

Cyberattacks Continue to Increase—Are Investors in Cybersecurity Software Providers Benefitting?

Published September 12, 2024

Christopher Gannatti, CFA

Global Head of Research

Key Takeaways

- The 30% rise in global cyberattacks in 2024 highlights the growing need for cybersecurity solutions.
- Despite rising demand, cybersecurity stocks have been highly volatile, affected by factors like interest rate sensitivity and exposure to early-stage companies.
- Some cybersecurity companies, like Palo Alto Networks and CrowdStrike, have shown resilience by recovering from significant stock price drops in 2024.

Check Point Research Reports Highest Increase of Global Cyber Attacks Seen in Last Two Years—A 30% Increase in Q2 2024 Global Cyber Attacks¹

Some of the notable events²:

- On August 23, 2024, Halliburton was impacted by a cyberattack and had to take certain systems offline.
- In February 2024, United Healthcare's Change Healthcare unit was breached. The fix is expected to cost United Healthcare \$2 billion in 2024 alone.
- In June 2024, CDK Global was breached. This company provides systems for auto dealerships, which struggled subsequently to complete sales.
- Microchip Technology indicated in August 2024 that a cyber breach had impacted its manufacturing facilities and ability to complete orders.

Data breaches and ransomware attacks seem to occur with an alarmingly regular cadence.

Do Cyber Breaches Portend Strong Returns for Cybersecurity Providers?

On initial view, they don't. The rate of breaches seems to always be going up, but cybersecurity providers have experienced a lot of share price volatility.

In our opinion, the existence of the attacks emphasizes the market need for protection as well as the market need to continue to evolve and improve that protection. The companies that can ultimately provide this will be in a position to serve a very important market demand.

Cybersecurity Software vs. Broader Software-as-a-Service (SaaS)

One way to highlight the strength of cybersecurity businesses is to compare them to a broader set of software stocks.

- 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 focused on companies that represent the future, in Team8's opinion, of where the cybersecurity megatrend is going. Team8 has delineated eight specific cybersecurity themes and every constituent must provide a strong solution serving at least one of these.
- The [WisdomTree Cloud Computing Fund \(WCLD\)](#), which is designed to track the total return performance, before fees and expenses, of the BVP Nasdaq Emerging Cloud Index, is focused on companies that provide software solutions to enterprises. BVP notes that each company is getting more than 50% of revenue from delivering cloud software solutions to enterprise customers, as well as delivering greater than 15% revenue growth. The specific use case of the software does not need to be focused on any particular type of solution, so it is a very broad-based representation of what businesses can use SaaS for.

Figure 1: Standardized Returns

Fund Name	Fund Ticker	Fund Inception Date	Fund Expense Ratio	Year-to-Date	1-Year	3-Year	Since Inception
WisdomTree Cybersecurity Fund (NAV)	WCBR	1/28/2021	0.45%	-1.03%	29.72%	1.06%	1.24%
WisdomTree Cybersecurity Fund (MP)	WCBR	1/28/2021	0.45%	-1.14%	29.29%	0.94%	1.21%
WisdomTree Cloud Computing (NAV)	WCLD	9/6/2019	0.45%	-9.61%	-0.38%	-17.30%	4.94%
WisdomTree Cloud Computing (MP)	WCLD	9/6/2019	0.45%	-9.64%	-0.41%	-17.36%	4.93%

Source: WisdomTree, specifically data from the Fund Comparison Tool in the PATH suite of tools, as of 6/30/24. 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 performance and to download the respective Fund prospectuses, click the relevant ticker: [WCBR](#), [WCLD](#).**

Cyber Stands Out

There has been a 48.2% difference in returns between [WCBR](#) and [WCLD](#) from essentially January 2021 to August 2024. Both [WCBR](#) and [WCLD](#):

- Have a high degree of interest rate sensitivity, which contributed to a very difficult period in 2022 while the Federal Reserve was raising its policy rate to combat inflation.
- Have high exposure to earlier stage high-growth companies that do not yet have positive earnings.
- Have high exposure to mid- and small-cap stocks because the weighting scheme is meant to emphasize pure play exposures and not market cap.
- Focus on SaaS businesses as the dominant business model that the constituent companies employ.

Figure 2: Cumulative Return Comparison: WCBR vs. WCLD



Source: WisdomTree, specifically data from the Fund Comparison Tool in the PATH suite of tools, as of 8/23/24. 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 performance and to download the respective Fund prospectuses, click the relevant ticker: [WCBR](#), [WCLD](#).

Figure 3 breaks down the overall history, which we showed in figure 2, into some different sub-periods. For us, the one-year period, as of August 22, 2024, was particularly notable:

- Both [WCBR](#) and [WCLD](#) experienced a rally toward the end of 2023. The catalyst for this rally was the market's expectation that the Fed had contained inflation and would have to start lowering its policy rate, quickly, in the early part of 2024.

Still, to see that [WCBR's](#) return was roughly 30% higher on a one-year basis, as of August 22, 2024, when measured against [WCLD](#)—that is a huge difference and one we would not have initially expected.

Figure 3: Massively Different Returns between WCBR & WCLD Are Persistent in Different Sub-Periods of the Total History



Source: WisdomTree, specifically data from the Fund Comparison Tool in the PATH suite of tools, for the period 1/27/21 to 8/22/24). 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 performance and to download the respective

Fund prospectuses, click the relevant ticker: [WCBR](#), [WCLD](#).

Conclusion: Do Cybersecurity Providers Exhibit Resilience?

When we speak to investors, there is clear demand for cybersecurity, but many expect the companies to almost exhibit defensive share price type of behaviors because the need for the services is not really changing week by week or month by month. Yet, the volatility of share prices has been with us and doesn't show signs of going away.

However, we are able to look at two examples of companies that exhibited massive drawdowns in 2024. First, Palo Alto Networks:

- In February 2024, Palo Alto Networks reported earnings. There was a quote that got a lot of attention on the earnings call: “We’re beginning to notice customers are facing spending fatigue in cybersecurity.” It was said by Nimesh Arora, chairman and CEO of the firm. It was, to be fair, part of a nuanced discussion of the firm’s customers and what they are facing, but it ended up being a great headline-grabber.
- Palo Alto was also, on the same call, discussing shifting their business model from being about individual products to being more about a broader platform of cybersecurity services. On the day of the announcement, which included lower revenue growth expectations in the near term, there was a huge drop in the share price—roughly 30% based on closing prices.

In figure 4, we show that in about six months, Palo Alto Networks had nearly re-attained its pre-drop levels. We believe this indicates a degree of resilience, but we also recognize that it did not come without serious volatility.

Figure 4: The Palo Alto Networks Share Price in 2024

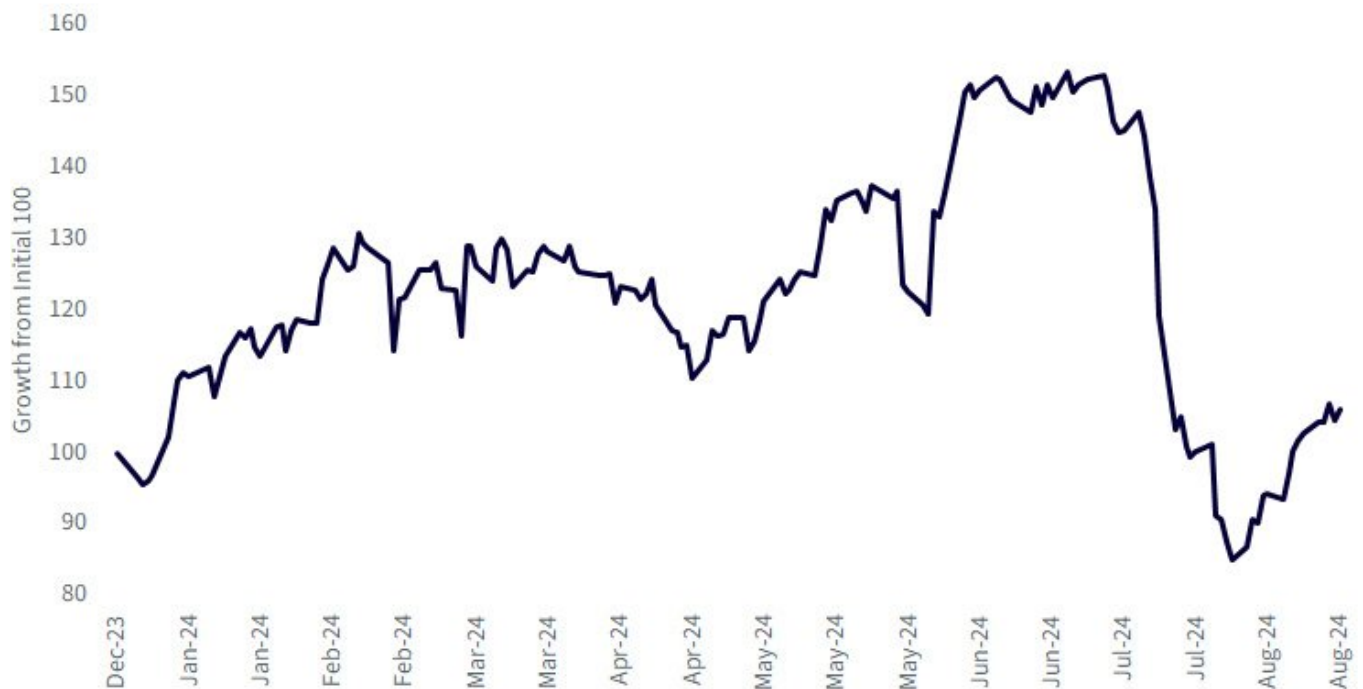


Source: www.macrotrends.net. As of 8/23/24, Palo Alto Networks was a 6.16% weight in WCBR and a 1.59% weight in WCLD. **Past**

performance is not indicative of future results. Holdings are subject to change.

Another company, CrowdStrike, also experienced a massive drawdown in 2024, and many of us experienced the “blue screen of death” on our Windows-based computers in July 2024 as a result. This was an unfortunate mistake—mistakes do happen—and it highlighted how systems have intricate interdependencies.

Figure 5: The CrowdStrike Share Price in 2024



Source: www.macrotrends.net. As of 8/23/24, Palo Alto Networks was a 6.16% weight in WCBR and a 1.59% weight in WCLD. **Past**

performance is not indicative of future results. Holdings are subject to change.

Our takeaway is that we have a megatrend, cybersecurity, that people and companies must remain attentive to. We don't know exactly which companies or technologies will be the winners, but that is one benefit of working with experts like Team8 and having their knowledge influence the WisdomTree Team8 Cybersecurity Index every six months. So far, cybersecurity has seemed to separate itself, performance-wise, from more general software solutions, and we think that the market demand for these kinds of services could continue over the coming years.

1 Check Point Team, "Check Point Research Reports Highest Increase in Global Cyber Attacks Seen in Last Two Years—A 30% Increase in Q2 2024 Global Cyber Attacks," blog.checkpoint.com, 7/16/24.

2 Source for bullets: Colin Kellaher, "Halliburton Hit by Cyberattack," *Wall Street Journal*, 8/23/24.

3 Source: Palo Alto Networks, Inc., Q2 2024 earnings call transcript, 2/20/24.

Important Risks Related to this Article

For current holdings of, please click the respective ticker: [WCBR](#), [WCLD](#). Holdings are subject to risk and change.

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 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.

WCLD: There are risks associated with investing, including the possible loss of principal. The Fund invests in cloud computing companies, which are heavily dependent on the Internet and utilizing a distributed network of servers over the Internet. Cloud computing companies may have limited product lines, markets, financial resources or personnel and are subject to the risks of changes in business cycles, world economic growth, technological progress and government regulation. These companies typically face intense competition and potentially rapid product obsolescence. Additionally, many cloud computing companies store sensitive consumer information and could be the target of cybersecurity attacks and other types of theft, which could have a negative impact on these companies and the Fund. Securities of cloud computing companies tend to be more volatile than securities of companies that rely less heavily on technology and, specifically, on the Internet. Cloud computing companies can typically engage in significant amounts of spending on research and development, and rapid changes to the field could have a material adverse effect on a company's operating results. 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.