

Cybersecurity Is National Security

Published September 27, 2021

Kara Marciscano, CFA

Associate, Research

Aaron Dubin

Director of Business Research, Team8

Cyber risk is one of the few tangible threats that we experience on an individual, national and global level all at once. The [WisdomTree Cybersecurity Fund \(WCBR\)](#) provides investors with targeted exposure to the businesses at the forefront of fortifying our networks and systems. It is based on the [WisdomTree Team8 Cybersecurity Index](#), a first-of-its-kind Index geared toward tracking innovations in cybersecurity made by public companies, which it does by leveraging data from cybersecurity expert and global venture group, Team8. The Fund just completed its September 2021 rebalance (done semiannually) with six additions at this rebalance cycle, and an average year-over-year revenue growth rate of 43%.¹

Commenting on the growth in cyber security and the importance of being able to differentiate between solutions, Admiral Michael Rogers, Operating Partner, Team8, explains: "Cyber security has been catapulted to the top of mind for the executive suite in recent years, accelerated by the pandemic. The cost of security for organizations contrasts with the relative low costs for cyber attackers. As such, firms that are prioritizing cybersecurity solutions that provide smart, cost-effective ways to reduce, mitigate, or even prevent cyber attacks is key. Inevitably, as we move to an increasingly digital world, these options are game-changers in safeguarding our society and digital future."

The changes made to the portfolio reflect the latest trends in cybersecurity, including the continued focus and evolution in the Security of Things, greater attention to injecting security throughout the development lifecycle and growth in ransomware protection.

WCBR Turnover and Fundamentals

[WCBR](#) had six additions at this rebalance cycle, with an average year-over-year growth rate of 43%. This subset of companies is internationally listed (across the United States, Canada and the United Kingdom) with focuses on data protection and management or network and endpoint security.

Company	Business Description	Weight	TTM Revenue Growth
Darktrace Plc	A provider of AI for the enterprise, with the first at scale deployment of AI in cyber security. It specializes in self-learning AI and is at the forefront of autonomous response technology. Darktrace's platform uses machine learning and AI algorithms to neutralize cyber threats across diverse digital estates, including the cloud and networks, IoT and industrial control systems.	5.1%	17.8%
SentinelOne, Inc.	Engages in the provision of endpoint security software that detects, models, and predicts threat behavior to block attacks on any computing device. Its services include vigilance, support, and training.	3.8%	142.1%
Sumo Logic, Inc.	Engages in the provision and development of continuous intelligence software platform. Its product enables organizations to automate the collection, ingestion, and analysis of application, infrastructure, security, and internet of things (IoT) data to derive insights.	3.8%	23.5%
Elastic NV	Engages in the provision of open source search and analytics engine services. It offers Elastic Stack, a set of software products that ingest and store data from various sources and formats, as well as perform search, analysis, and visualization. It also provides software solutions on the Elastic Stack that address cases, including app search, site search, enterprise search, logging, metrics, application performance management, business analytics, and security analytics.	3.8%	44.1%
Datto Holding Corp.	Engages in the provision of cloud-based software and technology services. Its cloud-based offerings include unified continuity, networking, and business management software solutions.	2.9%	14.9%
Absolute Software Corp.	Engages in the provision of cloud-based service that supports the management and security of computing devices, applications, and data for a variety of organizations. Its solutions includes education, financial services, general data protection regulations (GDPR) compliance, government, healthcare, professional services, and technology solutions such as Absolute for Android, and Absolute for Chromebook.	0.9%	15.4%

Sources: WisdomTree, FactSet, as of 8/31/21. TTM is an abbreviation for "trailing 12 months."

For definitions of terms in the table, please visit the [glossary](#).

The Fund had three removals, including Proofpoint, McAfee and FireEye. Proofpoint was acquired by private equity firm Thoma Bravo at a 34% acquisition premium.² Meanwhile, McAfee and FireEye were removed after their trailing revenue growth fell below the necessary threshold for current constituents of 5%.

Approximately 25% of the Fund's weight was turned over with no single current constituent experiencing a weight change significantly above 2%.

These changes brought the constituent count of the Fund up to 28 companies from 25. The weighting mechanism behind [WCBR](#) assigns over-weight exposure to companies that are exhibiting both fast revenue growth and involvement in an array of cybersecurity themes, which helped drive an increase in the weighted average trailing-12-month growth rate to 32.4% from 28.1%.

	# of Companies	TTM Growth Rate	Price-to-Sales Ratio	Total Market Cap	Weighted Average Market Cap	Median Market Cap	Average Market Cap	Large Cap	Mid-Cap	Small Cap
Before Rebalance	25	28.1%	10.5x	\$417bn	\$17bn	\$7bn	\$22bn	53%	42%	5%
After Rebalance	28	32.4%	12.0x	\$428bn	\$15bn	\$7bn	\$18bn	43%	51%	6%

Sources: WisdomTree, FactSet, as of 8/31/21.

For definitions of terms in the table, please visit the [glossary](#).

Team8 Update on Latest Cybersecurity Trends

Major cyber security attacks can bring about the greatest cybersecurity innovations, and we expect the last 6 months of cybersecurity to be no different. We leverage Team8's cybersecurity industry knowledge, our cyber domain experts, our diverse community of C-level executives and CISOs from Fortune 1000's, and the latest market and technology developments to track the evolution of cybersecurity themes driving growth in the industry. Several developments we've been seeing include:

- **Security of Things** – The endpoint, though perhaps one of the oldest security categories, continues to evolve with better behavioral anomaly detection, across more environments, and with more context from richer threat intelligence. Beyond traditional endpoints such as laptops and servers, lately there is also an increased focus on the security of physical supply chains and critical infrastructure such as oil, transportation, or food companies, as recent attacks have demonstrated just how brittle some of our most important infrastructure can be and the consequences they can have on our broader supply chain.
- **Shift-Left** – With the rise in software supply chain attacks in particular, we're seeing even greater attention go into injecting security throughout the development lifecycle, further bridging the gap between developers and security professionals. This can be seen with an increased focus on container/workload and application security solutions or solutions that help automate and orchestrate the software development life cycle and patch management; static application security testing (SAST), which analyzes source code to identify vulnerabilities; and an overall deeper integration of security into the continuous integration/continuous delivery pipeline. As more security professionals learn to code and more developers learn to implement security functionality, we will see the barriers between these team structures break down and the security bottlenecks shift with it.
- **Resilience & Recovery** – Ransomware has become a household word as cyber attackers fundamentally evolve their strategies from just stealing data or manipulating systems to business disruption and data extortion, which can sometimes be even more devastating for the victim and even easier for the attacker to monetize their crimes. This has led to the introduction of new government security directives and has spurred an increased focus on ransomware protection, data backup and disaster recovery, and business continuity solutions that can help companies get back to business in the face of a total system lockout or mission-critical system downtime. As the resilience “playbook” continues to develop, so too will the regulation and the various components of the toolbox to support it.

Cybersecurity as a Government Priority

Cybersecurity is an escalating and complex challenge requiring an equally robust and coordinated defense, which is why cybersecurity is one of the U.S. administration's highest priorities. President Biden recently held a cybersecurity summit with a range of private sector companies as a call-to-action to establish a public-private partnership to protect against malicious cyber activity.

Representatives from technology, insurance, education and critical infrastructure were present at the summit, including some of the nation's largest companies like Google, Amazon, Apple, Microsoft, IBM, ADP, JP Morgan, Bank of America and Travelers.

The meeting covered a range of topics focused on fortifying our critical infrastructure, driving better cybersecurity practices and increasing the cybersecurity workforce. The key outcome from the meeting was the announcement of substantial commitments and initiatives aimed at bolstering the nation's cybersecurity, a few of which we highlight below:

- Microsoft committed to invest \$20bn over 5 years to accelerate efforts to integrate cybersecurity in product design. The company made \$150mn immediately available in technical services to help federal, state, and local governments upgrade their security protection, and is expanding partnerships with community colleges and non-profits for cybersecurity training.
- Google is investing \$10bn over 5 years to expand zero-trust programs, help secure the software supply chain, and enhance open-source security. The company will also help 100,000 Americans earn industry-recognized digital skills certificates.
- Apple is establishing a new program to drive continuous security improvements throughout the technology supply chain. The program will help drive the mass adoption of multi-factor authentication, security training, vulnerability remediation, event logging, and incident response.
- IBM will train 150,000 people in cybersecurity skills over the next three years, and will partner with more than 20 Historically Black Colleges & Universities to establish Cybersecurity Leadership Centers to grow a more diverse cyber workforce.
- Amazon will make available to the public at no charge the security awareness training it offers its employees. Amazon will also make available to all Amazon Web Services account holders at no additional cost, a multi-factor authentication device to protect against cybersecurity threats like phishing and password theft.

A Historic Opportunity for the Cybersecurity Industry

"Cybersecurity is a national security and economic security imperative for the Biden Administration and we are prioritizing and elevating cybersecurity like never before."³

This statement from the White House and the commitments from the private sector signify the important role that the cybersecurity industry will play in both the public and private sectors going forward.

Diversifying Your Portfolio with Differentiated Cybersecurity Exposure

Investors may not have any exposure to companies captured in [WCBR](#)—the Fund provides differentiated exposures relative to broad-based benchmark indexes, which allocate at most 1% of their weight to the companies held in [WCBR](#).

To gain targeted exposure to the companies we view as having the highest exposure to critical cybersecurity trends with the greatest potential for future growth, we suggest investors consider adding [WCBR](#) to their portfolio.⁴

¹WisdomTree, FactSet, as of 8/31/21.

²<https://www.proofpoint.com/us/newsroom/press-releases/proofpoint-enters-definitive-agreement-be-ac>

quired-thoma-bravo-123-billion

3<https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/>

4Sources: WisdomTree, FactSet, S&P Global, FTSE Russell, Nasdaq. As of 6/31/21, the S&P 500, S&P 500 Growth, Nasdaq 100, Russell 1000 Growth and S&P 500 Information Technology Indexes held 0.1%, 0.2%, 0.4%, 1.1% and 0.5% of their weight in the companies held in WCBR.

Important Risks Related to this Article

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 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.

References to specific securities and their issuers are for illustrative purposes only and are not intended to be, and should not be interpreted as, recommendations to purchase or sell such securities.

This article represents the opinions of Team8 Labs Inc. ("Team8") and is for informational purposes only. You should not treat any opinion expressed by Team8 as a specific inducement to make an investment in any security, but only as an expression of Team8's opinions. Team8's statements and opinions are subject to change without notice. Team8 is not registered as an investment adviser under the Investment Advisers Act of 1940, as amended (the "Advisers Act"), and relies upon the "publishers' exclusion" from the definition of investment adviser under Section 202(a)(11) of the Advisers Act. As such, the information contained in this article does not take into account any particular investment objectives, financial situation or needs and is not intended to be, and should not be construed in any manner whatsoever as, personalized investment advice. The information in this article is provided for informational and discussion purposes only and is not intended to be, and shall not be regarded or construed as, a recommendation for a transaction or investment or financial, tax, investment or other advice of any kind by Team8. You should determine on your own whether you agree with the information contained in this article. Certain of the securities referenced in this article may currently, or from time to time, be constituents of an index developed and maintained by WisdomTree Investments, Inc. using data provided by Team8, which has been or will be licensed for a fee to one or more investment funds. In addition, certain officers or employees of Team8 or funds or other persons or entities affiliated or associated with Team8 may hold shares of, be officers or directors of, or otherwise be associated with some or all of the issuers of the securities referenced in this article or included in such index. Team8 expressly disclaims all liability with respect to any act or omission taken based on, and makes no warranty or representation regarding, any of the information included in this article.