Securing the Future: The Ever-Growing Need for Cyber Defense

Published February 20, 2025

Christopher Gannatti, CFA
Global Head of Research

Key Takeaways

- The cybersecurity landscape is evolving rapidly, with generative AI amplifying both threats and defenses as cyber incidents surge to unprecedented levels.
- Industry leaders like Rubrik, Palo Alto Networks and CrowdStrike are driving innovation, while businesses increasingly prioritize zero-trust security, data protection and AI-driven threat detection.
- With rising costs and fierce competition, cybersecurity firms must balance growth with operational efficiency, while investors seek high-growth opportunities in AI-powered security solutions.

In the kaleidoscope of cybersecurity, 2024 stands as a hallmark year—equal parts challenge and opportunity. Generative AI, a marvel reshaping digital landscapes, has amplified the scale and sophistication of cyber threats. Amazon's revelation of daily incidents surging from 100 million to 750 million by year-end paints a vivid picture.[1] Microsoft, on the other hand, processed more than 78 trillion security signals daily[2]—an unrelenting barrage that emphasizes the ceaseless evolution of the threat landscape.

Beyond the technical, geopolitics add their own weight to the narrative. The breach of U.S. communication networks by Chinese hackers is a stark reminder that nation-states are key players in the cyber arena. This underscores the pervasive and indiscriminate nature of today's threats.

Against this backdrop, economic currents further complicate the waters. Tax cuts introduced by a Republican-led government have paved the way for SMBs to bolster their cybersecurity budgets, yet December's market volatility tempers optimism. Inflation and labor market resilience continue to stoke debates about monetary tightening, leaving businesses to navigate a world where robust cybersecurity is no longer optional—it's existential.

A Closer Look at the Companies Driving Growth

Amid this dynamic backdrop, certain companies have distinguished themselves as architects of the future. Rubrik, for instance, has emerged as a paragon of growth, delivering an eye-popping 103.3% share price appreciation in Q4 2024.[3] It's not just financial numbers driving this success; Rubrik's advanced cloud data management solutions, spanning backup, disaster recovery and ransomware protection, have redefined

operational efficiency for its clients. Meanwhile, Qualys continues to leverage market buzz around its potential acquisition, further strengthening its standing.[4]

Palo Alto Networks' vision is equally ambitious. Targeting $15 billion in annual recurring revenue (ARR) by 2030, its current ARR of $4.5 billion—up 40% year-over-year—provides a glimpse of its trajectory.[5] Growth in platform customers and a knack for navigating competitive waters have fortified its market leadership. Meanwhile, CrowdStrike's retention rates, surpassing 97%, and its strong customer expansion following a July 2024 outage tell a story of resilience.[6]

Not all stories are of triumph. SentinelOne's achievement of positive free cash flow on a trailing 12-month basis was overshadowed by its rising expenses. Its $246.5 million in operating costs—driven by investments in talent, R&D and aggressive marketing—reflects the cost of growth.[7] Akamai, Zscaler and Varonis also wrestle with cautious guidance and competitive pressures, showing that even strong players must constantly adapt.

Insights from Industry Leaders

The 2024 CISO Survey[8] provides invaluable insights, drawing from more than 100 CISOs across industries like finance, technology, health care and manufacturing. With 60% reporting cybersecurity teams of 20 or more, the survey reflects a robust yet varied approach to resource allocation.

Data security is paramount. Sixty-five percent of CISOs identified issues like data loss prevention and insider threats as their top concerns. Third-party risk management (TPRM) also featured prominently, underscoring the growing complexity of managing vendor relationships. Meanwhile, the ascent of zero-trust architectures highlights a collective pivot toward proactive security strategies.

AI's role in cybersecurity remains paradoxical. While 70% of CISOs perceive AI as a security risk, 85% acknowledge its transformative potential. The duality demands nuanced solutions—leveraging AI's strengths while mitigating its vulnerabilities. Sectoral nuances emerge, too, with financial services prioritizing data security and manufacturing zeroing in on TPRM.

The Economics of Cybersecurity: Key Cost Drivers

For cybersecurity companies, growth is expensive. Employee salaries and benefits dominate budgets, often accounting for 50%–70% of operating costs. CrowdStrike exemplifies this, channeling substantial resources into competitive compensation packages to attract top talent. Palo Alto Networks' employee investments further illustrate the emphasis on workforce quality.

Sales and marketing form the second pillar, consuming 10%–20% of budgets. Zscaler's expenditure on marketing, aimed at differentiating itself in a crowded market, exemplifies the sector's challenges in achieving visibility. Meanwhile, R&D investments vary but remain critical. Fortinet's consistent R&D spending has underpinned its innovation, while SentinelOne's heavy investment in cutting-edge technologies underscores its commitment to staying ahead in a fast-paced field.

The Promise and Pitfalls of Generative AI

Generative AI offers immense promise but comes with pitfalls. On one hand, it powers advanced threat detection and automation—a frontier being led by companies like Datadog and Elastic. On the other, it necessitates constant vigilance as the sophistication of AI-driven cyberattacks escalates.

The burgeoning demand for identity management and cloud security further cements the relevance of firms like CrowdStrike and CyberArk. Subscription-based models, championed by Rubrik and Palo Alto Networks, highlight the adaptability of companies to evolving market needs.

Navigating the Road Ahead

The cybersecurity sector's narrative is one of enduring growth amid constant flux. Companies with a sharp focus on AI, cloud computing and analytics are well-positioned to seize future opportunities. Yet, rising costs and competitive dynamics serve as a reminder that agility and strategic foresight are non-negotiable.

Short-term volatility coexists with long-term promise. While SentinelOne and Zscaler navigate uneven terrain, industry leaders like Palo Alto and CrowdStrike continue to set benchmarks for resilience and innovation. For investors, the sector offers both opportunity and complexity—a landscape where informed decision-making is crucial.

At WisdomTree, the WisdomTree Cybersecurity Fund (WCBR), which is designed to track the total return performance, before fees and expenses, of the WisdomTree Team8 Cybersecurity Index, is poised to capture the potentially fast growth within the cybersecurity megatrend, particularly amongst companies that are providing software solutions.

Team8, a venture firm with cybersecurity expertise, defines different key themes deemed essential to the future of cybersecurity. Technology is changing quickly, so the manner in which we secure against different risks must also be quite nimble.

WisdomTree ensures that the Index is tilting focus toward those cybersecurity software companies with faster revenue growth.

Figure 1: Standardized Performance

Fund/Index Name	Fund Ticker Symbol	Fund Expense Ratio	Fund Inception Date	1-Year	3-Year	5-Year	10-Year	Since Fund Inception
WisdomTree Cybersecurity Fund (NAV)	WCBR	0.45%	1/28/2021	11.82%	2.83%	N/A	N/A	4.27%
WisdomTree Cybersecurity Fund (MP)	WCBR	0.45%	1/28/2021	11.62%	2.76%	N/A	N/A	4.23%
S&P 500 Index				25.02%	8.94%	14.53%	13.10%	N/A
Russell 1000 Growth Index				33.36%	10.47%	18.96%	16.78%	N/A

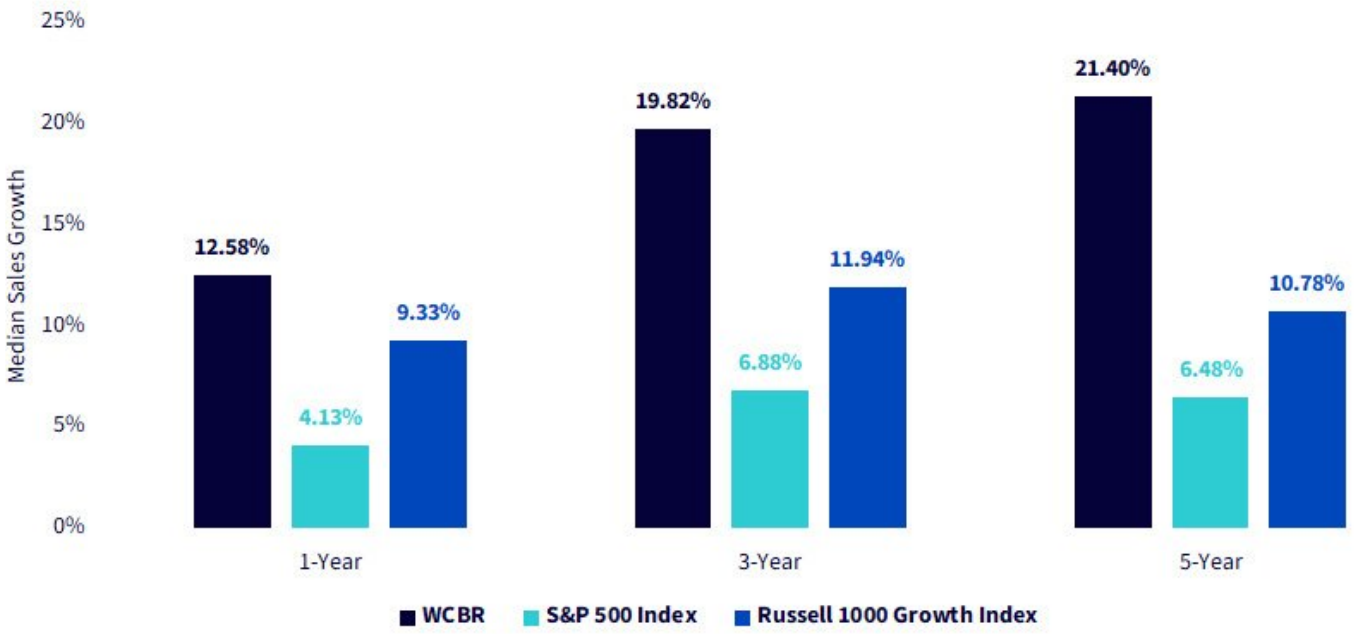
Source: WisdomTree, specifically data is from the PATH Fund Comparison Tool, accessed as of 1/15/25, for the standardized period ending 12/31/24. NAV denotes total return performance at net asset value. MP denotes market price performance. **Past performance is not indicative of future results. Investment 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.**

At each semiannual rebalance of the WisdomTree Team8 Cybersecurity Index, companies are classified into three groups based on their sales growth:

- **Fast Growth:** These are companies with annualized revenue growth greater than 20%.
- **Growth:** These are companies with annualized revenue growth between 7% and 20%.
- **Slow Growth:** These are companies with annualized revenue growth below 7%. Initially, these firms would be excluded from the Index unless there is a scenario where less than 25 constituents qualify for inclusion. In that case, some slow-growth companies can be included to bring the total number of constituents to 25.

Figure 2 looks over the past one-, three- and five-year periods, noting the median sales growth of WCBR as compared to that of the S&P 500 and Russell 1000 Growth Indexes. We believe a core tenet that makes thematic strategies like cybersecurity more interesting is the capability to capture faster growth than broad benchmarks.

Figure 2: Tilting toward Sales Growth



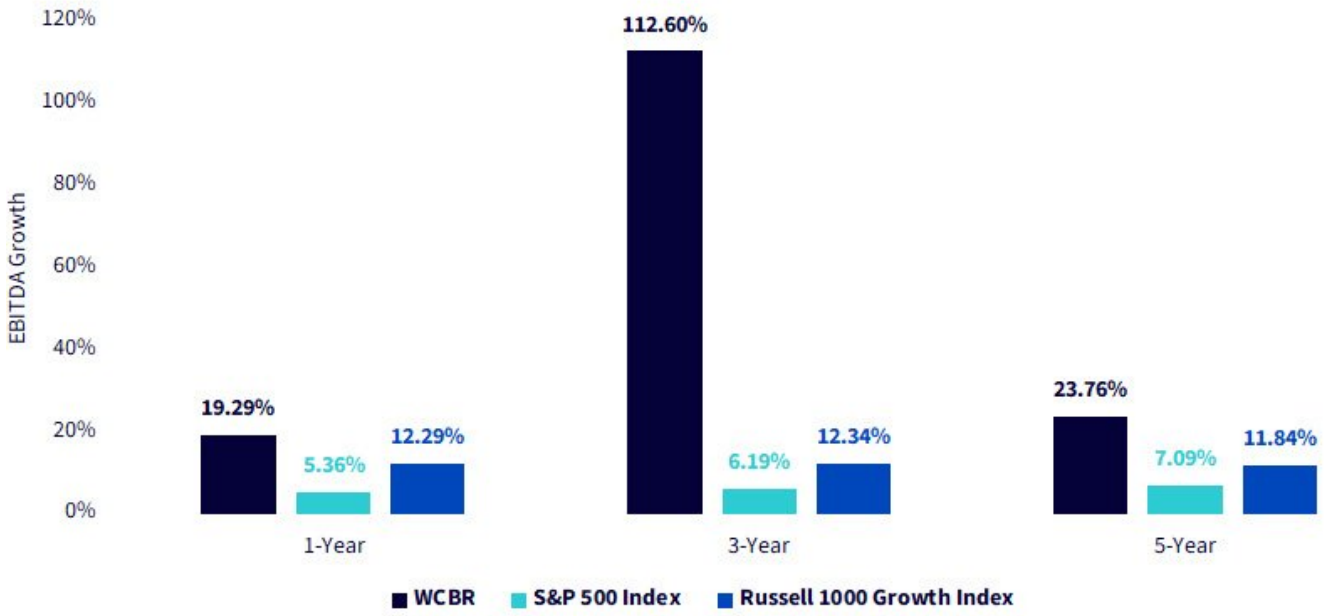
Source: WisdomTree, specifically data is from the PATH Fund Comparison Tool, accessed as of 1/15/25, for the standardized period ending 12/31/24.

Shifting from looking at sales growth to EBITDA growth brings us from the top line of the income statement into the middle of the income statement. Certain operational costs are accounted for, whereas certain non-cash expenses like depreciation and amortization are not.

While the top-line sales growth gives us a sense of the growing demand for the offering of these firms, EBITDA growth gives more of a sense of the operational characteristics of the business.

In figure 3, the three-year growth in EBITDA is basically off of the chart's regular axis, showing a median figure above 100%. Remember, a median is not pulled up by outlier values.

Figure 3: Strong Growth in EBITDA (Earnings before Interest, Taxes, Depreciation and Amortization)



Source: WisdomTree, specifically data is from the PATH Fund Comparison Tool, accessed as of 1/15/25, for the standardized period ending 12/31/24.

Conclusion

As the cybersecurity sector evolves, its challenges and opportunities are interwoven in complex patterns. Companies like Rubrik, Palo Alto Networks and CrowdStrike exemplify the sector's ability to adapt and innovate. Insights from the 2024 CISO Survey further illuminate a path forward, emphasizing the need for robust data security, strategic risk management and AI integration. In this dynamic landscape, the future of cybersecurity promises to be as rewarding as it is demanding.

[1] Source: James Rundle, "The AI Effect: Amazon Sees Nearly 1 Billion Cyber Threats a Day," *Wall Street Journal*, 11/21/24.

[2] Source: Microsoft Digital Defense Report, 2024.

[3] Source: Wall Street Journal company share price quotes.

[4] Source: Baker et al., "Cybersecurity Company Qualys Is Said to Explore Sale (1)," *Bloomberg Law*, 11/6/24.

[5] Source: Reinhardt Krause, "Palo Alto Networks Fiscal Q1 Results Fuel Debate Over 'Platformization,'" I*nvestors Business Daily*, 11/21/24.

[6] Source: https://www.investing.com/news/swot-analysis/crowdstrikes-swot-analysis-resilient-cybersecurity-leader-faces-challenges-stock-outlook-93CH-3794671

[7] Source: Emily Dattilo, "SentinelOne's Revenue Soars 28%. Why the Stock Is Tumbling," *Barron's*, 12/5/24.

[8] Source: Key findings from Team8's 2024 CISO Village Survey, September 2024.

Important Risks Related to this Article

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 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.