities.
- **Shift-Left**
  - Developing and managing software is more agile and faster than ever. However, developers currently have neither the expertise nor the tools to handle the security issues while the security team doesn't have the staff to cover the gap. Cybersecurity needs to be shift-left in the application development process to ensure that security considerations are embedded from the start.
- **Smarter Security**
  - The pace of change in technology brings immense complexity to security, causing organizations to integrate dozens of products. Orchestrating this is a growing challenge and contributing to technology debt and overhead. Further, an expanding enterprise network and shortage of cyber talent combined with an adversary leveraging increasingly sophisticated capabilities is stretching response capacity to its limits. Smarter security solutions can incorporate automation, data, and AI to plug the gaps and provide teams with greater leverage on their human capital.
- **Layer 8**
  - A common first entry point of an attacker to an organization is usually a human (employee), who can easily be compromised by malicious software, social engineering techniques, or simply by human error. 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.

- **AI Security**
  - The rapid adoption of artificial intelligence across enterprise software, infrastructure, and workflows is creating entirely new attack surfaces and risk vectors. AI systems introduce vulnerabilities across data pipelines, model training environments, and inference layers, while also enabling new forms of attack such as model manipulation, data poisoning, and sensitive information leakage. At the same time, the rise of autonomous and agentic AI systems—capable of interacting with applications and executing tasks—further expands the potential blast radius of a breach. As a result, a new generation of security solutions is emerging to protect AI models, secure data and model supply chains, monitor system behavior, and enforce governance and control. AI Security is rapidly becoming a distinct and critical category within cybersecurity, reflecting both the scale of AI adoption and the unique risks it introduces.

Introducing a Unique Cybersecurity Investment Approach

Our approach leverages a proprietary methodology that systematically identifies global innovations in cybersecurity and measures the exposure of public cybersecurity companies, and their products and services, to these key development areas.

The WisdomTree Team8 Cybersecurity Index is constructed to track exposure to the cybersecurity megatrend. The two key tenets of the methodology are designed to increase exposure to companies that are exhibiting both 1) fast revenue growth and 2) involvement in an array of cybersecurity development themes.

WisdomTree Team8 Cybersecurity Index Methodology

WisdomTree Team8 Cybersecurity Index Methodology	
Security Eligibility	+ Minimum $300mn market capitalization + Minimum 3-month average daily trading volume of $1m + List shares on developed and developing world stock exchanges[1]. + Common stocks, REITs, tracking stocks, holding companies, ADRs, GDRs and EDRs
Company Selection	**Focus Score:** Companies are assigned a "Focus Score" based on their degree of involvement across cybersecurity development themes. Eligible companies must be classified as "Broad Focus" or "Narrow Focus". + "Broad Focus" – High exposure to 3 or more cybersecurity themes + "Narrow Focus" – High exposure to 1 or 2 cybersecurity themes + "N/A" – Not involved in any cybersecurity themes
	Revenue Growth Score: Companies are assigned a "Growth Score" based on their compound average annual revenue growth over the trailing 3-years. Eligible companies must be classified as "Growing Fast" or "Growing". + "Growing Fast" – Revenue CAGR of 20% or higher. + "Growing" – Revenue CAGR of 7% or higher for new constituents; 5% or higher for current constituents. + "N/A" – any other company
	Revenue Threshold: At least 50% of revenue derived from providing cyber security products and services
Weighting & Rebalancing	+ Companies with "Growing Fast" or "Growing" Growth Scores without an "N/A" Focus Score are selected. + At least 25 companies are selected. If less than 25 companies pass both the "Growth" and "Focus" screens, the remaining companies from "Broad Focus" and "Narrow Focus" are ranked by revenue CAGR, and higher growth companies are selected for inclusion. + Companies classified as "Broad Focus" & "Growing Fast" are assigned a 1.33x weighting factor. + Companies classified as "Narrow Focus" & "Growing" are assigned a 0.75x weighting factor. + All other companies are assigned a 1x weighting factor. + Semi-annual reconstitution and rebalance in March and September

Source: WisdomTree

Developed world stock exchanges in the U.S., Europe, Tokyo Stock Exchange or on stock exchanges in Australia, Israel, Hong Kong, Singapore, or Canada. Developing world stock exchanges in Brazil, Chile, China, Czech Republic, Hungary, Indonesia, Korea, Malaysia, Mexico, Philippines, Poland, Russia, South Africa, Taiwan, Thailand, or Turkey.

3 Year revenue CAGR is computed as the compound average annual revenue growth over the trailing three years (two years or one year if the data is missing).

Pure-play Exposure to the Cybersecurity Megatrend

Digital systems are no longer just supporting the economy—they are becoming the economy. As AI agents begin to autonomously execute workflows, robots extend into logistics and manufacturing, and software increasingly makes real-time decisions, the number of connected, intelligent endpoints is expanding rapidly. Each new layer of autonomy introduces new vulnerabilities—and a greater need for security embedded at every level of the stack.

Cybersecurity is evolving alongside this shift, moving from reactive defense to continuous, AI-driven protection of dynamic systems. We believe the companies enabling this transition are positioned at the center of a durable and expanding growth opportunity. The WisdomTree Cybersecurity Fund provides targeted, pure-play exposure to this increasingly critical layer of the digital economy.

Quick Facts	
Ticker	WCBR
Exchange	NASDAQ
Expense Ratio	0.45%
Structure	Open-end ETF
Exposure	High-growth companies that drive key developments and innovations in the cyber security market over the medium to long term.
Rebalancing	Semi-annually
Inception Date	01/28/2021

For more information on WCBR, contact your WisdomTree representative or visit WisdomTree.com/investments.

Please see the WisdomTree Glossary for definition of terms and indexes.

References specific to securities and their issues are for illustrative purposes only and are not intended to be, and should not be interpreted as, recommendations to purchase or sell securities.

Investors should carefully consider the investment objectives, risks, charges and expenses of the Fund before investing. For a prospectus or, if available, the summary prospectus containing this and other important information about the fund, call 866.909.9473 or visit WisdomTree.com/investments. Read the prospectus or, if available, the summary prospectus carefully before investing.

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.

Statements concerning financial market trends are based on current market conditions, which will fluctuate. References to specific securities and their issuers are for illustrative purposes only and are not intended to be, and should not be interpreted as, recommendations to purchase or sell such securities.

WisdomTree Funds are distributed by Foreside Fund Services, LLC. Foreside Fund Services, LLC, is not affiliated with the entities mentioned.