Authored by:

Tejas Dessai
Research Analyst

Date: November 23, 2022
Topic: Thematic

Related ETFs

Please click below for fund holdings and important performance information.

BUG – Global X Cybersecurity ETF

CLOU - Global X Cloud Computing ETF

GLOBAL X ETFs RESEARCH

Cybersecurity: Discovering Growth in a Recession

The COVID-19 pandemic was fuel for the economy's digitization. Rapid adoption of cloud technology, multiplication of devices, and increase in data generation ended up straining existing systems, exposing gaps in enterprise defenses. Parallelly, cyberattacks saw a broad uptick worldwide. Both factors are now pushing global businesses to ramp up spending on security solutions. Cybersecurity pure-play vendors serving emerging demands across enterprise, consumer, and government use cases are seeing growth accelerate. This presents an opportunity for investors seeking exposure to growth themes amidst the ongoing macro-induced challenges.

Key Takeaways

- Cyberattacks are growing in frequency and sophistication. Security of digital operations continues to be a major concern for global enterprises.
- Leading cybersecurity solutions vendors are witnessing growth accelerate as security spending increases. Earnings display resilience in billings, revenues, and margins.
- We expect increasing use of technology to further strengthen tailwinds. Cybersecurity spend will likely continue to outpace the rest of the IT market in the near to medium term.

Attack Landscape Is Getting Worse

The threat of COVID-19 may be receding, but the increased digital activity that the pandemic spurred isn't. First, hybrid work remains popular and is likely to be standard practice for many businesses. Even if they're largely back in the office, employees expect to be able to work from anywhere. This dynamic enhances the surface area that enterprises must defend, requiring investment in specialized solutions.

Second, the conflict in Ukraine illustrates new threats that companies face. Hacking organizations, hacktivists, and criminal organizations are seen targeting infrastructures of nation states they do not agree with. Businesses are often caught in the middle, which has elevated cyber security from an engineering challenge to an executive concern. Even the U.S. government recommends businesses place tighter protections in place.[1]

Third, we appear to be in the middle of a broad digital transformation where enterprise data and applications are moving to the cloud. Securing this shift of data assets is a priority area of investment.

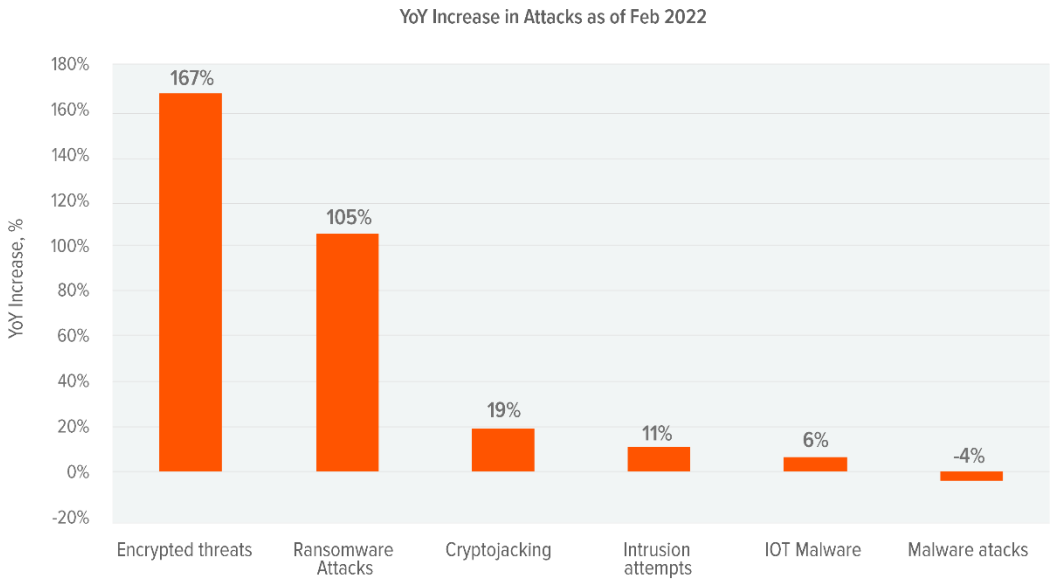
Fourth, the operational technology running critical infrastructure such as pipelines, dams, electric grids, and the industrial control systems running supply chains and production facilities are being digitized. Securing these nodes presents challenges for governments around the world.

The threat landscape is increasingly dangerous. For the first half of 2022, ransomware attacks grew nearly 52% year-over-year (YoY).[2] Ransom-ware-as-a-service attacks from well tracked and notoriously popular hacking organizations such as Conti and LockBit, which caused some of the worst ransomware outages during COVID, grew 500% YoY.[3] Encrypted threats continue to grow as well.[4] Other common attacks include Distributed denial of service (DDoS), malware, and simple attacks like phishing and social engineering. An average U.S. business can lose $9.4 million in a data breach.[5] The longtail impact of such

attacks can be far worse. Data assets, credentials, and company secrets are often seen changing hands on the dark web for decades after the attack.[6]

GLOBAL CYBERATTACKS CONTINUED TO INCREASE IN 2022

Sources: Global X ETFs with information derived from: Help Net Security. (2022, February 18). *Ransomware's savage reign continues as attacks increase 105%.*



Earnings Show Resilience

Cybersecurity businesses may be able to leverage strengthening tailwinds to accelerate growth. Cybersecurity companies grew revenues by approximately 19% year-over-year (YoY) for the most recently reported quarter on an annualized basis, up 680 basis points (bps) sequentially and 1,250 bps year-over-year (YoY).[7] In our view, this acceleration is the best evidence of increased enterprise spending.

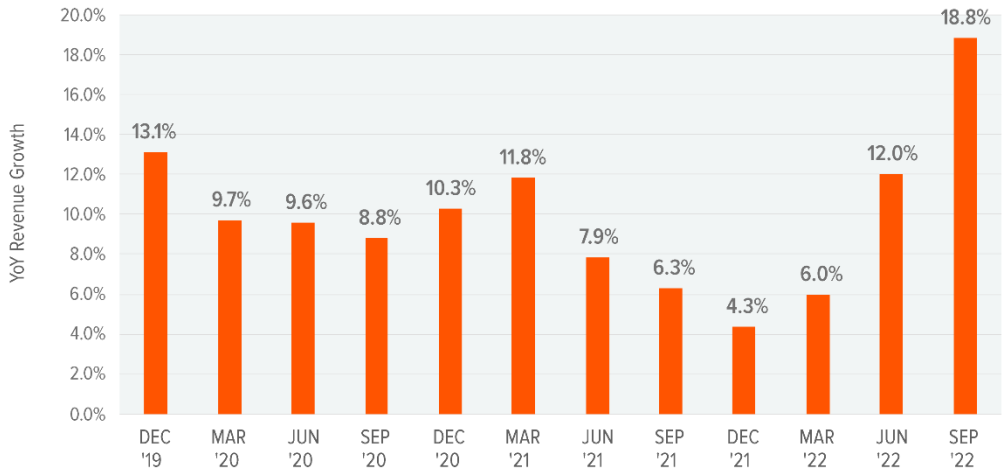
Looking deeper at the fundamentals of these companies, gross margins for cybersecurity companies remained healthy, averaging more than 70%.[8] Earnings before interest and taxes (EBIT) margins at -0.5% showed some contraction because of the current macro-induced hiccups.[9] Free cash flow margins were over 20%.[10]

Demand for subscription-first platforms is particularly strong. Palo Alto Networks, a network security software provider, grew its top line by 27% YoY for Q2 2022 and revised its Q3 2022 guidance to the upside.[11] Sales for CrowdStrike, a vendor of endpoint security software, grew its top line by ~59%, beating estimates by 3.6%.[12] CrowdStrike also raised its guidance.[13] Traffic monitoring software vendor ZScaler grew its top line by ~61% YoY and revised guidance to the upside.[14] Industry bellwethers Fortinet, Sentinel One, and Checkpoint all beat estimates for the last reported quarter.[15,16,17]

Many of these companies are also pushing innovative frameworks and approaches in a bid to capture incremental share. Zero Trust architecture is a comprehensive security framework that distrusts all software and hardware agents by default, thereby enforcing the need to verify each end system every time it interacts with a broader network.[18] Another emerging framework called SASE combines best practices of traditional network security with cloud-native security frameworks – allowing remote logins and endpoint interactions in a much more secure fashion.[19]

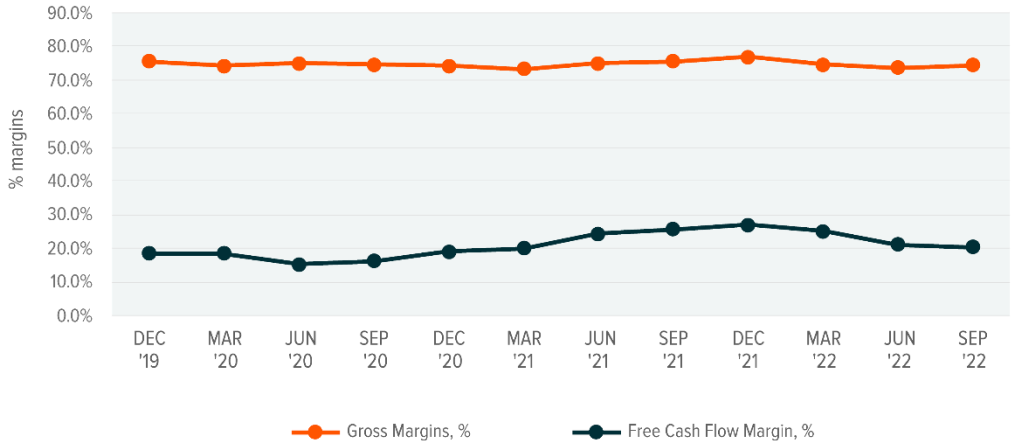
TRAILING 12 MONTHS REVENUE GROWTH (REPORTED EACH QUARTER) FOR INDXX CYBERSECURITY INDEX SHOWS ACCELERATION

Sources: FactSet Research Systems. (n.d.) [Data set]. Data as of September 30, 2022, and accessed on November 10, 2022



MARGINS FOR STOCKS PART OF INDXX CYBERSECURITY INDEX HAVE HELD STEADY EVEN AS MACRO PRESSURE PILE UP

Sources: FactSet Research Systems. (n.d.) [Data set]. Data as of September 30, 2022, and accessed on November 10, 2022



Cybersecurity M&A Hasn't Slowed Down

As the market grows, we believe that leading solution providers positioned as one-stop shops will be able to consolidate more share, boost margins, and grow more efficiently than their competition. Mergers and acquisitions (M&A) activity remains high with leading cybersecurity companies looking to acquire smaller startups and fill gaps in their product portfolios. Palo Alto Networks acquired Apiiro for $600 million in September.[20] CrowdStrike acquired Humio for $400M in Nov 2021.[21]

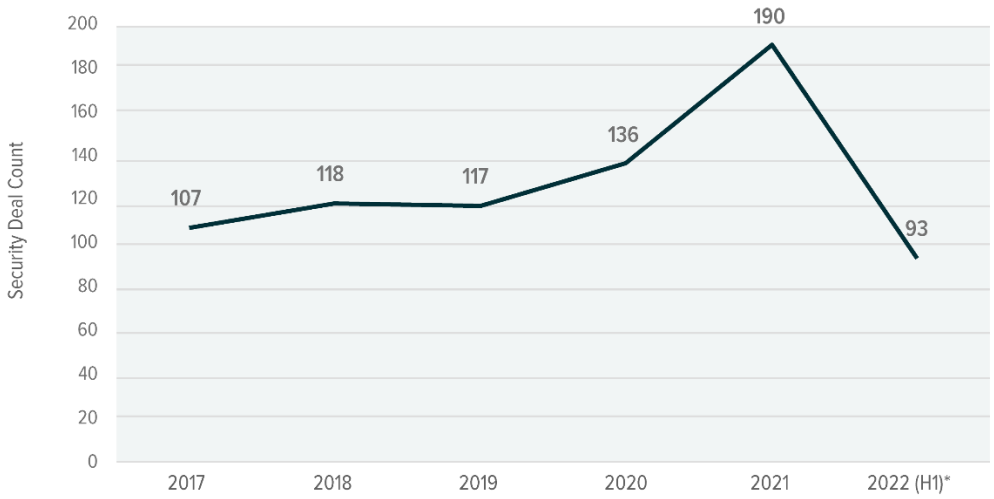
Other potential buyers of cybersecurity companies include big cloud franchises and hyperscalers looking to bolster their existing infrastructure software portfolios. For these companies, security software can be

a way to retain large clients and improve margins. Also, private equity companies are becoming major players in cybersecurity M&A. The playbook is simple: Buy smaller cyber businesses within a specific category and bundle them to create a market dominating player.

Most recent cybersecurity acquisitions were completed at a premium to the rest of the technology market. As of June 2022, the median deal multiple for deals announced was at over 9 times revenues, nearly 25% higher than average sales multiple for cybersecurity companies.[22]

CYBERSECURITY M&A REMAINED HIGH IN H1* 2022

Sources: Global X ETFs with information derived from: Williams, J., & Nazir, D. (2022, July 22). Cybersecurity M&A still hot in Q2, but economic uncertainties weigh on outlook. S&P Global Intelligence. *Indicates first half of 2022.



SUMMARY OF MAJOR CYBER SECURITY ACQUISITIONS IN THE LAST 12 MONTHS, LIMITED TO DEALS VALUED AT OVER $1 BILLION

Sources: Global X ETFs with information derived from: Crunchbase Data. (n.d.). [Data set]. Accessed on October 25, 2022.; Momentum Cyber. (n.d.). Home. Accessed on October 25, 2022.; Security Week. (2022). Accessed on October 25, 2022.; Company Press Releases.

Announced Date	Target	Acquirer	Enterprise Value ($M)	Sector
Nov-21	McAfee	Advent International	$14,085	Consumer security application
Apr-22	Sailpoint	Thoma Bravo	$6,900	Identity & Access Management
Apr-22	Datto	Kaseye	$6,200	Data Security
Aug-22	Microfocus	Opentext	$5,656	Application Security
Dec-21	Mimecast	Primera	$5,516	Messaging Security
Nov-21	Quest	Clearlake Capital	$5,400	Identity & Access Management
Mar-22	Mandiant	Google	$5,326	Security Operations & Incident Response
Oct-22	KnowBe4	Vista Equity Partners	$4,600	Identity & Access Management
May-22	ManTech	Carlyle Group	$4,200	Defense Contractor
Apr-22	Baracuda	KKR	$4,000	Network & Infrastructure Security
Aug-22	Ping Identity	Thoma Bravo	$2,793	Identity & Access Management
Mar-22	Veracode	Taassociates	$2,500	Application Security
Dec-21	Sirius Computer Solutions	CDW	$2,500	Cybersecurity Consulting
Oct-22	ForgeRock	Thoma Bravo	$2,300	Identity & Access Management
Apr-22	Watchdog	Vector Capital	$1,500	Network & Infrastructure Security
Mar-22	Hub	Mount Rainer	$1,201	Network & Infrastructure Security
Feb-22	Linode	Akamai	$900	Cloud Security

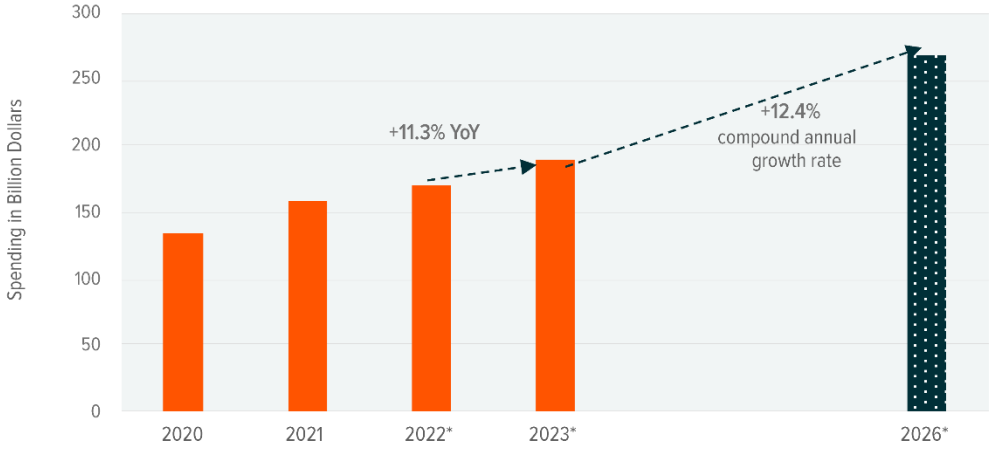
Governments Expected to Ramp Up Cyber Spending

Securing the online operating environment for businesses is a priority for governments around the world. Global businesses lost nearly $6 trillion annually to cybercrime because of lost data, penalties, productivity loss, ransoms, and attacks that led to total business failure.[23] Cybercrime's impact can be particularly damaging for small businesses.

The U.S.' fiscal year 2023 budget increased cybersecurity spending by nearly 10% YoY.[24] The budget included $11 billion for the Department of Defense to implement zero-trust architecture across its vendor systems.[25] In addition, the Infrastructure and Jobs Act included a couple billion dollars to secure local government assets.[26] We believe the U.S. government's commitment to cybersecurity may be a sign of cyber spending to come as other governments ramp up their defense.

SECURITY SPENDING IS EXPECTED TO GROW AT 12%+ RATES THROUGH 2026

Sources: Global X ETFs with information derived from: Upadhyay, S., Yadav, R., Wah, M., Messett,D., Smith, N., Rakheja,S., Kim, E., Contu, R., & Canales, C. (2022, June 30). Forecast: Information security and risk management, worldwide, 2020-2026, 2Q22 update. Gartner Research.* indicates forecast.



Conclusion: Cybersecurity Appears Well Positioned in This Recession

Cybersecurity must evolve in lockstep with broader technology. As attacks rise and businesses consume more technological products, the importance of cyber defenses will be paramount. Even in a potential recessionary environment in 2023, we believe security spending will be the last item squeezed. Chief Information Officers around the world call out cybersecurity as a top priority budget item in 2023.[27] It is estimated that global security spending will grow ~7% to more than $165 billion in 2022, following ~14% growth in 2021 and nearly 7% in 2020.[28,29]

Spending is expected to be particularly visible in cloud security, end point security, data security, ID and access management, and infrastructure security, which were brought into focus by computing needs surfaced during the pandemic. Nearly 50% of all cybersecurity spending today goes to custom services, and cloud deployed solutions can also attack this pocket.[30]

Overall, we expect spending growth rates to likely remain elevated over the next 5 years, boosted by appetite for more scalable cloud-deployed solutions. Meanwhile, cybersecurity stocks are trading down 28% year-to-date as of Nov 10, 2022.[31] Given this growth trajectory and pullback, we see attractive potential upside for the theme.

Footnotes

1. Cybersecurity & Infrastructure Security Agency (CISA). (n.d.). *Shields up*. Accessed on November 3, 2022.
2. Trend Micro Incorporated. (2022, August 31). *Trend Micro warns of 75% surge in ransomware attacks on Linux as systems adoptions soared.*
3. Ibid.
4. Poireault, K. (2022, August 30). Ransomware attacks on the rise in 2022. Iapp.

5. IBM Security. (2022, August 1). *Cost of a data breach 2022: A million-dollar race to detect and respond*. IBM.
6. Help Net Security. (2021, October 21). *Increased activity surrounding stolen data on the dark web.*
7. Refers to stocks part of the Indxx Cybersecurity Index. Data derived from FactSet, on November 10, 2022.
8. Refers to stocks part of the Indxx Cybersecurity Index. Data derived from FactSet, on November 10, 2022.
9. Refers to stocks part of the Indxx Cybersecurity Index. Data derived from FactSet, on November 10, 2022.
10. Refers to stocks part of the Indxx Cybersecurity Index. Data derived from FactSet, on November 10, 2022.
11. Palo Alto Networks. (2022, August 22). Palo Alto Networks reports fiscal fourth quarter and fiscal year 2022 financial results [Press release].
12. CrowdStrike. (2022, August 30). *CrowdStrike reports second quarter fiscal year 2023 financial results*.
13. Ibid.
14. Bansal, T. (2022, September 8). *Zscaler reports fourth quarter and fiscal 2022 financial results*. Zscaler.
15. Fortinet. (2022, November 2). *Q3 2022 financial results* [PowerPoint slides].
16. Schwed, G., Payne, T., & Meintzer, K. E. (2022, October 27). *2022 third quarter financial results.* Check Point.
17. SentinelOne. (2022, August 31). *SentinelOne announces second quarter fiscal year 2023 financial results* [Press release].
18. Raina, K. (2022, October 17). *Cybersecurity 101: Zero trust security: Zero trust security explained: Principles of the zero trust model*. CrowdStrike.
19. Zscaler. (n.d.). *Resources: Security terms glossary: What is secure access service edge (SASE)*? Accessed on November 3, 2022.
20. Orbach, M. (2022, September 19). *Palo Alto Networks on verge of $600 million acquisition of Apiiro*. CTech.
21. CrowdStrike. (2022, June 6). *CrowdStrike introduces humio for falcon, redefining threat hunting with unparalleled scale and speed* [Press release].
22. CrowdStrike. (2022, June 6). *CrowdStrike introduces humio for falcon, redefining threat hunting with unparalleled scale and speed* [Press release].
23. Tech Xplore. (2022, May 10). *Global cost of cybercrime topped $6 trillion in 2021: Defence firm*.
24. Jones, D. (2022, March 30). *Biden administration's FY 2023 budget includes 11% increase for cyber*. Cybersecurity Dive.
25. Austin III, L, J. (2022, March 28). *The department of defense releases the president's fiscal year 2023 defense budget*. U.S. Department of Defense.
26. BGR Group. (n.d.). *Infrastructure investment and jobs act – Cybersecurity*. Accessed on November 3, 2022.
27. Rosenbush, S. (2022, October 17). Cybersecurity tops the CIO agenda as threats continue to escalate. *The Wall Street Journal*.
28. Gartner. (2021, May 17). *Gartner forecasts worldwide security and risk management spending to exceed $150 billion in 2021* [Press release].
29. Gartner. (2022, October 13). *Gartner identifies three factors influencing growth in security spending* [Press release].
30. Ibid.
31. Measured by the Indxx Cybersecurity Index. Data derived from FactSet, on November 10, 2022

Glossary

The **Indxx Cybersecurity Index** is designed to track the performance of companies that operate in the cybersecurity industry.

Index returns are for illustrative purposes only and do not represent actual Fund performance. Index returns do not reflect any management fees, transaction costs or expenses. Indexes are unmanaged and one cannot invest directly in an index. Past performance does not guarantee future results.

This material represents an assessment of the market environment at a specific point in time and is not intended to be a forecast of future events, or a guarantee of future results. This information should not be relied upon by the reader as research or investment advice regarding the fund or any stock in particular.

Investing involves risk, including the possible loss of principal. Cybersecurity Companies are subject to risks associated with additional regulatory oversight with regard to privacy/cybersecurity concerns. Declining or fluctuating subscription renewal rates for products/services or the loss or impairment of intellectual property rights could adversely affect profits. The investable universe of companies in which the Funds may invest may be limited. The Funds invest in securities of companies engaged in Information Technology, which can be affected by rapid product obsolescence and intense industry competition. International investments may involve risk of capital loss from unfavorable fluctuation in currency values, from differences in generally accepted accounting principles or from social, economic or political instability in other nations. The Funds are non-diversified.

Shares of ETFs are bought and sold at market price (not NAV) and are not individually redeemed from the Fund. Brokerage commissions will reduce returns.

Carefully consider the funds' investment objectives, risks, and charges and expenses before investing. This and other information can be found in the funds' full or summary prospectuses, which may be obtained at globalxetfs.com. Please read the prospectus carefully before investing.

Global X Management Company LLC serves as an advisor to Global X Funds. The Funds are distributed by SEI Investments Distribution Co. (SIDCO), which is not affiliated with Global X Management Company LLC or Mirae Asset Global Investments. Global X Funds are not sponsored, endorsed, issued, sold or promoted by Indxx, nor does Indxx make any representations regarding the advisability of investing in the Global X Funds. Neither SIDCO, Global X nor Mirae Asset Global Investments are affiliated with Indxx.