ARE YOU INVESTING IN CYBERSECURITY DEFENSE OR JUST DIVERSIFYING WITHIN TECHNOLOGY?

Chris Gannatti, CFA, Global Head of Research; **Jonathan Flynn**, Director of Market Strategy

Key Takeaways

+ As AI shrinks the gap between vulnerability discovery and exploitation from weeks to hours, cybersecurity is becoming a mission-critical layer of global digital infrastructure.
+ Without a universally accepted benchmark, cybersecurity ETFs can differ significantly in their exposures, making index methodology critical for investors seeking pure-play access.
+ Even as cybersecurity SaaS stocks face valuation pressure in 2026, long-term demand for digital defense may continue to favor focused strategies like the WisdomTree Cybersecurity Fund (WCBR).

The Promise and the Problem

When an investor buys a cybersecurity-focused thematic ETF, we think they are making a very specific bet:

That the companies dedicated to protecting the world's digital infrastructure will outperform the broader equity market.

The premises are intuitive. Cybercrime is now the world's third-largest economy, if you choose to measure it that way, with $10.5 trillion in projected annual damages, trailing only the gross domestic product GDP of the United States and China[1]. Possibly, the more visceral way to measure it is:

+ Hospital systems that cannot process prescriptions
+ Pipelines that go dark
+ In financial exchanges that freeze

The threat has moved beyond data theft. It is infrastructure warfare now, conducted by ransomware syndicates that run help desks and nation-state actors that have decided critical civilian systems are fair game.

AI has made everything in terms of risks worse and everything that is measured by speed faster. The time between vulnerability discovery and active exploitation, once measured in weeks, is now measured in hours. For example:

Phishing campaigns that once required skilled social engineering are generated at scale in seconds.

[1] Source: Morgan, S. (2025). 2025 cybersecurity almanac: 100 facts, figures, predictions and statistics. Cybersecurity Ventures.

Malware evolves in real time to evade the defenses it encounters.

Defenders are adapting, covering machine-speed detection, behavioral analytics, and zero-trust architectures, but the fundamental asymmetry of attack and defense remains:

Attackers need one opening; defenders need to close all of them, forever.

Against this backdrop, we see the investment case for pure-play cybersecurity companies not as a bet on a trend, but rather a bet on a necessity.

Thematic Exposures do not have Established Benchmarks

There is no cybersecurity benchmark, which, put another way means there is no canonical list of stocks that defines the asset class, and therefore no agreed-upon index that separates what belongs from what does not. Every manager draws their own map. And when every manager draws their own map, the maps diverge in ways that matter enormously to investors who assume the territory is shared.

The word "cybersecurity" on a fund's label is, in this sense, a starting point for a conversation rather than a conclusion, and it is also a declaration of intent that says nothing about where the lines are drawn, how tightly the theme is interpreted, or how much of your capital will actually end up in companies for which cybersecurity is the business rather than a business line. In the absence of objective standards, definitional choices become the most consequential investment decisions a thematic fund manager makes. They are also the least visible ones.

This analysis examines the largest ETF focused on cybersecurity on the basis of assets under management, the First Trust Nasdaq Cybersecurity ETF (CIBR) and compares it to the WisdomTree Cybersecurity Fund (WCBR)[2].

What types of conclusions can we draw based on underlying exposures?

The Architecture of a Definition: How Each Index Decides What Cybersecurity Means

The index underlying for CIBR, the Nasdaq CTA Cybersecurity Index, delegates its definitional authority to the Consumer Technology Association, or CTA. CTA classifies eligible companies into two buckets:

- **Core:** These companies are those providing what most investors would recognize as cybersecurity products, things like application security, endpoint protection, identity and access management, and network security. In terms of weighting, the methodology places an 8% cap on the top five Core securities by market capitalization, and a 4% cap on all other Core securities.
- **Complementary:** These companies are a considerably broader category, encompassing consultants, contractors, managed service providers, diversified technology providers, and governance and compliance solutions. In terms of weighting, Complementary securities are given a 2% cap.

[2] As of April 27, 2026, CIBR was the largest ETF in the 'Cybersecurity' theme within WisdomTree thematic classification, with data sourced from Morningstar and FactSet.

The bottom line: If CTA classifies a company as cybersecurity, whether Core or Complementary, it is eligible, regardless of how much of its actual revenue derives from that activity.

The index underlying for WCBR, the WisdomTree Team8 Cybersecurity Index, is built around an entirely different philosophy. WisdomTree partnered with Team8, a venture group built around alumni of Israel's elite Unit 8200 military intelligence operation, one of the world's most sophisticated cybersecurity organizations. Team8 does not define cybersecurity as a static category. It maps it as a living landscape of eight themes:

+ AI Security
+ Smarter Security
+ Perimeterless World
+ Shift-Left development security
+ Data Security
+ Resilience and Recovery
+ Security of Things
+ Layer 8 — the human element

Each eligible company is then assessed for its degree of exposure across these themes, receiving a Focus Score.

+ Companies with high exposure to three or more themes receive a Broad Focus designation.
+ Those with exposure to one or two themes are Narrow Focus.
+ Companies with no meaningful theme exposure are excluded entirely.

Weighting then reinforces selection, and it is not based on measures of company size. WCBR starts from an equal-weight premise. It then tilts toward companies with both broad thematic focus and fast revenue growth, with fast revenue growth defined as growing revenues at a rate greater than 20% for multiple years.

+ Companies classified as Broad Focus and Growing Fast receive a 1.33x weight factor.
+ Narrow Focus and Growing companies receive a 0.75x factor, meaning companies with a strong offering in fewer themes, growing revenues more slowly, get less exposure.

The effect is to actively reward cybersecurity depth and penalize peripheral exposure, rather than simply rewarding size, defined specifically as size of the company on a market capitalization basis.

The Companies Behind the Weights

We think there are some more diversified companies in CIBR, to do this we to combed through the current holdings on April 27th and look at the publicly available information to see if we could piece together the most cogent possible case we could make to connect these firms, that we think are diversified, back to the cybersecurity theme.

We selected eight companies at more than 29% weight of CIBR in total where we tried to make a cybersecurity case, but where our auditing of the publicly available data led us to think it would be difficult to make the case these were pure-play cybersecurity companies. It is meant to illustrate a point that there is a difference between 'possibly connected to cybersecurity' and 'pure-play cybersecurity.'

Importantly, the holdings of both of these funds are subject to change, and both of these funds do have exposure to pure play cybersecurity companies. Our point is simply that, as of April 27, 2026, it appeared that CIBR did contain significant exposure to technology-oriented firms that we would consider more diversified, based on the information that we could see.

Broadcom: A 9.6% Weighting

In 2019, Broadcom paid $10.7 billion for the enterprise security division of Symantec, inheriting a portfolio of endpoint, network, and information security products that today carries the Symantec and Carbon Black brand names[3]. Now, this is one chapter in a very long book. Broadcom reports two business segments[4]:

+ **Semiconductor solutions,** which represented 58% of revenue in fiscal 2025
+ **Infrastructure software,** which represented 42%.

Broadcom lists cybersecurity as one of five major infrastructure software portfolios, alongside Private Cloud, Mainframe Software, Enterprise Software, and FC SAN Management. To pause for a second, FC SAN stands for Fiber Channel Storage Area Network, and it is essentially the high-speed private networking infrastructure that large enterprises use to connect servers to storage systems in data centers. Cybersecurity, however, is not separately disclosed as a revenue line[5].

Cisco Systems: An 8.1% Weighting

We can recognize that this presents a more nuanced case. Cisco's cybersecurity business is real, growing, and increasingly important to the company's strategic narrative. In fiscal 2025, Cisco's security segment generated $8.09 billion in revenue, representing approximately 15% of total company revenue, and a 59% increase from the prior year, driven largely by its $28 billion acquisition of Splunk[6]. But it also means that even after the largest acquisition in Cisco's history, explicitly designed to deepen its security and observability capabilities, roughly 85% of Cisco's revenue still comes from networking hardware, collaboration software, services, and other businesses.

[3] Source: Broadcom Inc. (2019, November 4). Broadcom completes acquisition of Symantec Enterprise Security business [Press release]. PR Newswire.
[4] Source: Broadcom Inc. (2025, December 18). Annual report pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934 (Form 10-K) (Filing date: December 18, 2025). U.S. Securities and Exchange Commission.
[5] Source: Broadcom Inc. 10-K, 2025, December 18.
[6] Source: Cisco Systems, Inc. (2025, September 3). Form 10-K: Annual report for the fiscal year ended July 26, 2025. U.S. Securities and Exchange Commission.

Alphabet: A 2.1% Weighting

Google has made enormous and sincere investments in cybersecurity. Its $5.4 billion acquisition of Mandiant in 2022 brought one of the world's most respected threat intelligence firms under the Google Cloud umbrella[7]. And in March 2025, Alphabet announced the acquisition of Wiz, a leading cloud security platform, for $32 billion in an all-cash deal, the largest acquisition in Google's history, surpassing its $12.5 billion purchase of Motorola Mobility in 2012. Wiz had achieved over $1 billion in annual recurring revenue prior to the deal's closure, and will operate under Google Cloud while maintaining its independent brand and multi-cloud platform support[8].

But here is the thing about a $32 billion acquisition inside a company generating over $400 billion in annual revenue[9]: it barely moves the needle on the income statement. Alphabet's revenue is driven overwhelmingly by advertising, search, YouTube, and the broader Google Cloud infrastructure business. Mandiant, Chronicle, Wiz, and BeyondCorp represent real assets operated by serious people solving hard problems. They are also, in aggregate, a rounding error against the advertising empire that funds them.

Microsoft: A 2.0% Weighting

The last time Microsoft publicly disclosed a specific security revenue figure was January 2023, when Satya Nadella announced on an earnings call that the security business had surpassed $20 billion annually[10]. Since then, despite total company revenue growing from roughly $200 billion to $281.7 billion, Microsoft has stopped providing an updated security revenue figure in its public disclosures.

Microsoft's licensing architecture makes this dynamic difficult to escape. The company's enterprise tiers, most notably Microsoft 365 E3 and E5, bundle security capabilities directly into the same subscription that organizations purchase for email, Office applications, and collaboration tools. An enterprise that licenses Microsoft 365 E5 for its workforce receives Defender, Sentinel, Entra, and Purview as part of that package, whether or not security was the reason for the upgrade[11].

Arista Networks: A 2.4% Weighting

Arista reported revenue of $9.006 billion for the full year ended December 31, 2025, an increase of 28.6% compared to fiscal year 2024[12]. The company's own earnings disclosures show that core cloud, AI, and data center switching products drove 65% of 2025 revenue, campus and routing contributed 18%, and software and services the remaining 17%. Arista does not report a security revenue line because security is not a product category for Arista, but rather it is a feature of its networking platform[13].

[7] Source: Google LLC & Mandiant, Inc. (2022, September 12). Google completes acquisition of Mandiant [Press release, Exhibit 99.1, Form 8-K]. U.S. Securities and Exchange Commission.
[8] Source: Alphabet Inc. (2025, March 18). Google announces agreement to acquire Wiz [Press release, Exhibit 99.1, Form 8-K]. U.S. Securities and Exchange Commission.
[9] Source: Alphabet Inc. (2026, February 4). Alphabet announces fourth quarter and fiscal year 2025 results [Press release, Exhibit 99.1, Form 8-K]. U.S. Securities and Exchange Commission.
[10] Source: Microsoft Corporation. (2023, January 24). Microsoft cloud strength drives second quarter results [Press release, Exhibit 99.1, Form 8-K]. U.S. Securities and Exchange Commission.
[11] Source: Novet, J. (2024). FTC digs deeper into Microsoft's bundling and licensing practices. Computerworld.
[12] Source: Arista Networks, Inc. (2026, February 12). Arista Networks, Inc. reports fourth quarter and year end 2025 financial results [Press release, Exhibit 99.1, Form 8-K]. U.S. Securities and Exchange Commission.
[13] Source: Arista Networks, Inc. (2026, February 12). Q4 2025 earnings presentation [Investor presentation]. Arista Networks Investor Relations.

NetApp: A 2.0% Weighting

NetApp is a data storage and hybrid cloud infrastructure company, and its primary products are storage systems and data management software that help enterprises manage, protect, and migrate data across on-premises and cloud environments. It has layered cybersecurity features into its storage platform, including ransomware detection capabilities for stored data. NetApp's security revenue is not disclosed separately because it is not a separate business, but instead it is a product feature[14].

Accenture: A 1.6% Weighting

Accenture is one of the world's largest professional services and consulting firms, with $69.7 billion in total revenue in fiscal 2025 spread across five industry verticals and more than 120 countries[15]. Its cybersecurity practice is genuinely large and respected, encompassing thousands of practitioners, major enterprise clients, and a growing portfolio of managed security services. However, Accenture did not build itself around cybersecurity. It added cybersecurity to an existing consulting empire because its clients needed it.

IBM: A 1.7% Weighting

IBM Security has been a recognized brand in enterprise cybersecurity for decades, built around products like QRadar, Guardium, and X-Force threat intelligence. These are products used by governments and Global 2000 enterprises to detect breaches, protect data, and respond to incidents. The cybersecurity pedigree is genuine.

And yet in September 2024, IBM transferred the Software-as-a-Service (SaaS) assets of QRadar, its flagship security information and event management platform, to Palo Alto Networks, one of the world's leading pure-play cybersecurity firms[16]. That is not the act of a company for whom cybersecurity is a defining strategic identity.

In a telling structural footnote, IBM quietly removed Security as a separately reported revenue category within its Software segment beginning in fiscal year 2025, meaning investors can no longer even track what the business generates on its own terms[17].

Taken together, these eight holdings:

+ Broadcom
+ Cisco
+ Alphabet
+ Microsoft
+ Arista
+ IBM
+ NetApp
+ Accenture

accounted for more than 29% of CIBR's total weight as of April 27, 2027. Not one of them derives its primary identity, its primary revenue, or its primary strategic orientation from cybersecurity, at least from what we could discern.

[14] Source: NetApp, Inc. (2025, June 9). Form 10-K: Annual report for the fiscal year ended April 25, 2025. U.S. Securities and Exchange Commission.
[15] Source: Accenture plc. (2025, September 25). Accenture reports fourth-quarter and full-year fiscal 2025 results [Press release, Exhibit 99.1, Form 8-K]. U.S. Securities and Exchange Commission.
[16] Source: Palo Alto Networks. (2024, September 4). Palo Alto Networks closes acquisition of IBM's QRadar SaaS assets [Press release]. PR Newswire.
[17] Source: IBM. (2025). IBM 2025 annual report.

They are in this fund because an index methodology said they qualified. The financial disclosures, in our opinion, say something different.

In Figure 1, we take the top 25 holdings in each strategy, and we do this so we can see all 8 of the positions that we mentioned in this piece for CIBR. As we noted, WCBR is different, in that we have a domain expert studying the specific offering of each company and noting exposure to specific cybersecurity themes. It is also different in that there are only 25 positions, so in Figure 1 we are seeing the full WCBR constituent list.

The bottom line is that, even if performance is a separate question, there are no broad-based diversified businesses in WCBR that are tricky to relate back to the cybersecurity theme. We say performance is a separate question because being exposed to cybersecurity, while we think it is what investors are looking for within a cybersecurity strategy, does not necessarily guarantee outperformance. WCBR's holdings are primarily SaaS business models, which have had issues in 2026 in proving their value to the overall equity market. When comparing strategies, it's important to be balanced.

Figure 1: A Comparison of the Top 25 Constituents

CIBR		WCBR	
Company Name	**Weight**	**Company Name**	**Weight**
Broadcom Inc.	**9.59%**	Sentinelone Inc -Class A	6.63%
Palo Alto Networks, Inc.	9.00%	Crowdstrike Holdings Inc - A	6.43%
CrowdStrike Holdings, Inc. (Class A)	8.95%	Zscaler Inc	5.52%
Cisco Systems, Inc.	**8.14%**	Palo Alto Networks Inc	5.05%
Fortinet, Inc.	7.23%	Datadog Inc - Class A	4.88%
Cloudflare, Inc. (Class A)	4.52%	Trend Micro Inc	4.80%
Zscaler, Inc.	3.25%	Netskope Inc-Cl A	4.80%
F5, Inc.	2.96%	Fortinet Inc	4.76%
Check Point Software Technologies Ltd.	2.87%	Tenable Holdings Inc	4.74%
Akamai Technologies, Inc.	2.86%	Cloudflare Inc - Class A	4.70%
Okta, Inc.	2.43%	Rubrik Inc-A	4.62%
Arista Networks, Inc.	**2.37%**	Okta Inc	4.52%
Datadog, Inc. (Class A)	2.17%	Check Point Software Technolog	4.15%
Gen Digital Inc.	2.14%	CommVault Systems Inc	3.84%
Alphabet Inc. (Class A)	**2.06%**	Fastly Inc - Class A	3.74%
NetApp, Inc.	**2.01%**	F5Inc	3.71%
Microsoft Corporation	**1.98%**	Varonis Systems Inc	3.64%
Dynatrace, Inc.	1.82%	Sailpoint Inc	3.59%
Rubrik, Inc. (Class A)	1.76%	Elastic Nv	3.25%
Booz Allen Hamilton Holding Corporation	1.74%	Akamai Technologies Inc	3.19%
International Business Machines Corporation	**1.74%**	Qualys Inc	3.05%
Thales S.A.	1.65%	Ffri Security Inc	2.30%
Infosys Limited (ADR)	1.56%	Rapid7 Inc	1.77%
Accenture plc	**1.55%**	Vasco Data Security International Inc	1.73%
Leidos Holdings, Inc.	1.51%	Ahnlab Inc	0.59%
Total in Top 25 Positions	**87.86%**	**Total in Top 25 Positions**	**100.00%**

Sources: First Trust and WisdomTree, with holdings as of April 27, 2026. **Subject to change.**

The Label Is Not the Product

Two funds. The same label. Dramatically different portfolios. For an investor who believes in the cybersecurity theme, and the structural case for that belief has never been stronger, the vehicle matters as much as the thesis. CIBR offers broad exposure to a loosely defined category, anchored by companies whose primary businesses have little to do with stopping breaches. WCBR offers something rarer in thematic investing: discipline. its practitioner-informed definition of cybersecurity, and its modified equal-weight construction (specifically tilting away from market cap weighting) combine to produce a portfolio that actually reflects the theme it claims to represent. When the next major breach makes headlines, you want to own the companies built to respond to it, not the ones that happen to be in the same index.

Figure 2: Additional Information

Fundamentals	WisdomTree Cybersecurity Fund (WCBR)	FirstTrust Nasdaq Cybersecurity ETF (CIBR)
Inception Date	1/28/21	7/6/15
Objective	The WisdomTree Cybersecurity Fund is built to track the total return performance of, before fees and expenses, the WisdomTree Team8 Cybersecurity Index. This index was developed in partnership with Team8 and focuses on defining eight specific cybersecurity themes and then analyzing the cybersecurity offering of each constituent stock twice per year to determine which are strongly exposed to those themes. Weighting and ultimately index exposure is derived from exposure to a broader spectrum of themes and faster revenue growth.	The First Trust Nasdaq Cybersecurity ETF is an exchange-traded fund. 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 Cybersecurity™ Index. The Nasdaq CTA Cybersecurity™ Index is designed to track the performance of companies engaged in the cybersecurity segment of the technology and industrials sectors. It includes companies primarily involved in the building, implementation, and management of security protocols applied to private and public networks, computers, and mobile devices in order to provide protection of the integrity of data and network operations.
Total Expense Ratio	0.45%	0.58%
Underlying Index Name	WisdomTree Team8 Cybersecurity Index	Nasdaq CTA Cybersecurity Index
Total Assets Under Management (millions)	$77.25	$10,230.97

Sources: WisdomTree and FirstTrust, with assets under management data as of April 27, 2026. **Subject to change.**

IMPORTANT INFORMATION

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

Investors should carefully consider the investment objectives, risks, charges and expenses of the Fund before investing. To obtain a prospectus, or summary prospectus, containing this and other important information, please call 866.909.9473, or visit WisdomTree.com/investments to view or download a prospectus. Investors should read the prospectus carefully before investing.

WCBR: There are risks associated with investing, including the 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.

CIBR: Current market conditions risk is the risk that a particular investment, or shares of the fund in general, may fall in value due to current market conditions. For example, changes in governmental fiscal and regulatory policies, disruptions to banking and real estate markets, actual and threatened international armed conflicts and hostilities, and public health crises, among other significant events, could have a material impact on the value of the fund's investments. A fund is susceptible to operational risks through breaches in cyber security. Such events could cause a fund to incur regulatory penalties, reputational damage, additional compliance costs associated with corrective measures and/or financial loss. Information technology companies and cyber security companies are generally subject to the risks of rapidly changing technologies, short product life cycles, fierce competition, aggressive pricing and reduced profit margins, loss of patent, copyright and trademark protections, cyclical market patterns, evolving industry standards and frequent new product introductions. Cyber security companies may also be smaller and less experienced companies, with limited product lines, markets, qualified personnel or financial resources.

WisdomTree Funds are distributed by Foreside Fund Services, LLC.

WisdomTree, Inc. and Foreside Fund Services, LLC are not affiliated with the other entities mentioned.