Two Roads to the Same Megatrend

Published September 29, 2026

Christopher Gannatti, CFA
Global Head of Research

Key Takeaways

- AI adoption is expanding cybersecurity attack surfaces while also giving attackers faster, more automated tools, reinforcing security's role in enterprise technology spending.
- WisdomTree Cybersecurity Fund (WCBR) requires at least 50% cybersecurity revenue and emphasizes thematic focus and growth across a concentrated 25-stock portfolio.
- CIBR and WCBR define cybersecurity exposure differently, creating structurally distinct portfolios that may respond differently as AI security reshapes the industry.

What CIBR and WCBR Reveal About Cybersecurity Investing

Every conversation about artificial intelligence, especially in the second half of 2026, eventually turns into a conversation about security. Enterprises racing to deploy generative and agentic AI are discovering that each new model, pipeline and autonomous workflow is also a new attack surface. At the same time, the attackers are using the same technology.

- Phishing is faster
- Social engineering is more convincing
- Vulnerability discovery increasingly runs on automation rather than human effort

Cybersecurity, once a background IT cost, has become a genuine "have-to-have" category in enterprise technology spending, which is a rare place where AI adoption is creating demand rather than just responding to it.

2 Funds, 2 Different Methodologies

The First Trust Nasdaq Cybersecurity ETF (CIBR) is the largest fund focused on cybersecurity by assets. The WisdomTree Cybersecurity Fund (WCBR) is smaller by assets under management and is also newer, but has been the stronger performer of late. It would be tempting to write the obvious headline, something like 'Look how WCBR is winning', and stop there. We're not going to do that, for a simple reason.

Nobody, including us, knows in advance which construction methodology will outperform in any given stretch.

Performance differentials over any short window can come from factor tilts, sector composition, single-stock idiosyncrasies or plain luck, and treating a few quarters of relative strength as proof of a superior process is bad analysis dressed up as a good story.

What *is* worth writing about, and what we think is the more durable and more interesting story, is that WCBR and CIBR are not actually making the same bet. They start from different definitions of what a "cybersecurity company" is, and those definitions produce two structurally different portfolios that will behave differently as new themes, like AI security, reshape the industry. Recent performance is simply the visible surface of a deeper methodological divergence. If you want to understand why these funds might diverge further from here, and which one is more directly wired into the AI-security storyline, you have to look at how each one is built.

CIBR tracks the Nasdaq CTA Cybersecurity Index, which sorts companies into two buckets.

- "Core" firms whose products are cybersecurity itself, which could appear as application security, identity and access management, or network security, to name a few functional areas
- "Complementary" firms that touch cybersecurity as part of a broader business, such as diversified technology providers, consultants and managed service providers

The Nasdaq CTA Cybersecurity Index ranks eligible companies by "notional thematic revenue," essentially, estimated cybersecurity revenue multiplied by total company size, and weights by modified free-float market cap, with the largest Core names capped at 8%. That construction rewards scale. It's why CIBR's largest positions include Palo Alto Networks and CrowdStrike, but also why names like Microsoft, Alphabet, Broadcom, Cisco, IBM and Accenture, companies where cybersecurity is one line of business among many, show up as real, non-trivial weights. It's a portfolio built around total thematic exposure, wherever it resides.

WCBR takes a narrower view. It tracks the WisdomTree Team8 Cybersecurity Index, built with Team8, a venture group specializing in cyber, data, AI and fintech. The methodology starts by screening for a revenue threshold, which, simply put, says at least 50% of a company's revenue must come from cybersecurity products and services. From there, companies are scored on two axes

A "Focus Score" measuring how many of Team8's defined cyber development themes a company is meaningfully exposed to (Security of Things, Data Security, AI Security and others),

A "Growth Score" based on trailing three-year revenue growth, with a 20%+ CAGR earning the top "Growing Fast" tier.

Only companies with real focus *and* real growth make the cut, and the highest-conviction combination, broad thematic exposure paired with fast growth, gets a higher weight. The result is a more concentrated positioning.

WCBR holds 25 names, essentially all of them cybersecurity-native businesses like CrowdStrike, Okta, SentinelOne, Palo Alto Networks and Rubrik, with no mega-cap diversified technology companies diluting the exposure.

If we have to say it simply:

- CIBR asks “how much cybersecurity revenue exists across the market, including inside giants where it’s a small piece of a much bigger pie?”
- WCBR asks “which companies are built around cybersecurity, growing fastest, and most exposed to where the industry is actually heading next?”

Those are two different research questions, and they lead to two different answers on the same underlying megatrend.

This distinction is where the AI-security narrative becomes more than a talking point. Team8 explicitly names AI Security as one of its cyber development themes, and this is the idea that AI systems introduce new vulnerabilities across data pipelines, training environments and inference layers, and that a new category of security vendor is emerging specifically to govern and protect them. A methodology built to reward focus on that theme, combined with fast revenue growth, is by design more likely to concentrate in the smaller, more specialized companies building for that future, rather than in the mega-cap technology companies for whom cybersecurity is a mature, slower-growing division layered onto a much larger business.

None of this tells us what happens next. But it does tell us that the recent divergence between these two funds isn’t noise. It’s the direct, mechanical output of two different definitions of what deserves to be called a cybersecurity investment.

Performance in 2026

As we write these words in September of 2026, the focus on the intersection of AI and cybersecurity could not be clearer. Go back to February 20, when Anthropic introduced Claude Code Security, a tool that used its models to autonomously scan codebases and surface vulnerabilities human reviewers had missed for years.1 The market’s first reaction was fear, not validation, and we saw shares of CrowdStrike, Okta, SailPoint and other cybersecurity names sell off sharply that day, on the theory that if an AI lab’s own model could find and patch flaws better than dedicated security software, the vendors themselves might be the ones getting disrupted.2 For a stretch of this year, every fresh capability announcement from a frontier lab carried the same undertone.

Is AI about to eat cybersecurity’s lunch?

The tenor has shifted. Anthropic’s September 2026 threat intelligence report, its fourth since last year, didn’t describe AI replacing security vendors. It described AI-equipped attackers running multi-agent frameworks that handle reconnaissance, exploitation and data exfiltration with minimal human involvement, collapsing the gap between a lone actor and a state-sponsored operation.3 That is a demand story, not a disruption story, as the more capable offense becomes, the more indispensable capable defense becomes. What

started the year as a threat to the sector's business model has increasingly come to look like the sector's most durable tailwind.

That shift in framing is the backdrop against which WCBR's and CIBR's recent performance is worth examining. We can see that the difference appeared to accelerate WCBR's performance in the first half of September 2026.

Figure 1a: Cumulative Returns for Year-to-Date 2026



Sources: Morningstar, FactSet and WisdomTree, specifically, data are from the PATH Fund Comparison Tool, accessed as of September 17, 2026, but showing returns for the period ended September 16, 2026 for Figure 1a and June 30, 2026 for Figure 1b. 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 and to download the respective Fund prospectuses, click the relevant ticker: WCBR, CIBR.**

Even if this is a short period and we need to see the persistence of any sort of return differential to learn more, it is notable given just how much of the world's attention has shifted to this topic. Risk and concepts of what could go wrong have come to the forefront of AI discussions, and proper attention to cybersecurity is paramount. It's fascinating to see what a difference seven months of learning in 2026 has made.

Figure 1b: Standardized Returns

Fund Name	Fund Ticker Symbol	Fund Inception Date	Fund Expense Ratio	Fund SEC 30-Day Yield	Year-to-Date	1-Year	3-Year	5-Year	10-Year	Since Fund Inception
WisdomTree Cybersecurity Fund (NAV)	WCBR	1/28/21	0.45%	-0.35%	30.15%	13.81%	23.30%	8.32%	N/A	7.86%
WisdomTree Cybersecurity Fund (MP)	WCBR	1/28/21	0.45%	-0.35%	29.99%	13.63%	23.13%	8.23%	N/A	7.83%
First Trust Nasdaq Cybersecurity ETF (NAV)	CIBR	7/6/15	0.58%	0.06%	17.38%	11.29%	23.09%	12.84%	17.69%	15.29%
First Trust Nasdaq Cybersecurity ETF (MP)	CIBR	7/6/15	0.58%	0.06%	17.41%	11.31%	23.13%	12.85%	17.71%	15.29%

Sources: Morningstar, FactSet and WisdomTree, specifically, data are from the PATH Fund Comparison Tool, accessed as of September 17, 2026, but showing returns for the period ended September 16, 2026 for Figure 1a and June 30, 2026 for Figure 1b. 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 and to download the respective Fund prospectuses, click the relevant ticker: WCBR, CIBR.**

Even if this is a short period and we need to see the persistence of any sort of return differential to learn more, it is notable given just how much of the world's attention has shifted to this topic. Risk and concepts of what could go wrong have come to the forefront of AI discussions, and proper attention to cybersecurity is paramount. It's fascinating to see what a difference seven months of learning in 2026 has made.

Figure 2: Additional Information

Fundamentals	WisdomTree Cybersecurity Fund (WCBR)	First Trust Nasdaq Cybersecurity ETF (CIBR)
Objective	The WisdomTree Cybersecurity Fund (the "Fund") seeks to track the price and yield performance, before fees and expenses, of the WisdomTree Team8 Cybersecurity Index (the "Index").	The First Trust Nasdaq Cybersecurity ETF (the "Fund") seeks investment results that correspond generally to the price and yield (before the Fund's fees and expenses) of an equity index called the Nasdaq CTA CybersecurityTM Index.
SEC 30-Day Yield	-0.35%	0.06%
Total Expense Ratio	0.45%	0.58%
Total Assets Under Management (millions)	$150.20	$16,274.12

Sources: WisdomTree, First Trust, respective fund pages, with assets under management shown as of September 16, 2026. **Subject to change.**

Sources: WisdomTree, First Trust, respective fund pages, with assets under management shown as of September 16, 2026. **Subject to change.**

1Source: Anthropic. (2026, February 20). *Claude Code Security*.

2Source: Vlastelica, R. (2026, February 20). *Anthropic unveils 'Claude Code Security,' sending cyber stocks lower*. Bloomberg.

3Source: Anthropic. (2026, September 10). *Detecting and countering misuse of AI: September 2026*.

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.

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 CIBR's risk disclosures, click here.