The Cybersecurity Crossroads: How Public Companies Are Defending a Digital World in 2025

Published July 21, 2025

Christopher Gannatti, CFA
Global Head of Research

Key Takeaways

- In 2025, the rise of Ransomware as a Service and increasing digital connectivity have made cybersecurity a boardroom imperative, with public companies racing to defend against billion-dollar threats.
- AI adoption has emerged as perhaps the most transformative boardroom priority—offering the potential for exponential gains in productivity, decision-making and competitive differentiation, while also introducing new vectors of risk.
- The WisdomTree Cybersecurity Fund (WCBR) has demonstrated strong returns and consistent revenue growth, reflecting the sector's shift from niche IT concern to foundational economic infrastructure.

In 2025, cybersecurity is no longer a technical issue whispered about in IT departments. It has broken into boardrooms, earnings calls and geopolitical strategy meetings. What began as a conversation about firewalls and antivirus software is now about economic resilience, national security and investment risk.

We've arrived at a point where ransomware can stall a global manufacturing operation in hours, a compromised login can unlock millions in financial losses, and a single software vulnerability in one vendor can ripple across hundreds of downstream companies. This isn't theory—it's reality, and it's happening with increasing regularity.

To understand where we are now, we must first recognize what has changed.

The Rise of RansomwareasaService

In the past, cyberattacks were often the domain of skilled individuals or nation-states. Today, ransomware has become a business. With Ransomware as a Service (RaaS), anyone with a motive can rent the tools and support to launch an attack, with pre-written code, customer service portals and revenue sharing.

This model has dramatically lowered the barrier to entry. In 2024 alone, public intelligence sources recorded record highs in ransomware victim counts.1 These attacks aren't just encrypting files—they're stealing data, leaking it and sometimes threatening physical systems. The economic damage is measured in billions.

What Companies Are Doing aboutIt

To respond, an entire ecosystem of public cybersecurity companies is arming enterprises with layered defenses. One of the first and most crucial lines of defense is something called endpoint detection and response (EDR). Think of this as the security guard for every laptop, server and smartphone. Companies like CrowdStrike, SentinelOne and Palo Alto Networks provide EDR platforms that use artificial intelligence to detect and neutralize threats as they emerge.2

But sometimes the threat slips through. That's where data backup companies like Rubrik, Commvault and NetApp come in. They provide tools to take "snapshots" of data that can't be changed or deleted by attackers, enabling businesses to restore operations quickly without paying a ransom.3

And finally, there are the companies trying to stop the threat before it even reaches your device. Zscaler, Cloudflare and Fortinet offer secure access platforms that act like custom-built roadblocks, deciding who gets in and where they can go.4 This model, known as Zero Trust, assumes every user or device is a potential threat until proven otherwise.

The Supply Chain's Soft Underbelly

Beyond the direct attacks lies a more insidious risk: supply-chain infiltration. In many cases, hackers don't target their primary victim directly. Instead, they exploit a weaker link—a software vendor, a contractor, even a cloud services provider—to gain access.

This happened in the MOVEit breach, where a vulnerability in a file-transfer tool exposed millions of individuals' data.5 Governments around the world now refer to supply chains as the "soft underbelly" of national security.

Here, companies like Tenable, Qualys and Rapid7 shine. They specialize in scanning an organization's infrastructure for vulnerabilities before attackers can find them. At the same time, edge-security vendors like Akamai, Fastly and Cloudflare are building digital checkpoints to inspect every request and block suspicious activity in real time.6

Industrial Systems Go Online

As factories, power plants and water utilities digitize, their old, isolated control systems are being connected to the internet. This creates new opportunities for efficiency—and new openings for attackers.

A cyberattack on an oil pipeline in 2021 caused fuel shortages across the Eastern U.S. That was a wake-up call.7 Since then, cybersecurity for operational technology (OT) has become critical. Companies like Fortinet and Palo Alto Networks now offer industrial-grade firewalls and sensors built for harsh environments, while Trend Micro and CrowdStrike are developing tools to detect threats inside factory networks without disrupting operations.

Specialist firms like AhnLab in South Korea and Digital Arts in Japan are also gaining traction, particularly in Asia, by offering regionally customized industrial-security solutions.

Identity: The Front Door to Everything

For all the complexity of modern attacks, sometimes the biggest weakness is still the simplest: stolen passwords. Whether through phishing or leaked credentials, attackers often walk in the digital front door.

That's why identity and access management (IAM) is booming. Okta offers secure single sign-on systems, while CyberArk focuses on protecting the most sensitive accounts—like the digital keys to your company's vault. Identity-focused tools are now using behavior analysis to detect when a legitimate user is acting suspiciously. CrowdStrike, Zscaler and Cloudflare are all leaning into this area as well.8

Cloud Sprawl and Security Blind Spots

As more companies move their operations to the cloud, the attack surface grows. Every cloud service, app and integration is another potential weak point. Misconfigured access controls or forgotten storage buckets can become open doors.

To manage this, vendors like Palo Alto Networks, Datadog and Elastic offer tools that monitor cloud environments for missteps, misconfigurations or unauthorized activity. This is where cloud-native security lives: not just protecting a data center, but securing thousands of decentralized services in real time.9

And because more of this traffic happens over the internet, companies like Akamai and Fastly are becoming essential infrastructure—inspecting and filtering data before it reaches its destination.

Even the Defenders Are at Risk

Ironically, as security platforms themselves become more complex and more connected, they, too, become targets. In 2024, cybersecurity firm Palo Alto Networks was listed among the most-exploited vendors in the U.S. government's known vulnerabilities catalog.10

That's why we're now seeing a surge in what's called "attack surface management." Firms like Tenable, Rapid7 and Qualys offer services that simulate hacker reconnaissance, constantly probing for exposed systems—even inside security companies themselves.

What Comes Next

Cybersecurity today is a race—between the growing sophistication of attackers and the layered defenses of the companies trying to stop them. But there is no finish line. Threats evolve, technology shifts, and so the landscape constantly changes.

For investors, the takeaway is not to find a single "best" company, but to understand which companies are solving the most urgent problems. Ransomware protection, supply chain integrity, industrial system security, identity management, cloud risk visibility—these are not niche concerns anymore. They are foundational to how modern economies operate.

As governments tighten regulations and boards face liability for breaches, the market for these solutions will only grow. In 2025, cybersecurity is not just about defense. It's about trust, resilience and operational continuity. That makes it a macro trend—and a long-term investment story worth watching.

Conclusion: Performance of a Strategy Focused on Cybersecurity Equities

The WisdomTree Cybersecurity Fund (WCBR) represents a basket of cybersecurity equities as defined by the WisdomTree Team8 Cybersecurity Index. On a semiannual basis, Team8's cybersecurity research professionals are evaluating publicly traded cybersecurity companies that are focused on providing solutions aimed at the future of cybersecurity.

Even if we might think that the risks in cybersecurity are consistently rising and the focus on cybersecurity needs to keep pace, how are the equities performing?

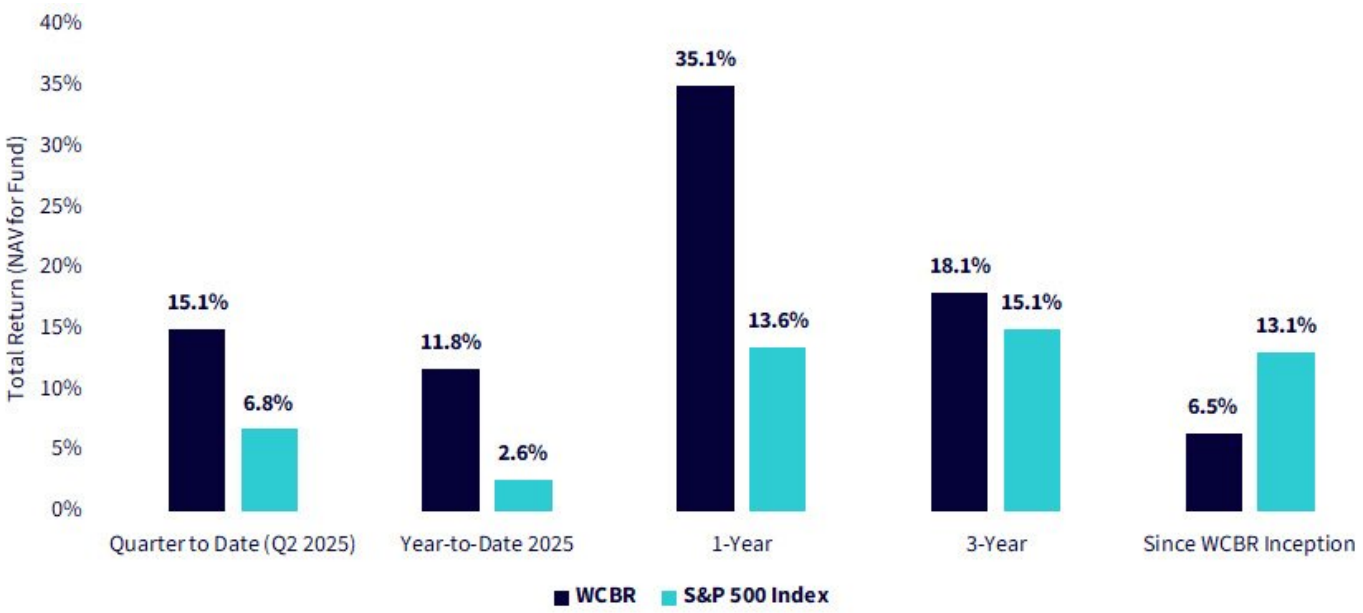
Figure 1: Standardized Returns

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	1/28/2021	0.45%	-4.27%	5.87%	3.22%	N/A	N/A	2.93%
WisdomTree Cybersecurity Fund (MP)	WCBR	1/28/2021	0.45%	-4.13%	5.88%	3.13%	N/A	N/A	2.93%
S&P 500 Index				-4.27%	8.25%	9.06%	18.59%	12.50%	N/A

Sources: WisdomTree, FactSet, Morningstar, specifically data from the Fund Comparison Tool in the PATH suite of tools, accessed 7/11/25, with returns as of 6/30/25. NAV denotes total return performance at net asset value. MP denotes market price performance. **The performance data quoted represents past 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 performances, click here.**

Figure 2 is interesting to us because many associate 2025's equity performance, so far, with volatility. WCBR has been strong when compared to U.S. broad market equities, such as the S&P 500 Index benchmark.

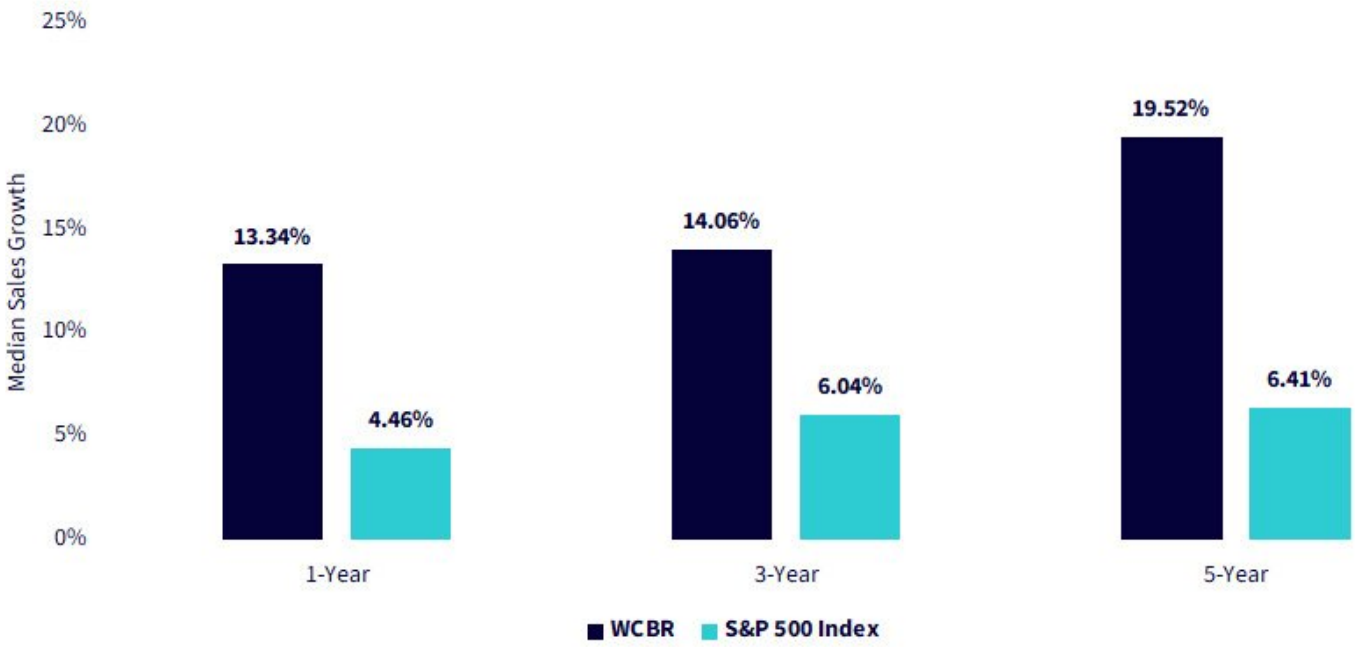
Figure 2: Amid the Noise: Cybersecurity Has Led in 2025



Sources: WisdomTree, FactSet, Morningstar, specifically data from the Fund Comparison Tool in the PATH suite of tools, accessed 7/11/25, with returns as of 7/10/25. "Since WCBR Inception" is from 1/28/21. 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 performances, click here.**

It's also important to look at revenue growth—the concept that customers are demanding more and more of the cybersecurity services. In figure 3, we look at median sales growth so as not to be unduly influenced by outlier values. One would expect faster-than-S&P-500-Index-level sales growth, but we think these figures are particularly robust for these past periods of one, three and five years. We'll continue to monitor this to see how it continues.

Figure 3: Outgrowing the Market: Cybersecurity's Long-Term Sales Strength



Sources: WisdomTree, FactSet, with data accessed from WisdomTree's Fund Compare Tool in the broader PATH suite of tools. Data is as of 6/30/25. **Past performance is not indicative of future results.**

1 Source: GRIT, "GRIT 2025 Ransomware and Cyber Threat Report" (p. 8–9), GuidePoint Security, 2025.

2 Source: United Kingdom Parliament, "A hostage to fortune: Ransomware and UK national security" (House of Commons and House of Lords Joint Committee on the National Security Strategy, Evidence RAN0017, RAN0033), 2024. https://committees.parliament.uk/publications/42087/documents/205936/default/

3 Source: Honeywell, "2025 Cyber Threat Report: Insights and Actions to Manage Cyber–Physical Threat Convergence (p. 6–8), Honeywell International Inc., 2025.

4 Source: Honeywell, "2025 Cyber Threat Report," 2025.

5 Source: UK Parliament, "A hostage to fortune," 2024.

6 Source: GRIT, "Ransomware and Cyber Threat Report," 2025.

7 Source: Cybersecurity and Infrastructure Security Agency, "The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years," 5/7/23.

8 Source: Honeywell, "2025 Cyber Threat Report," 2025.

9 Source: GRIT, "Ransomware and Cyber Threat Report," 2025.

10 Source: GRIT, "Ransomware and Cyber Threat Report," 2025.

Important Risks Related to this Article

For current holdings, click here. Holdings are subject to risk and change.

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 on 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 that 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 or take defensive positions in declining markets. The composition of the Index is heavily dependent on quantitative and qualitative information and data from one or more third parties, and the Index may not perform as intended. Please read the Fund's prospectus for specific details regarding the Fund's risk profile.