

Cybersecurity Investment Case: Unique, Defensive Play within Thematic Tech

April 2024

Sanjana Prabhakar, *Index Research Specialist*

What is cybersecurity?

Cybersecurity involves both measures and technologies that protect digital systems, networks, and data from unauthorized and/or unintended access. It has become a top priority for businesses and governments alike as cyber attacks have risen over the recent years due to several factors including the rise of connected devices, shift to the cloud, remote work, and increased network complexity.

The most common types of cybersecurity attacks include malware, ransomware, phishing, insider threats, DDoS (distributed denial of service) and social engineering-based attacks¹. As a defense against these attacks, companies have developed comprehensive defense tools that span network security, endpoint security, cloud security, application security, IAM (identity & access management) and data security².

Why is cybersecurity important?

Cybersecurity has become critical to ensuring that organizations are safe from attacks both from internal and external bad actors as the world continues to become more open, connected, and digital. It has been flagged as a top 20 risk by the World Economic Forum, along with other pressing global issues such as climate change, debt crisis, food insecurity, poverty, refugee crises.

Statistics validate what is now indisputable in the cybersecurity community, that both the cost and number of cyberattacks continue to increase at an alarming rate. As per a study by Statista, the cost of cybercrime amounted to a whopping \$8.2 trillion in 2023 and is expected to rise to \$13.8 trillion by 2028. Cyber attacks continue at the rate of every 39 seconds, as per another study by University of Maryland³. If measured as a country, cybercrime would be the third-largest economy after U.S. and China.

Additionally, ongoing pressures from geopolitical tensions and the rise of generative AI have added a layer of complexity to the threat landscape. Given the scale of impact of cyber attacks, it comes as no surprise that 96% of CEOs surveyed by Accenture said that cybersecurity is critical to organization stability.

What is the state of the cybersecurity industry?

The landscape of the cybersecurity industry is changing rapidly with the emergence of new growth drivers by way of generative AI. Companies in the cybersecurity industry face a demand and operating environment quite different from that of the previous decade with the rise of insider threats and demand for AI-driven security solutions. Following the attacks on U.S. critical infrastructure, cybersecurity became a national policy

¹ <https://www.ibm.com/topics/cybersecurity>

² <https://www.accenture.com/us-en/insights/cyber-security-index>

³ <https://ung.edu/continuing-education/news-and-media/cybersecurity.php>

issue, leading to the issuance of an 'Executive Order on Improving the Nation's Cybersecurity' in May 2021 by President Biden. Since the issuance of the Executive Order, the government has upped the regulatory ante by releasing the U.S. National Cybersecurity Strategy in 2023, following which several federal agencies have published new cybersecurity requirements and guidelines. Big Tech companies have pledged to ramp up investments in cybersecurity, adding another stabilizing force to the revenue growth trajectory of the overall market.

The new narrative of cybersecurity is likely to be dominated by the zero-trust model of security and AI-based security solutions. The zero-trust security model assumes that no user or device can be trusted without continuous verification. An estimate of the total addressable market by McKinsey suggests that the cybersecurity market is \$1.5-\$2.0 trillion globally, and at best only 10% penetrated with a very long runway for growth. As per Statista, during the period 2024-2028, cybersecurity revenue is expected to grow at an annual rate of 10.6%, resulting in a total market size of \$273.6 billion by 2028. These projections suggest that the growth outlook is optimistic for the overall market and not limited to a few key players.

While the threat environment continues to drive strong demand for cybersecurity, there are risks from greater budget scrutiny and longer sales cycles. Management teams appear to have factored in these risks, as evinced by the conservative stance they have adopted on earnings calls. Additionally, companies are prioritizing certain areas of cybersecurity such as privileged access management (PAM) and Identity over others, as a response to recent high-profile attacks, including UnitedHealth, MGM Resorts International, Caesars Entertainment.

For the rest of 2024, there is expected to be higher demand for endpoint security, privileged access management and SASE (Secure Access Server Edge) versus other areas of cyber security, as per management commentary on earnings calls. This is likely to offset the slowdown in growth in areas such as firewall.

Cybersecurity Ecosystem Expansion

The cybersecurity ecosystem has expanded rapidly over the past decade or so, with the rise of generative AI as a potential new growth driver. Given the vastness of the attack surface, it comes as no surprise that there are solutions tailored to protect different parts of the attack surface, including firewalls, emails, networks, and the cloud. While there is increasing demand from customers for a single unified solution to prevent tool sprawl, the current landscape is still dominated by companies specializing in one or two areas of cybersecurity versus companies becoming a one-stop shop.

As it currently stands, cybersecurity companies offer more than a dozen offerings with a heightened focus on providing solutions to customers moving workloads to the cloud. The range of offerings by companies in the space include API security, email security, endpoint security, vulnerability management, identity, and access management (IAM), user entity and behavior analysis (UEBA), intrusion detection/prevention system (IDS/IPS), DDoS Mitigation, IoT Security, intrusion detection/prevention system (IDS/IPS), and security orchestration, automation, and response (SOAR).

While there is a potential for increasing revenue streams by specializing in multiple offerings, cyber security companies continue to focus on a few areas. Zscaler, for example, which went public in 2018, specializes in cloud-based security for protection against malware. Qualys and Rapid 7, which went public in 2012 and 2015 respectively, offer vulnerability management as well as identity and access management services. Okta, which went public in 2017, offers identity and access management solutions. Palo Alto Networks, which went public in 2012, offers enterprise-wide network and cloud security solutions. Darktrace, which went public more recently in 2021, is a leader in the global-AI cybersecurity domain. It has a self-learning AI tool that is

the industry's only solution to learn from data without reference to historical events. These examples illustrate the diversity of offerings by cyber security companies.

Tailwinds

Federal government agencies are expected to provide a fillip to cybersecurity sales as they work towards implementing zero trust architecture to comply with Executive Order 14028, "Improving the Nation's Cybersecurity"⁴. They are likely to upgrade their legacy IAM infrastructure, implement cloud security controls and upgrade risk controls as they ramp up their cybersecurity infrastructure⁵.

In keeping with the changing requirements, the Biden administration is seeking \$13 billion in cybersecurity funding across all agencies, with a fiscal 2025 proposal to include \$3 billion for the Cybersecurity and Infrastructure Agency, a \$103 million increase over the current budget⁶. The budget is likely to secure funding for improving basic and advanced cybersecurity in low-resourced hospitals and the treasury department's IT systems⁷.

The ongoing shift to the cloud has spurred higher demand for cloud-based security products. Cloud-based environments are more complex to secure than on-premise environments, necessitating new solutions. Some players - including CrowdStrike, Zscaler, Palo Alto, Cloudflare, Fortinet - are likely best positioned to capitalize on increased demand for cloud-based solutions. While security software continues to be a smaller market than infrastructure software and application software, the migration to the cloud is likely to propel the security market forward to an impressive \$290 billion by 2026, as per Bloomberg and IDC⁸. The pace of growth in security spending is even more encouraging when we note that overall security spend is likely to outpace IT spend by 200 bps through 2027⁹.

Interest rate cuts in the second half of the year could be another potential tailwind for companies in the cybersecurity universe, lifting valuations and boosting investor sentiment. As many of these stocks belong to the high-growth universe, they came under pressure when the Federal Reserve embarked on its most aggressive rate hiking cycle in decades.

Regulatory environment

Cybersecurity has become a national policy issue as evinced by the steps taken by the Biden-Harris administration in recent years to strengthen the cybersecurity framework for federal agencies, public and private enterprises.

Regulations worth noting include the National Security Strategy, Executive Order 14028 (Improving the Nation's Cybersecurity), National Security Memorandum 5 (Improving Cybersecurity for Critical Infrastructure Control Systems), M-22-09 (Moving the U.S. Government Toward Zero-Trust Cybersecurity Principles), and National Security Memorandum 10 (Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems)¹⁰. These strategies are likely to incentivize participants to make investments in cybersecurity for the long-term.

⁴ <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

⁵ https://www.ey.com/en_us/government-public-sector/top-seven-government-and-public-sector-cyber-trends

⁶ <https://federalnewsnetwork.com/budget/2024/03/biden-budget-request-includes-13b-for-cybersecurity-continuing-upward-trend/>

⁷ <https://www.bankinfosecurity.com/us-federal-budget-proposes-275b-for-cybersecurity-a-24575>

⁸ <https://www.bloomberg.com/professional/insights/trading/cloud-security-remains-in-secular-growth-mode-with-a-long-runway/>

⁹ <https://www.bloomberg.com/professional/insights/trading/cloud-security-remains-in-secular-growth-mode-with-a-long-runway/>

¹⁰ <https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/02/fact-sheet-biden-harris-administration-announces-national-cybersecurity-strategy/>

More recently, the SEC's 4-day breach disclosure rule went into effect for large public enterprises in December 2023, and is likely to be a near-term tailwind for growth. State-issued data privacy laws are expected to go into effect in July 2024 in Oregon, Texas, Montana, and Florida following California's CCPA laws that went into effect in January 2020¹¹. Further, zero trust mandates by the White House are likely to be implemented by federal agencies in 2024, with a focus on the categorization and securing of sensitive data, device inventory and visibility, and DNS/HTTP traffic encryption¹².

How to invest in the cybersecurity theme?

Investors can gain access to the cybersecurity space through the ISE Cyber Security UCITS™ Index (HUR™). The index consists of two kinds of cybersecurity companies including Infrastructure Providers and Service Providers. Infrastructure Providers include companies that provide hardware and software for cyber security and for which cyber security business activities are a key driver of the business. Service Providers, on the other hand, provide ancillary cybersecurity services such as consulting or monitoring.

Each component in the index must have a float-adjusted market capitalization of at least \$100 million and a three-month average daily dollar trading volume of at least \$1 million¹³. In addition, new additions into the index must also have a minimum five-day rolling average daily value traded over the previous 60 trading days of \$750 thousand¹⁴.

How are cybersecurity companies leveraging AI?

AI has emerged as a double-edged sword for cybersecurity companies. Bad actors have developed new attack strategies with generative AI. They are automating attacks, scanning wider attack surfaces, and targeting a broader range of victims. As these attacks are distinct by nature, they require more sophisticated solutions. On the flip side, cybersecurity companies are leveraging AI to automate threat response including prevention, detection, and response capabilities.

Several companies that make up the ISE Cyber Security UCITS Index (HUR) have brought to the market AI-based cybersecurity products and services, with a few companies ahead of the curve. Blackberry released CylancePROTECT, which delivers threat prevention powered by AI to identify threats before they cause harm. CrowdStrike announced a new AI-powered generative assistant called Charlotte AI in May 2023 to help users operate as a security professional. It announced a new AI-powered indicator of attack (IoA) model, which uses machine learning intelligence to stop breaches in real-time. Okta hasn't released an AI-based security product yet, but has announced that it will allocate \$40 million of its annual R&D to new AI projects. Generative AI-based solutions have also been leveraged quite rapidly. Zscaler has released AI-powered controls which use generative AI to improve threat detection and response. SentinelOne uses generative AI to stop attacks, combining a real-time neural network with a large language-model (LLM)-based natural language interface. Cloudflare released a tool called Cloudflare One, which uses generative AI tools without putting data at risk. The integration of AI into security offerings is expected to potentially act as a fillip to growth for companies in the near-term.

¹¹ <https://www.pillsburylaw.com/en/news-and-insights/consumer-privacy-laws-united-states-2024>

¹² <https://www.pwc.com/us/en/tech-effect/cybersecurity/zero-trust-security-cisas.html>

¹³ https://indexes.nasdaqomx.com/docs/Methodology_HXR.pdf

¹⁴ https://indexes.nasdaqomx.com/docs/Methodology_HUR.pdf

M&A Activity

M&A activity in the cybersecurity industry remained robust in 2022 and 2023, quite in contrast to overall M&A activity which was relatively subdued due to macroeconomic and geopolitical challenges^{15,16}. The table below illustrates the range of acquisitions in the cybersecurity space, with two big-ticket deals of note including Broadcom's \$61 billion acquisition of VMware and Cisco's \$28 billion acquisition of Splunk. Cisco's \$28 billion acquisition of Splunk, which was announced in September 2023, was the largest deal in the technology sector in 2023. This acquisition signaled to other participants Cisco's commitment to transition from a hardware-based business model to a more stable software-focused, recurring revenue model. It will allow Cisco to compete more effectively in a hybrid, multi-cloud and AIOps-driven world, and will position it as one of the dominant players in the Security and Information Event Management (SIEM) sub-segment.

Google's \$5.4 billion acquisition of Mandiant in 2022 sent a signal to market participants that cybersecurity, in particular cloud security, is a top priority for Big Tech companies. Mandiant, which was under the FireEye umbrella before it was rebranded, is credited for unearthing the high-profile SolarWinds hack¹⁷. This acquisition is also likely to help Google compete more closely with Amazon in the cloud cybersecurity space with a cyber defense toolkit that is more proactive than reactive in its operation¹⁸. The fragmented nature of the cybersecurity industry has lent itself to acquisition activity by private equity funds as well, including Thomas Bravo, Vista Equity, Crosspoint Capital Partners, and Carlyle.

With the Federal Reserve signaling initial rate cuts in 2024, the outlook for M&A activity in the U.S. is expected to improve, with M&A activity in the cybersecurity industry likely to receive a boost as well.

| Target | Acquirer | Deal Value | Announcement Date | Premium |
|------------------------|-----------------------------|---------------|-------------------|---------|
| Juniper | HPE | \$ 14 billion | 1/9/2024 | 32% |
| Splunk | Cisco | \$28 billion | 9/21/2023 | 31% |
| Absolute Software | Crosspoint Capital Partners | \$870 million | 5/16/2023 | 34% |
| Micro Focus | Open Text | \$5.8 billion | 31/1/2023 | 99% |
| KnowBe4 | Vista Equity | \$4.6 billion | 10/12/2022 | 44% |
| Ping Identity | Thoma Bravo | \$2.4 billion | 8/3/2022 | 63% |
| VMware | Broadcom | \$61 billion | 5/26/2022 | 44% |
| ManTech International | Carlyle | \$4.2 billion | 5/16/2022 | 17% |
| SailPoint Technologies | Thoma Bravo | \$6.9 billion | 4/11/2022 | 48% |
| Tufin | Turn/River | \$570 million | 4/6/2022 | 44% |
| Mandiant | Google | \$5.4 billion | 3/8/2022 | 57% |
| Mimecast | Permira | \$5.8 billion | 12/7/2021 | 16% |
| Talon Cybersecurity | Palo Alto | \$625 million | 11/6/2023 | |
| Ermetic | Tenable Holdings | \$265 million | 10/8/2023 | |
| Perimeter 81 | Check Point Software | \$490 million | 9/7/2023 | |

¹⁵ <https://www.pwc.com/us/en/industries/tmt/library/technology-deals-outlook.html>

¹⁶ <https://www.skadden.com/insights/publications/2023/12/2024-insights/corporate-trends/global-ma-activity>

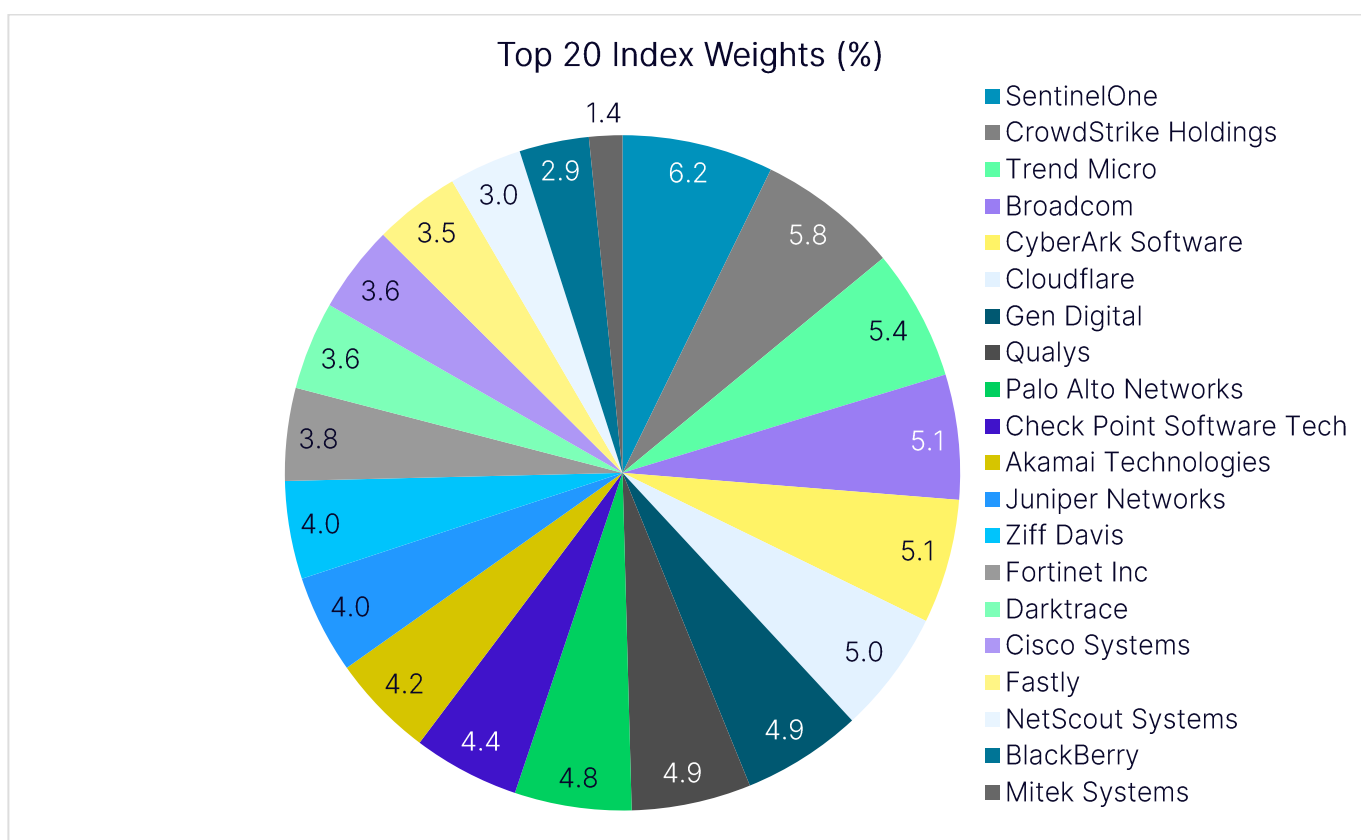
¹⁷ <https://www.cnn.com/2022/03/08/google-plans-to-acquire-mandiant-for-5point4-billion.html>

¹⁸ https://www.theregister.com/2022/10/11/google_mandiant_brain/

Top 20 Index Weights

As of December 29th 2023, there were 41 constituents in the ISE Cyber Security UCITS Index (HUR) index. The top 20 companies represent 85.7% of the total index weight, while the top 10 companies represent 51.6% of the total index weight.

The top 20 names include the likes of two well-known telecom hardware providers (Cisco and Juniper Networks), a diversified semiconductor provider (Broadcom), and several pure-play cybersecurity companies including SentinelOne, CrowdStrike, Trend Micro, CyberArk, Cloudflare, Qualys, and Palo Alto Networks. These companies span multiple sub-sectors of the Technology and Telecommunications industries, including software, semiconductors, telecommunications equipment, computer services and consumer digital services. Software, with an index weight of 48.2%, has the highest total index weight of all sub-sectors. These companies are at the forefront of innovation in cybersecurity and have launched security tools that protect endpoints, networks, and cloud environments. Recently, they have been integrating AI into their security tools to simplify operations and increase efficiency.

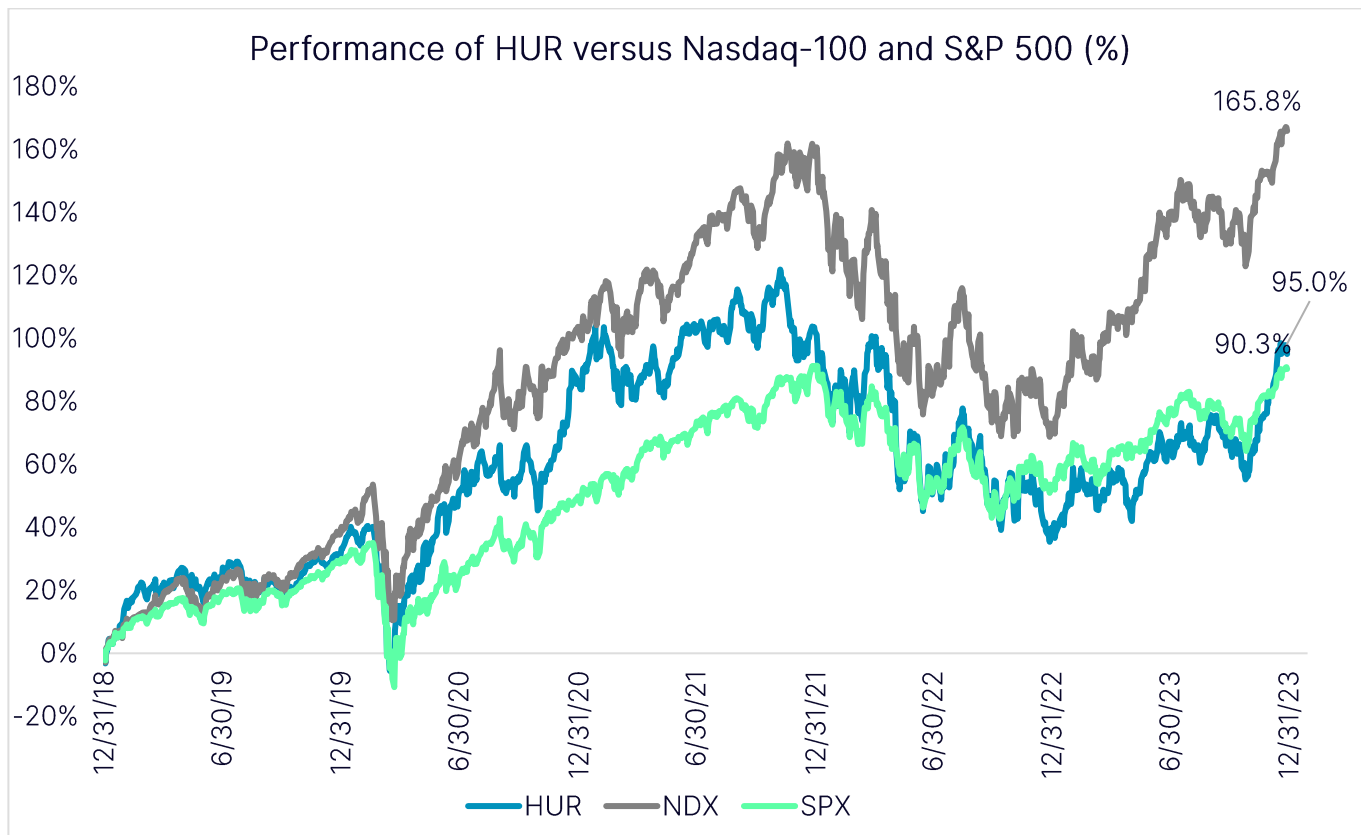


Performance vs. Competitor Indexes

For the five-year period ending December 29, 2023, the HUR index generated positive price returns of 95.0%, outperforming the S&P 500 by 5 percentage points, while underperforming the Nasdaq-100® by 71 percentage points.

For the full year 2023, the HUR index generated returns of 39.7%, outperforming the S&P 500 by 16 percentage points while underperforming the Nasdaq-100 by 14 percentage points.

As of March 28, 2024, the HUR index generated year-to-date returns of 1.8%, underperforming the Nasdaq-100 and the S&P 500, which generated returns of 8.7% and 9.9% respectively.



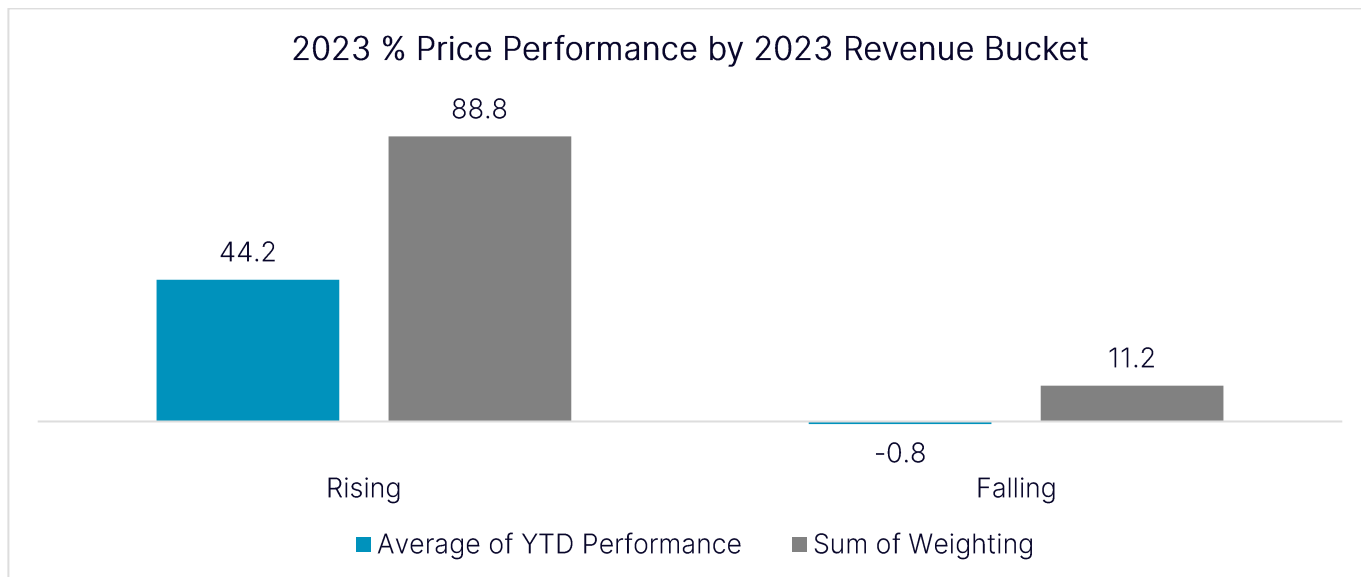
Revenue and correlation to performance

For the full year 2023, 34 of 41 companies (88.8% of index weight) tracked by the index grew their revenues by 17% on average, due to strong demand for cybersecurity products, with AI and cloud transformation boosting revenue growth. Several companies that make up the HUR index were able to post strong revenue growth despite headwinds from greater scrutiny on IT budgets. For example, CrowdStrike reported one of its best quarters in history in 2023, beating expectations on all metrics. Its total revenues grew by 33% y-o-y, with its ARR (annualized recurring revenues) growing by 34% y-o-y, largely due to the rapid growth in cloud and identity segments¹⁹. Other companies in the index including Cisco Systems and A10 Networks were weighed down by weaker demand from service providers, while Qualys was pressured by exposure to legacy virtual environments.

For the rest of 2024, the outlook for revenue growth for the index constituents remains cautiously optimistic. It is expected to be driven by robust demand for cybersecurity solutions, particularly from zero trust, as well as AI and cloud-related tailwinds, but somewhat offset by risks from longer sales cycles.

In terms of fundamentals leading performance, companies with revenues that grew in 2023 outperformed companies with revenues that declined, by an average of 45 percentage points.

¹⁹ <https://ir.crowdstrike.com/news-releases/news-release-details/crowdstrike-reports-fourth-quarter-and-fiscal-year-2024>

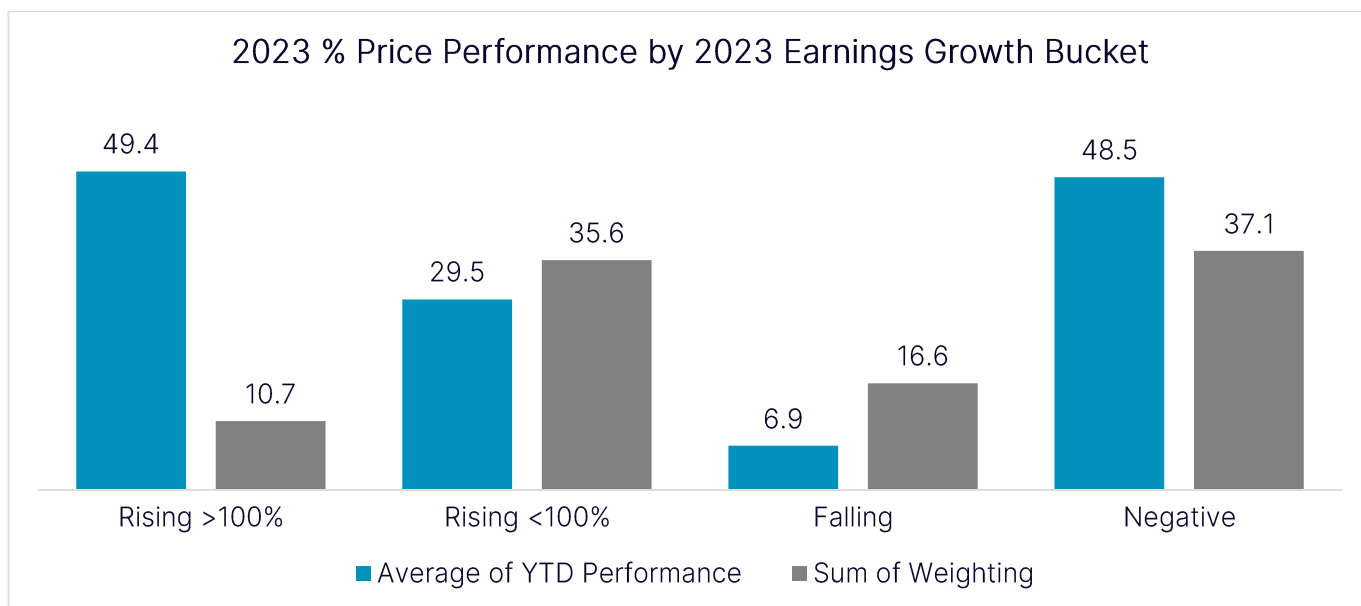


Earnings and correlation to performance

For the full year 2023, 15 out of 41 companies (46.3% of index weight) tracked by the index saw their earnings increase y-o-y. Of this subset, companies that grew earnings the fastest (>100%), with a total index weight of 10.7%, were up 49.4% on average, outperforming the rest of the index. Companies that saw their earnings decline, while remaining profitable overall, were up 6.9%, underperforming the rest of the index.

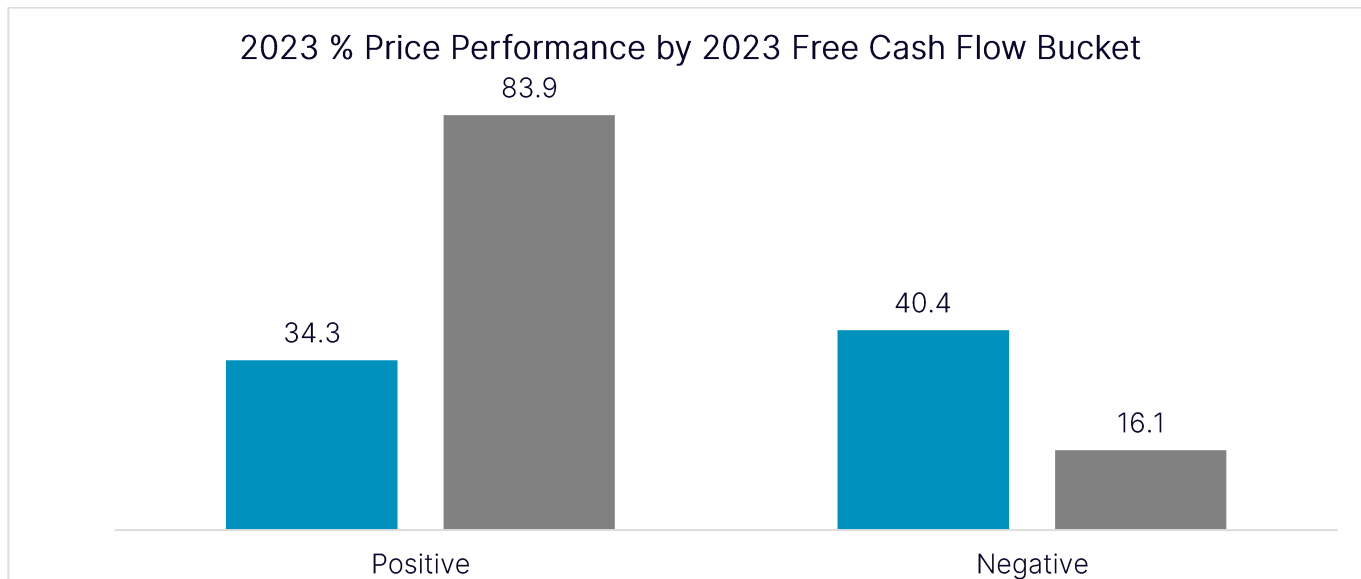
While these two subsets behaved as expected, there was a disconnect with the other two subsets of the index. Companies that posted losses, with an index weight of 37.1%, registered positive returns of 48.5% on average. As a subgroup, they outperformed the subset of companies that saw their earnings grow at a slower rate (<100%) by 19 percentage points.

Earnings of several companies that make up the index received a boost from strong traction for certain sub-segments of cybersecurity including cloud, AI, and identity, along with strong execution and expense discipline. For the rest of index constituents, macro/FX headwinds, longer sales cycles, and loss of share to competitors weighed more heavily on earnings.



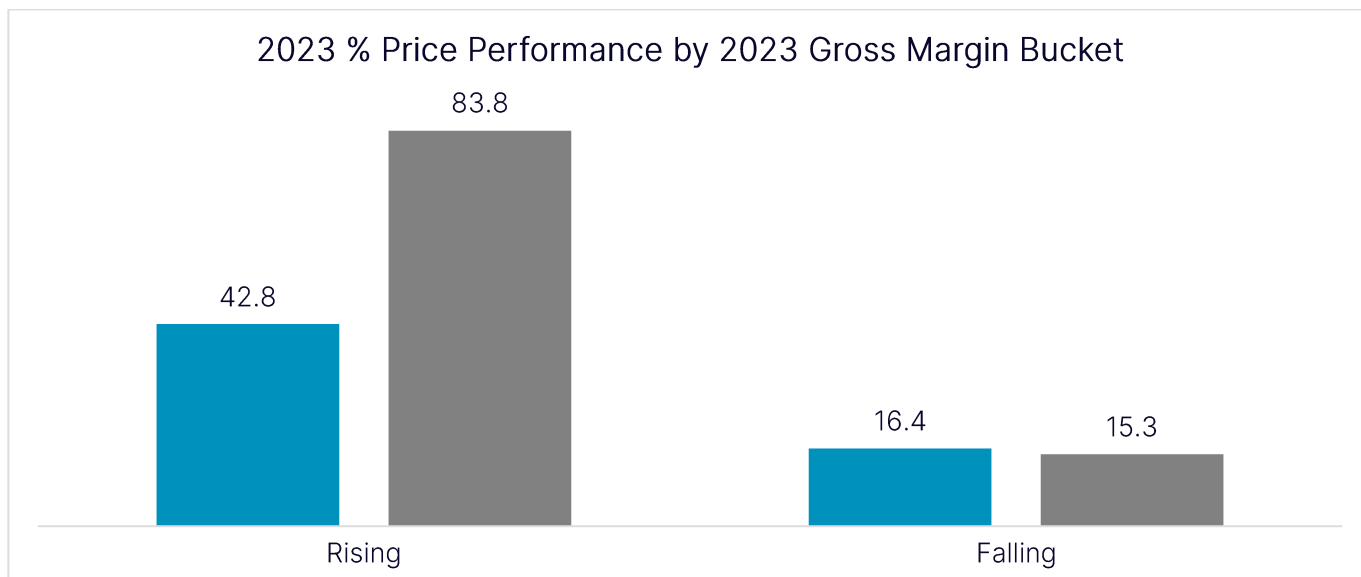
Free cash flow and correlation to performances

For the full year 2023, companies that were free cash flow positive made up 84% of index weight. As a group, they were up 34.3%, underperforming companies that were free cash flow negative by 6 percentage points. This suggests that there was a disconnect between performance and fundamentals. It is encouraging that there was an improvement by approximately 3 percentage points in terms of index weight that was free cash positive in 2023 versus 2022.



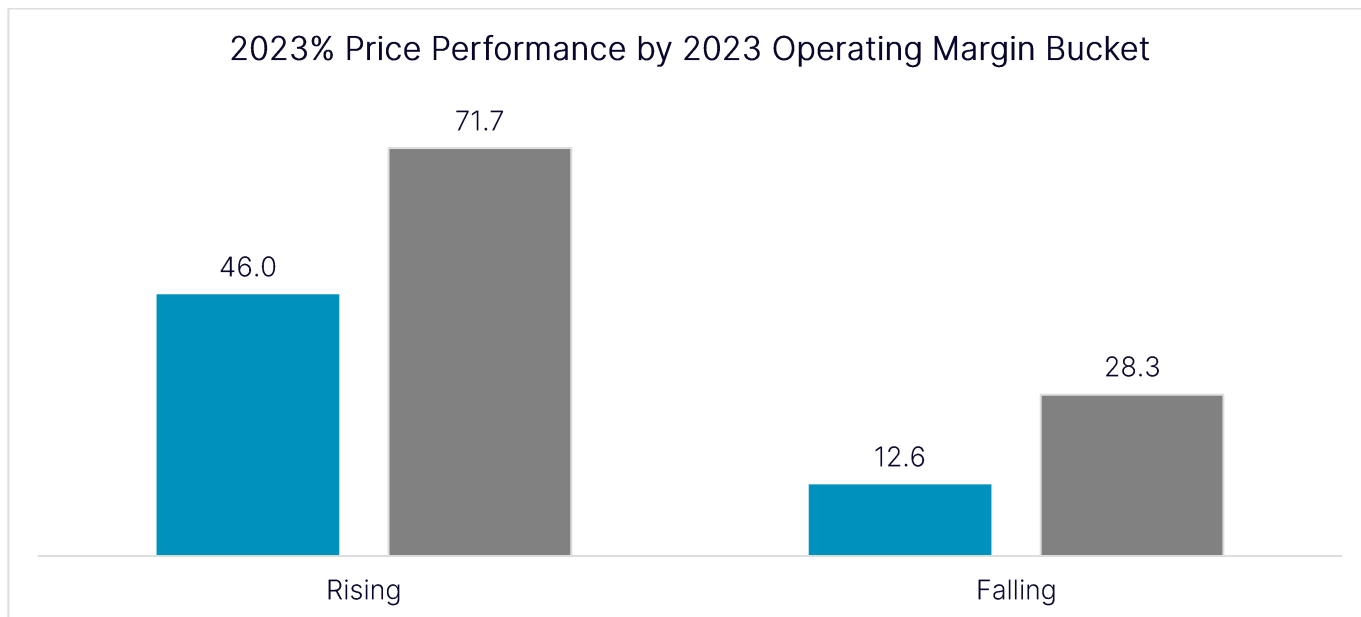
Gross margin and correlation to performance

For the full year 2023, 30 out of 41 companies (83.8% of index weight) tracked by the index saw their gross margins increase y-o-y. As a group, they outperformed the subset of companies that saw gross margins decline by 26 percentage points. 10 companies (15.3% of index weight) tracked by the index saw their gross margins decline y-o-y. What is encouraging is that several companies reported healthy gross margins in 2023 and are optimistic about gross margin expansion in 2024, despite operating in a challenging macroeconomic backdrop.



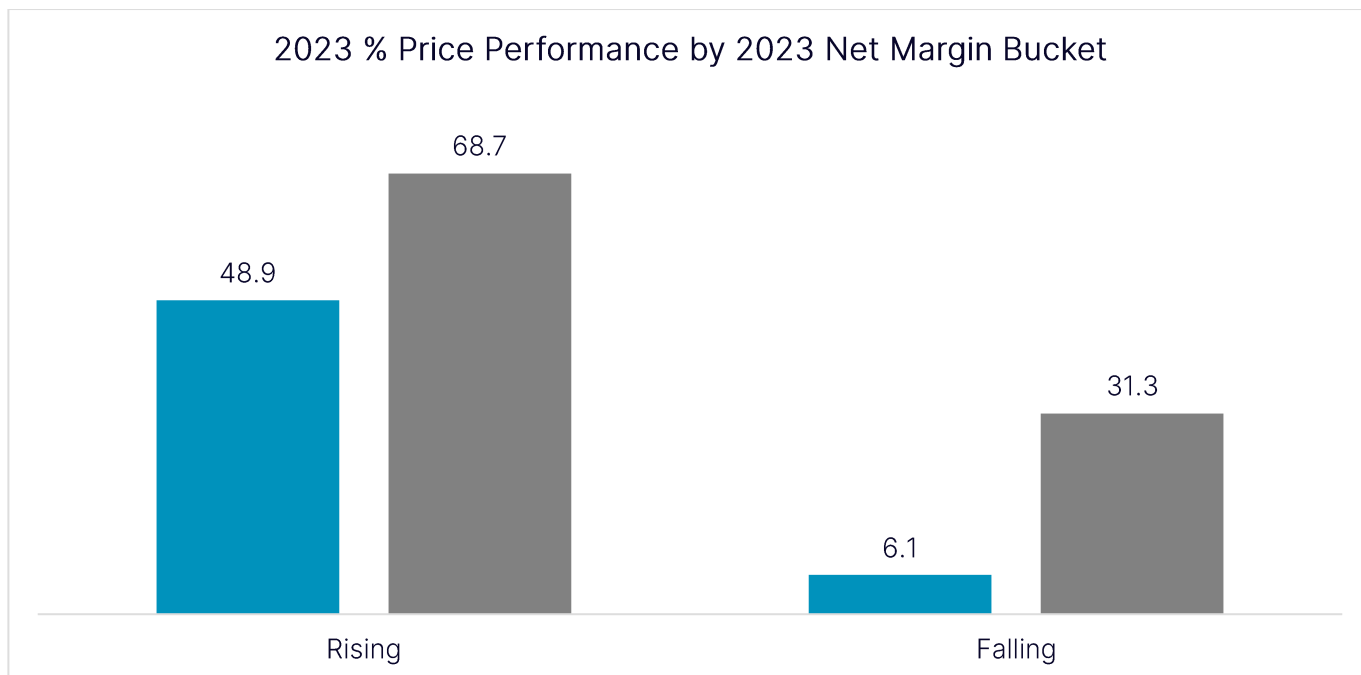
Operating margin and correlation to performance

For the full year 2023, 28 out of 41 constituents (71.7% of index weight) tracked by the index saw their operating margins increase y-o-y. As a group, they outperformed the subset of companies that saw operating margins decline by approximately 33 percentage points, on average. 13 out of 41 constituents (28.3% of index weight) tracked by the index saw their operating margins decrease y-o-y.



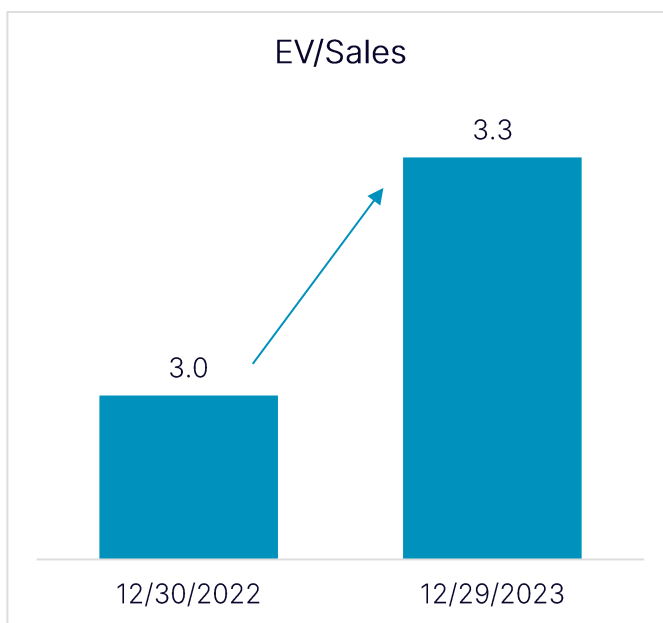
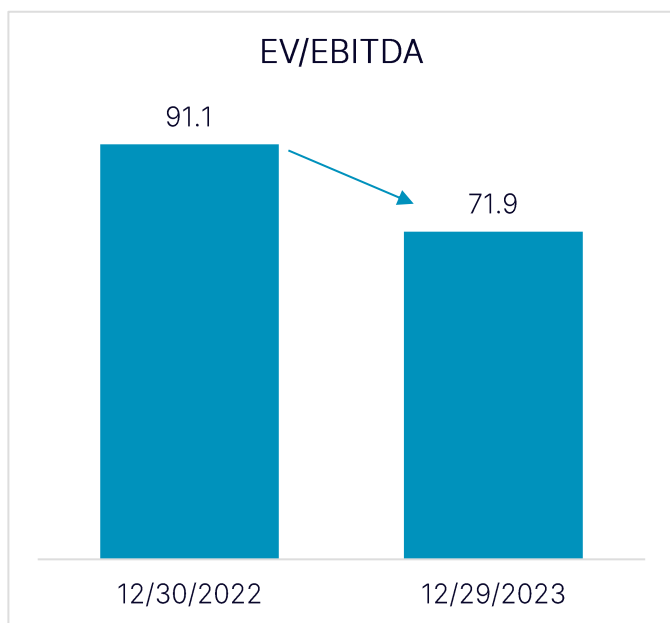
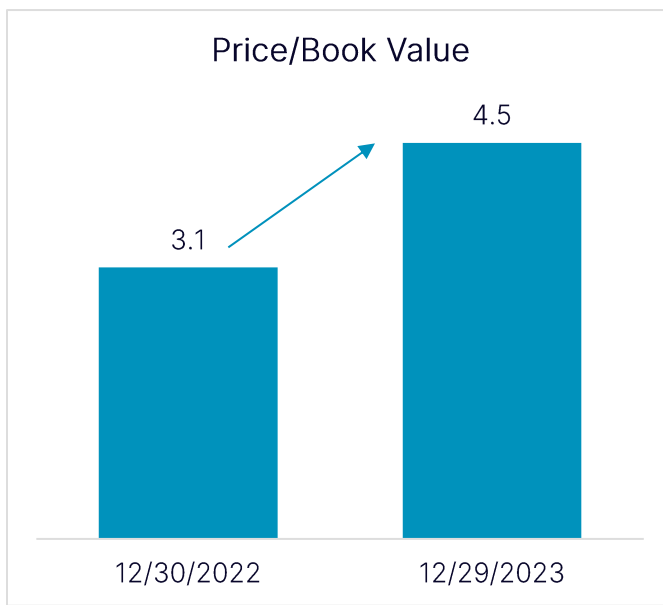
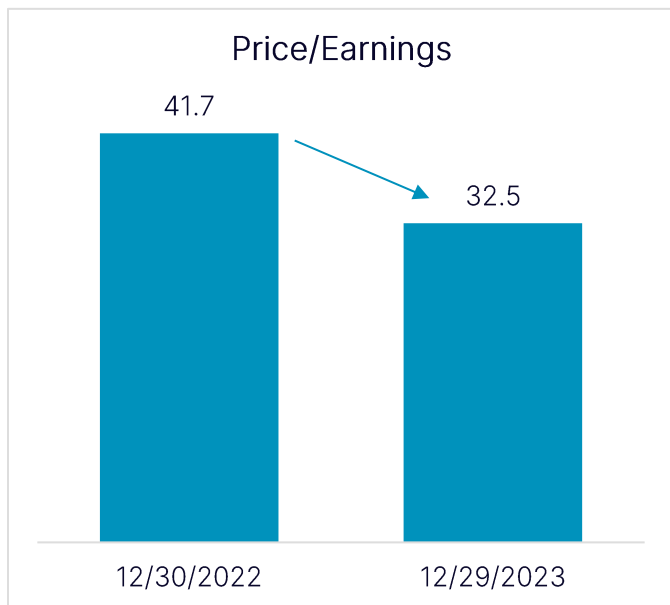
Net margin and correlation to performance

For the full year 2023, 28 out of 41 constituents (68.7% of the index weight) tracked by the index saw their net margins increase y-o-y. As a group, they outperformed the subset of companies that saw net margins decline by a whopping 43 percentage points, on average. 13 out of 41 constituents (31.3% of index weight) tracked by the index saw their net margins decrease y-o-y.



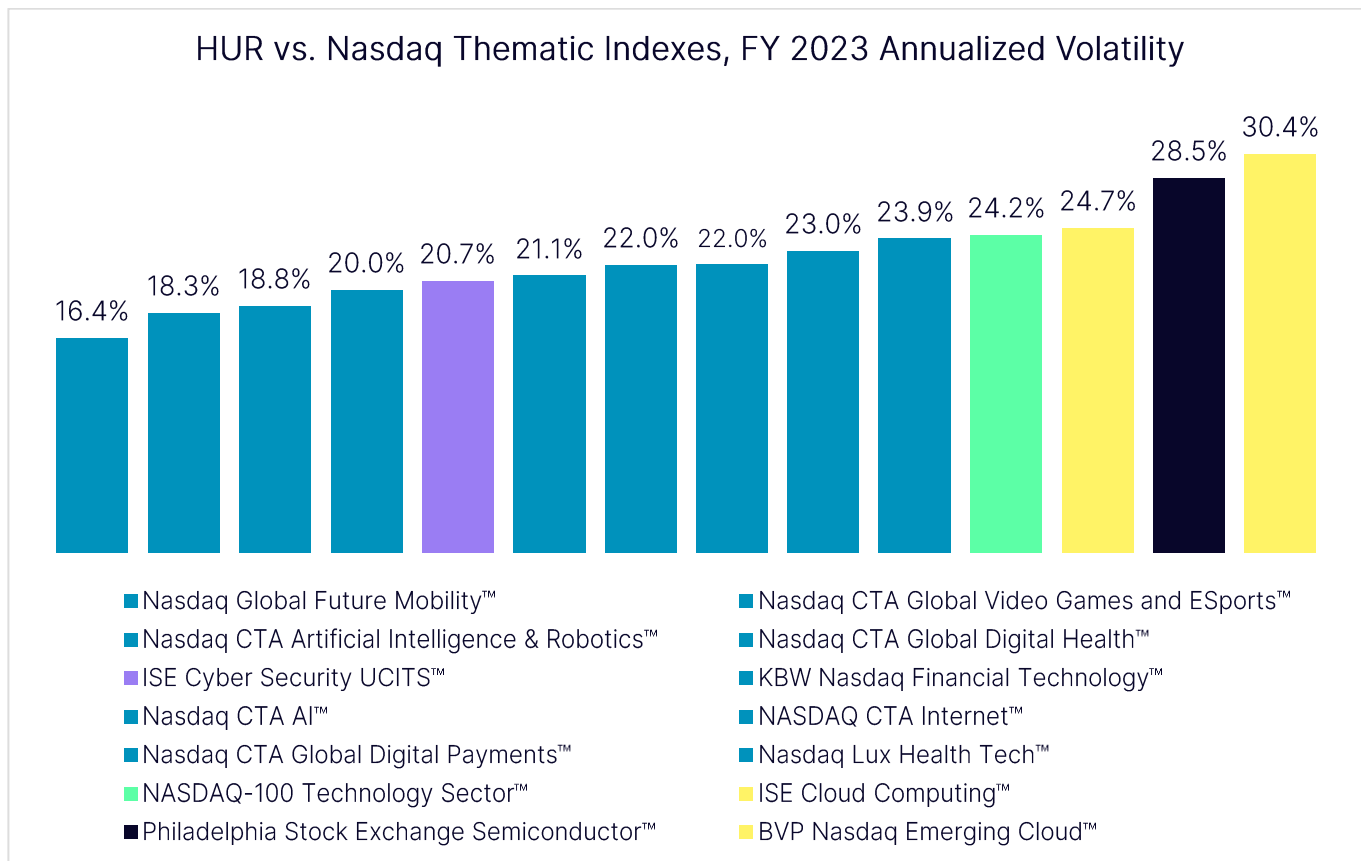
Index Valuations

Over the course of 2023, the ISE Cybersecurity UCITS Index (HUR) became cheaper on two out of four index-weighted valuation metrics: price-to-earnings, and EV/EBITDA. While high-growth stocks came back into favor in 2023, investors elevated AI as a theme over other areas of technology. Going into 2023, the sentiment towards other areas of technology was far more pessimistic than towards cybersecurity. While cybersecurity was expected to hold up relatively strongly in the face of a potential recession, expectations were far more pessimistic towards other areas of technology. This gap between expectations and actual results likely explains the contraction in multiples for HUR versus indexes tracking other areas of technology such as AI. Looking ahead into the rest of 2024, the latest consensus estimates anticipate the entire index to normalize to a P/E of approximately 24.7.



Defensive and Differentiated within Broad Tech

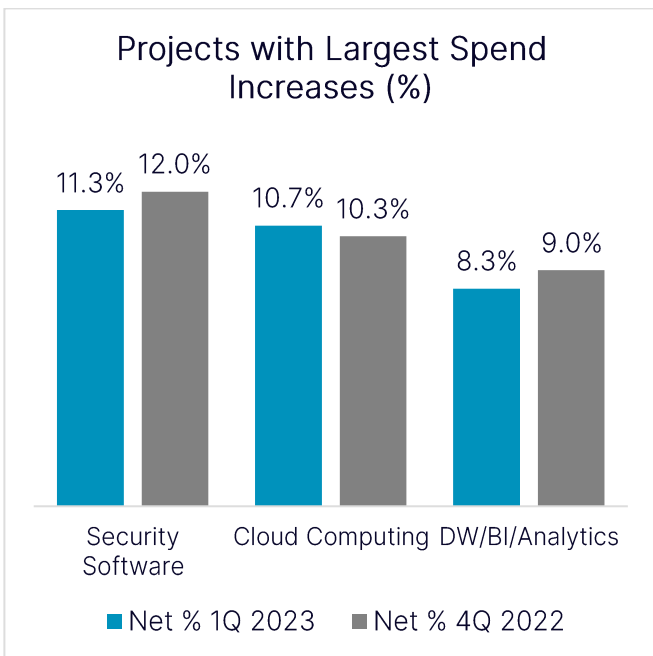
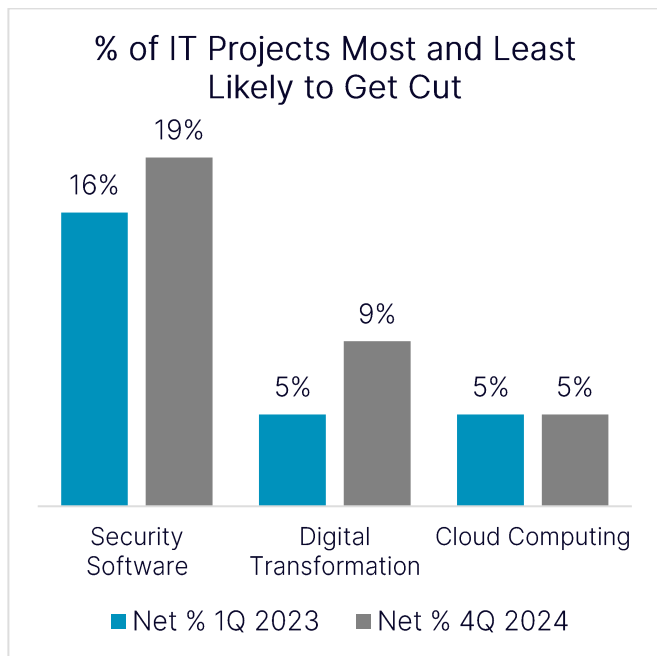
The ISE Cyber Security UCITS Index (HUR) registered lower volatility than more than half of a broad sampling of Nasdaq Thematic Tech Indexes, reinforcing the idea that it is a more defensive play within its peer group. For FY 2023, it registered annualized volatility of 20.7%, lower than nine of 13 other Tech indexes, including Semiconductors (SOX™), Cloud Computing (CPQ™, EMCLOUD™) benchmarks, and the broader Nasdaq-100 Technology Sector™ Index (NDXT™).



Cybersecurity Survey

As has been the case for several years running, CIOs again expect cybersecurity to be a top area of future investment in 2024, followed by business intelligence/data analytics and cloud platforms²⁰. As per the most recent survey by Gartner, 80% of respondents expect to increase investment in cybersecurity in 2024. The study's results reinforce findings from a survey done by Morgan Stanley in 2023, which concluded that security software is unlikely to be cut even in a recessionary environment. These findings continue to underscore the underlying defensive nature of cybersecurity versus other areas of technology.

²⁰ <https://www.gartner.com/en/newsroom/press-releases/2023-10-17-gartner-survey-of-over-2400-cios-reveals-that-45-percent-of-cios-are-driving-a-shift-to-co-ownership-of-digital-leadership>



Source: AlphaWise, Morgan Stanley Research, n=100 (US and EU data)

Conclusion

Companies that make up the ISE Cyber Security UCITS Index continue to be well-positioned to capture value in an environment that is seeing increased “platformization” and a shift towards the cloud. Fundamentals of the sector continue to be strong, with artificial intelligence driving renewed investor interest. While there are some near-term risks by way of weaker billings, longer sales cycles, and increased budget scrutiny, they are likely to be outweighed by a strong demand environment. Gartner’s most recent spending projections on cybersecurity were revised upward to a growth rate of 14% in 2024, lending further support to the theme’s underlying story of consistent, above-average growth. Lastly, as hacks continue to proliferate and regulatory pressures increase, end-users are ever more likely to shore up their cybersecurity defenses in the years ahead.

Investors looking to gain exposure to companies that provide cybersecurity solutions can invest in the product tracking the ISE Cyber Security UCITS Index, the Legal & General Cyber Security UCITS ETF (London: ISPY/USPY).

Sources: Nasdaq Global Indexes, FactSet, Bloomberg

Disclaimer:

Nasdaq® is a registered trademark of Nasdaq, Inc. The information contained above is provided for informational and educational purposes only, and nothing contained herein should be construed as investment advice, either on behalf of a particular security or an overall investment strategy. Neither Nasdaq, Inc. nor any of its affiliates makes any recommendation to buy or sell any security or any representation about the financial condition of any company. Statements regarding Nasdaq-listed companies or Nasdaq proprietary indexes are not guarantees of future performance. Actual results may differ materially from those expressed or implied. Past performance is not indicative of future results. Investors should undertake their own due diligence and carefully evaluate companies before investing. **ADVICE FROM A SECURITIES PROFESSIONAL IS STRONGLY ADVISED.**

© 2024. Nasdaq, Inc. All Rights Reserved.