

Cybersecurity Industry

May 2025 Outlook



Equity Research

Analysts

Stelian Cujba

stelian.cujba@studbocconi.it

Filippo Torsa

filippo.torsa@studbocconi.it

Savvina Salvaridou

savvina.salvaridou@studbocconi.it

Supervisors

Rezan Bagcioglu

Co-Head of Equity Research

rezan.bagcioglu@studbocconi.it

Giacomo Pietrosanti

Co-Head of Equity Research

giacomo.pietrosanti@studbocconi.it

Executive Summary

The cybersecurity industry is experiencing rapid growth, driven by increasing digitalization, evolving cyber threats, and rising regulatory demands. With the market projected to exceed \$500 billion by 2030, with an estimated double-digit CAGR between 12.5% and 14.5% and investment doubling in 2024 alone, cybersecurity has become a strategic priority for enterprises and governments. Trends like AI-powered threat detection, zero-trust architecture, and cloud-native security are reshaping the landscape, while leaders like Microsoft, IBM, and Cisco dominate through scale and integration. At the same time, challenges such as a global workforce shortage and growing system complexity highlight the need for consolidation and specialized solutions. The sector is poised for continued expansion, fueled by demand for secure digital infrastructure, compliance tools, and proactive threat defense. Recently announced \$32 billion Wiz's acquisition by Alphabet fully highlights the growing momentum.

Key Figures	Key Leaders
\$245.6B market in 2024 ¹	Microsoft – Cloud security leader
Forecast: \$500B+ market by 2030, 12–14% CAGR ²	IBM – Top security software provider
\$8.5B invested in 2024, double from 2023 ³	Cisco – Network security leader

¹ Grand View Research. Cyber Security Market Size, Share & Trends Analysis Report By Offering (Hardware, Software, Services), By Security (Endpoint Security), By Organization Size (Large Enterprises), By Deployment (Cloud), By Solution, By End Use, By Region, And Segment Forecasts, 2025 - 2030. Grand View Research, 2025,

² Fortune Business Insights. "CYBERSECURITY MARKET ANALYSIS - 2032." Cybersecurity Market Size, Share & Industry Analysis, vol. 6, no. 1, 2025, p. 160. Fortune Business Insights,

³ S&P Global

Key Tailwinds	Key Headwinds
Surge in cybercrime (esp. ransomware, supply chain attacks)	4.8M global workforce gap
AI & machine learning enhancing threat detection	Fragmented tools & growing IT complexity
Regulatory momentum (GDPR, AI compliance)	Quantum computing risks to current encryption methods

Industry Overview

Cybersecurity, also known as computer security or information technology (IT) security, involves the protection of computer systems, networks, and data against unauthorized access, theft, damage, or disruption. With computing technologies entering the daily, business, and governmental realms, cybersecurity has emerged as a central field dedicated to preserving confidentiality, integrity, and availability of information.

The primary segments of cybersecurity are tailored to address specific security needs in diverse environments. Network security focuses on safeguarding the integrity of a network against cyber threats using equipment like firewalls and intrusion detection systems. Endpoint security secures individual machines like laptops and phones against potential exposures. Cloud security is vital in protecting data stored in the cloud, offering safe access, storage, and transportation. Application security works on securing software applications from threats throughout their life cycle, and data security deals with the protection of sensitive information from unauthorized access, modification, or destruction.

It is at times challenging to define the boundaries of the cybersecurity sector since it intersects with other fields that are closely related to it. For instance, cybersecurity intersects with information security, whose scope is wide and encompasses safeguarding all forms of information, not necessarily digital information. It also intersects with physical security, whereby measures are put in place to prevent unauthorized physical access to facilities and hardware. The inclusion of cybersecurity in conjunction with software development, network engineering, and risk management further demonstrates the far-reaching nature of the industry and the necessity of multidisciplinary efforts to address shifting cyber threats.

Market Overview

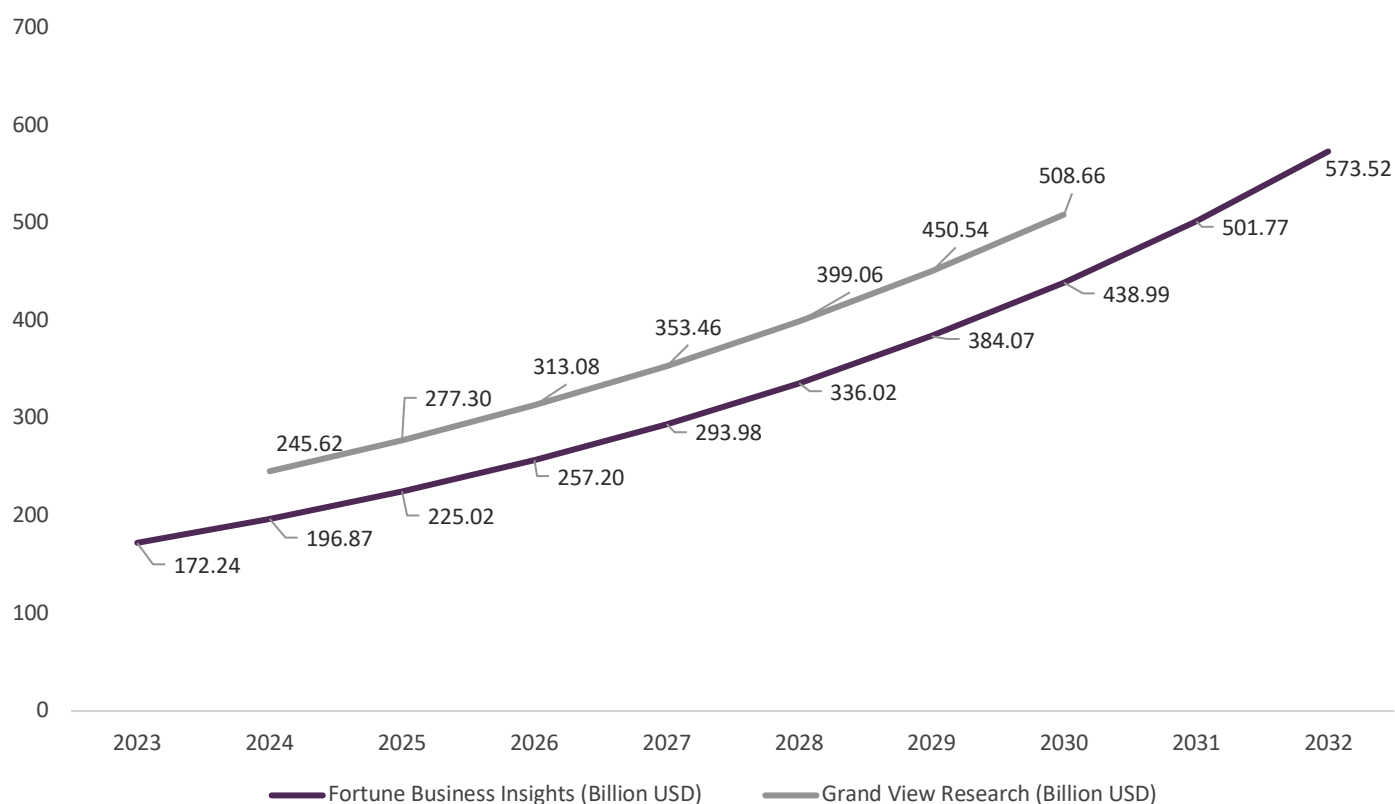
The cybersecurity industry has experienced remarkable growth in recent years, reflecting the increasing importance of protecting digital assets across the globe.

Global Market Valuation

The global cybersecurity market valuation has been estimated variously by market experts. Fortune Business Insights⁴ estimates the market at around \$172.24 billion in 2023 and estimates to increase to \$562.72 billion by 2032, with a CAGR of 14.3% during the forecast period. Grand View Research estimates the market size to be \$245.62 billion in 2024 and is estimated to grow from 2025 to 2030 at a CAGR of 12.9%, with an estimated growth to \$500.70 billion by 2030.

Figure 1: The uncertain boundaries of the industry make the forecasts vary in the absolute value

Cybersecurity Market Size forecasted by GVR and FB Insights (\$ billion)

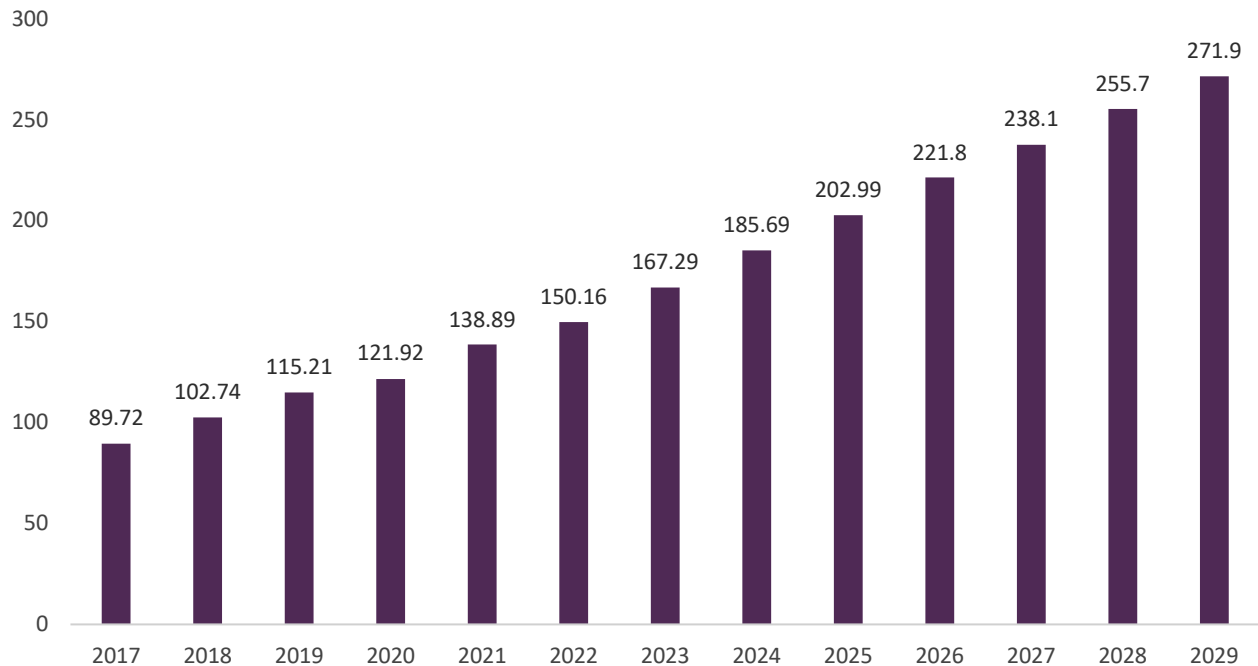


Source: Grand View Research, Cyber Security Market Size, Share & Trends Analysis Report

⁴ Fortune Business Insights. "CYBERSECURITY MARKET ANALYSIS - 2032."

Figure 2: Cybersecurity sector forecasted to continue the rapid growth trajectory

Cybersecurity Revenues (\$ billion)



Source: Statista. "Cybersecurity: market data & analysis"

Regional Market Breakdown

Regional research shows the dominant position of North America in the cybersecurity market. Fortune Business Insights⁵ demonstrates that North America accounted for 43.76% of the global market share in 2023. The heavy investment in cybersecurity products is driven by the wide variety of cybersecurity firms in the market and the increasing frequency of cyber threat attacks. On the other hand, the Asia-Pacific region is expanding at a higher rate with a forecasted higher CAGR compared to other regions in the future.

Key Growth Drivers and Limiters

The rising digitalization across industries—particularly through cloud computing, the Internet of Things (IoT), and e-commerce—continues to be a major growth driver for the cybersecurity market. As more organizations migrate operations to the cloud, securing these digital environments has become critical, especially for safeguarding sensitive data and maintaining business continuity. Cloud security, therefore, is not only a standalone concern but also a central aspect of broader cybersecurity strategies.

Another key driver is the increasing frequency and sophistication of cyber-attacks, including ransomware, phishing, and advanced persistent threats. These evolving threats compel organizations to invest in

⁵ Fortune Business Insights. "CYBERSECURITY MARKET ANALYSIS - 2032."

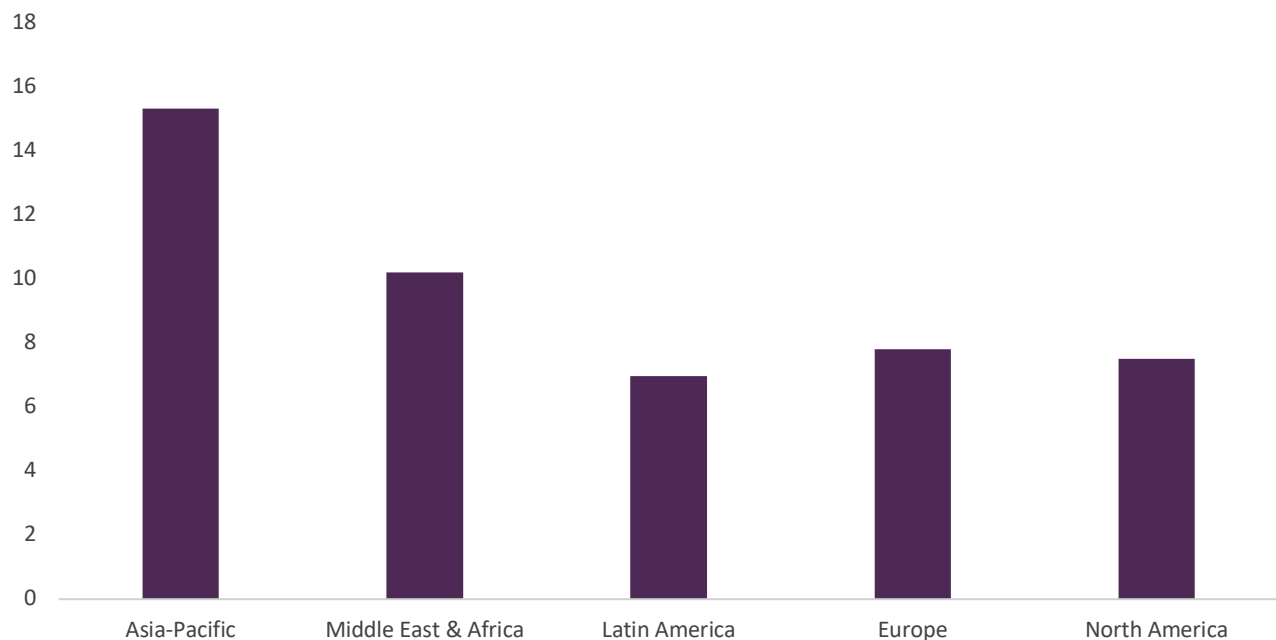
advanced cybersecurity infrastructures capable of real-time threat detection and rapid response. The integration of artificial intelligence (AI) and machine learning (ML) into security solutions has further strengthened these capabilities, enhancing the effectiveness and adaptability of cybersecurity systems.

Moreover, regulatory pressures are intensifying. Laws like the General Data Protection Regulation (GDPR) and similar regional frameworks are forcing organizations to comply with strict data protection standards, thus driving demand for more robust security solutions.

However, there are also significant market limitations. The complexity and cost of implementing advanced cybersecurity systems—particularly in cloud-based environments—can deter smaller organizations from adoption. In addition, the global shortage of skilled cybersecurity professionals' hampers organizations' ability to manage and maintain these systems effectively. Lastly, the fast pace of technological change can result in solution fatigue, where businesses struggle to keep up with the constant need for updates, training, and integration.

Figure 3: Asia-Pacific, Middle East and Africa are projected to grow at the fastest pace over the next years

Projected CAGR per Region in percentage points



Source: Fortune Business Insights, Markets and Markets, and Statista

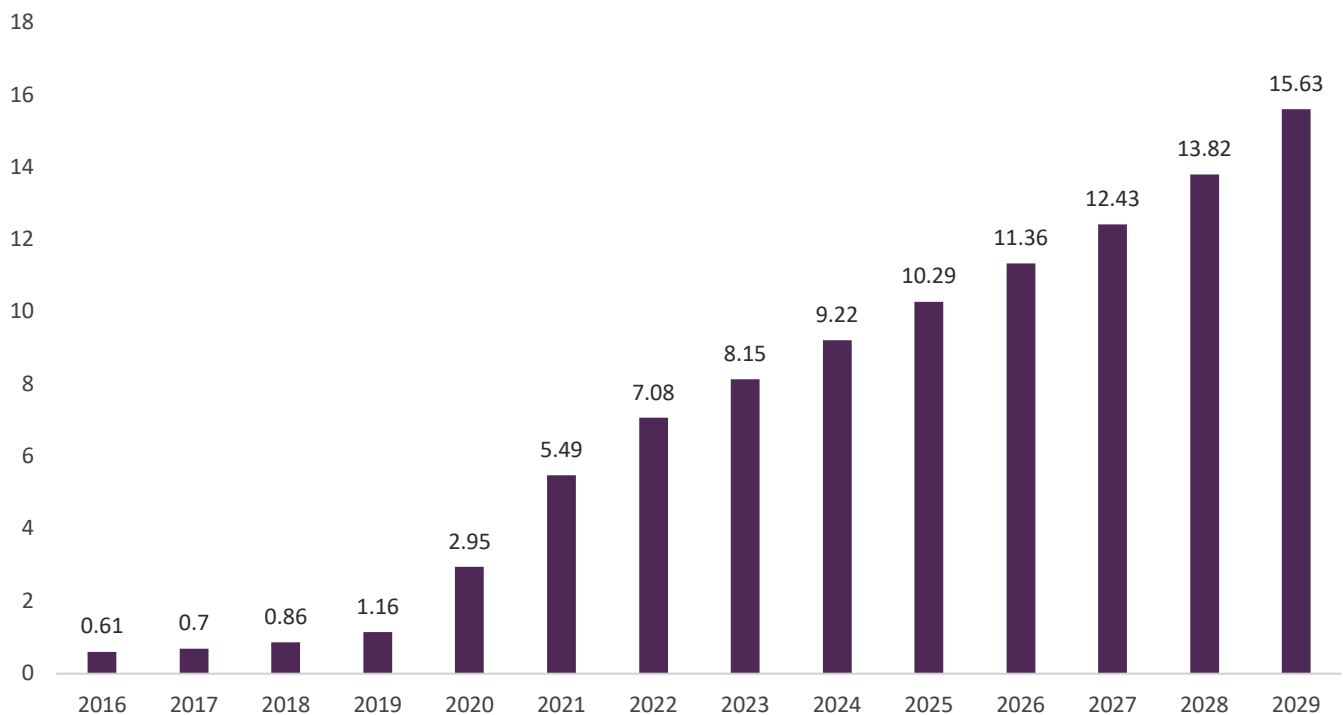
Overall, the cybersecurity market's expansion is driven by several key factors. Global economic conditions, particularly the rapid acceleration of internet penetration from 52.3% in 2019 to a projected 86.5% by 2029⁶, especially in Asia and Europe, are increasing the demand for robust security solutions.

⁶ Statista, "Cybersecurity, market data & analysis"

IT investments are also rising as enterprises prioritize security to safeguard sensitive data in the face of digital transformation. The widespread adoption of hybrid and multi-cloud environments is further shaping the industry, offering scalability and efficiency but also introducing new security risks, making cloud security a crucial concern. The increasing sophistication and frequency of cyberattacks have further amplified the urgency for advanced security solutions, as modern cybercriminals exploit vulnerabilities with greater efficiency. Additionally, cyber warfare has emerged as a critical geopolitical concern, with conflicts such as the Russia-Ukraine war driving heightened investments in cybersecurity to counteract digital threats in military and strategic domains. These macroeconomic, technological, and security factors collectively position cybersecurity as a top strategic priority for enterprises, governments, and institutions worldwide, ensuring sustained industry growth and market evolution⁶

Figure 4: The cost of cybercrime continues to increase at an accelerated rate

Estimated cost of cybercrime incurred by corporates (\$ trillion)



Source: Statista Estimates of Cost of Cybercrime

Market Segmentation

Key players in the cybersecurity market include Microsoft, IBM, Cisco, Palo Alto Networks, and Fortinet, with 2023 revenues of \$212 billion, \$62 billion, \$57 billion, \$7 billion, and \$5 billion, respectively.⁷ These companies, however, operate beyond cybersecurity, integrating security solutions within broader business segments. Microsoft, the market leader – if considering the whole firm, derived 38% of its total revenue from cloud services, while IBM's software division, encompassing security, accounted for 43%

⁷ Statista, "Cybersecurity, market data & analysis"

of total revenue. Cisco's security business represented 76% of its revenue, reflecting its deep integration into network security. Despite variations in product portfolios, these companies have shown steady growth, with single- and double-digit CAGRs. In 2022, IBM led the cyber solutions market with a 20% brand share, followed by Microsoft at 16%, Broadcom at 11%, Cisco at 6%, while smaller firms collectively accounted for nearly half of the market. Based in market capitalization, Microsoft (MSFT) leads with \$2.93 trillion, Broadcom (AVGO) is valued at \$937.10 billion, Cisco Systems (CSCO) at \$231.26 billion, Fortinet Inc (FTNT) at \$80.35 billion, Palo Alto Networks (PANW) at \$123.69 billion, while IBM (IBM) at approximately \$217.69 billion. Among these, Broadcom and Fortinet encountered the steepest 1-year market cap increase, respectively +54.28% and +58.47%.

The security industry is divided along several key dimensions to cater to the diverse security needs of modern-day organizations. *Based on solution type*, the industry includes network security, cloud security, and endpoint security. Network security means protecting internal infrastructure from cyber-attacks and unauthorized access via solutions like firewalls and intrusion prevention systems. Cloud security has also grown more applicable with growing adoption of cloud computing, where protection of data, applications, and services in cloud environments is provided. Endpoint security guards standalone machines - laptops, mobile phones, desktops, etc. - which are typical target machines for attacks such as phishing and malware. Every solution tackle one specific layer of vulnerability in existing digital worlds. *Deployment model segmentation* separates on-premises and cloud-based solutions. On-premises deployment provides full control over security infrastructure and data and is thus the choice of organizations with strict compliance or regulatory requirements. Cloud-based cybersecurity solutions are, however, more adaptable, scalable, and economical, and are favored therefore by small and medium-sized businesses (SMBs) particularly. Cloud models provide quicker deployment and easier updates, which becomes necessary in rapidly evolving threat environments.

Another aspect of segmentation is based on *organization size and vertical markets*. Businesses typically spend money on advanced, multi-layered cybersecurity frameworks integrating various technologies and threat intelligence. SMBs, with relatively smaller budgets and IT resources, prefer lightweight and less expensive security products. Government organizations form a unique category with highly specialized needs for protection of sensitive and classified information. Vertically, healthcare, finance, and mission-critical infrastructure (e.g., energy and utilities) are massive consumers of cybersecurity products due to the nature of the data that they work with being so valuable and the impact of a potential breach being so catastrophic. These sectors require strict regulatory requirements and are hacking favorites, and therefore cybersecurity is a business imperative.

Cybersecurity Trends

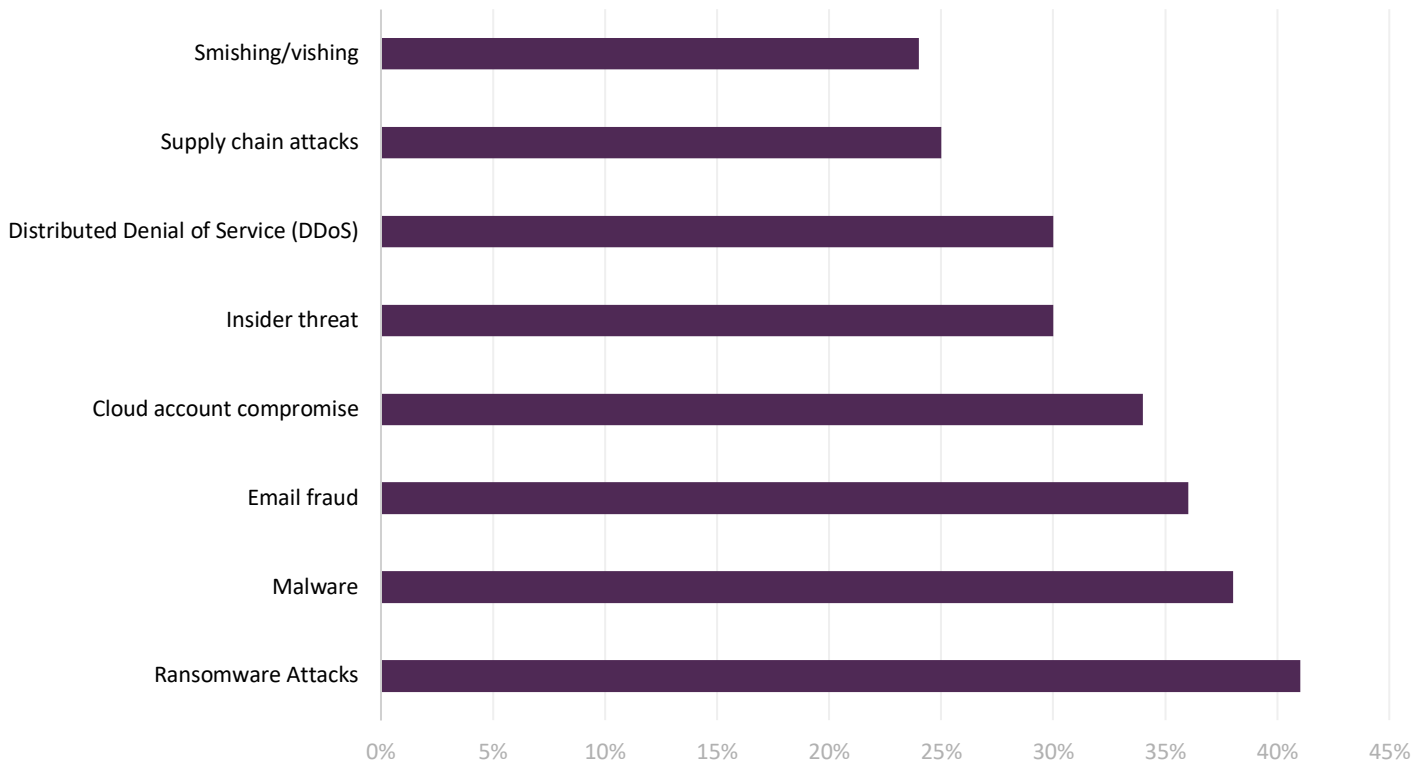
Prevalent attack vectors

The cybersecurity threat landscape has developed significantly in recent years, shifting from wide-net attacks to highly targeted, complex campaigns developed by both criminal organizations and world governments. Thus, understanding the predominant attack vectors is crucial for evaluating players in the cybersecurity industry and their strategic positioning in tackling these developing threats.

Ransomware continues to be the main threat for large enterprises. Now, attackers not only encrypt data, but also threaten to leak sensitive information and launch successive attacks on victims who refuse to pay, raising the average ransomware demand to \$2.73M in 2024⁸. Additionally, a new type of service, Ransomware-as-a-Service, has gained popularity among the cyber-criminals allowing the less technically skilled actors deploy advanced attacks through a subscription-based platform.

Figure 5: Ransomware attacks continue to be the main threat to organizations

Most significant cyber threats according to Chief Information Security Officers



Source: Statista Survey of Chief Information Security Officers

Supply chain attacks have also gained recent popularity, where attackers hack trusted software providers to gain access to the clients' networks. This approach where you "compromise one, and breach many" offers very attractive return on investment and poses an especially difficult task for defenders who have to scrutinize their entire digital supply chain.

Social engineering also remains a prevalent attack vector where the attackers exploit human error or human behavior through impersonation tactics targeting financial transfers and sensitive data especially. Normally, these attacks can be avoided through better personnel training, however the threat actors also continuously improve their techniques to more complex vectors than the classical phishing email.

⁸ Varonis, "Ransomware Statistics, Data, Trends, and Facts"

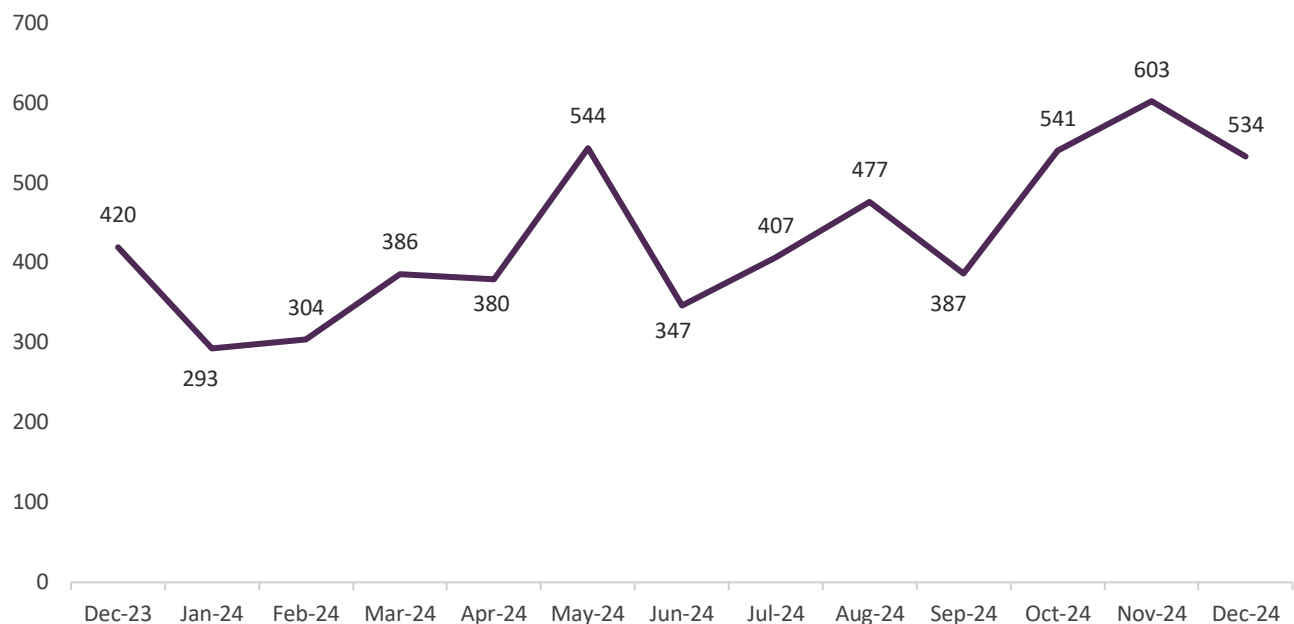
Notable breaches and Emerging threats

Over the years, we have seen multiple notable breaches that shaped the cybersecurity industry in different ways, either through raising awareness about digital risks, through exposing critical security issues or attracting big investments in the development of security measures. One of the most serious breaches was the “WannaCry attack”, a ransomware which exploited a windows vulnerability which had been leaked by the US National Security Agency, which led to the infection of huge networks across 150 countries.

One of the most sophisticated supply chain attacks in history was the SolarWinds attack in 2020, where Russian-affiliated hackers breached the update mechanism of Orion software, which led to the distribution of malware to over 18,000 customers including multiple branches of the US government and

Figure 6: Number of ransomware victims has constantly increased in 2024

Total number of ransomware victims reported



Source: Check Point Research “The State of Cyber Security 2025”

Fortune 500 companies. This attack was undetected for several months and shed light to the potential of supply chain attacks. As a response, there was a huge flow of investments in supply chain security solutions, which benefited especially the companies which specialized in software composition analysis. Since the industry is moving at an accelerating pace and is constantly shaped by new attack vectors from new technologies, it’s very important to understand the emerging threats that will most likely shape the industry in the future.

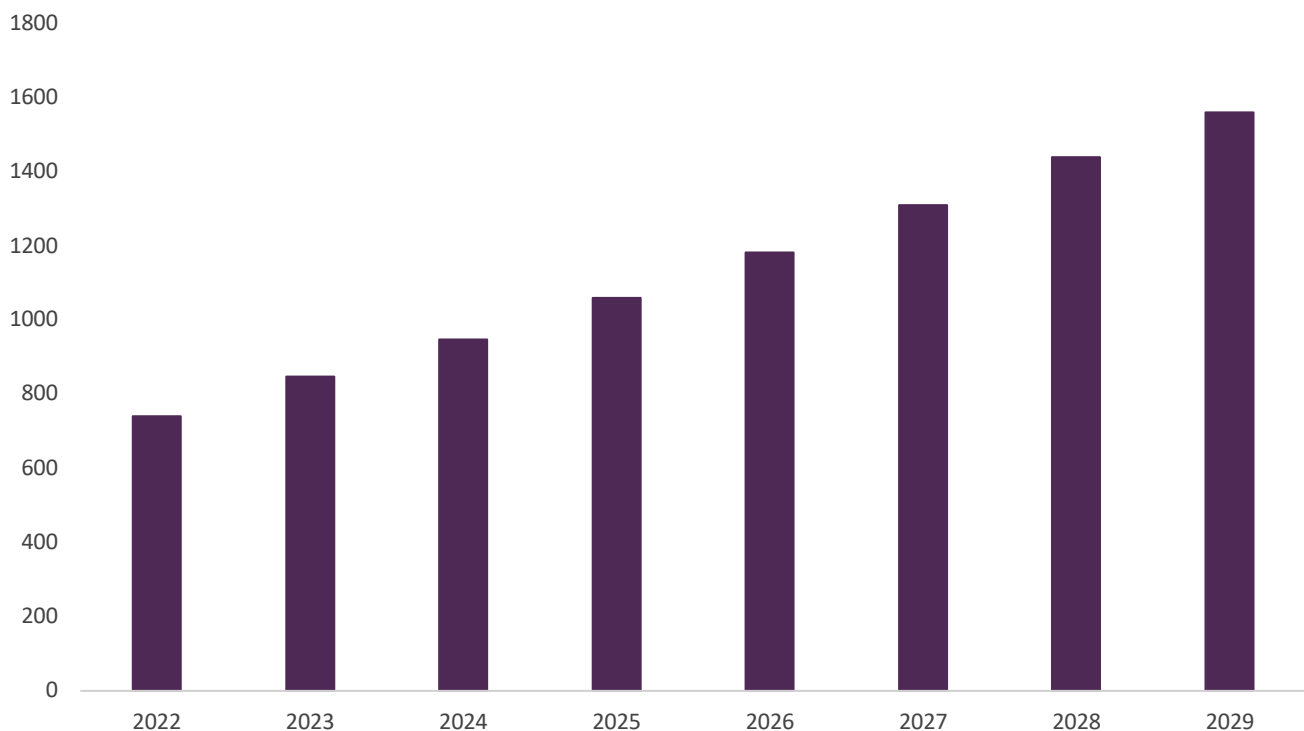
Artificial intelligence for example, is a double-edged technology for this industry. While cybersecurity firms leverage AI to improve security concerns, hackers also utilize the same technology to evade security

measures, to create more realistic deepfakes for social engineering and to even automate most of the processes. Companies that develop AI-based solutions ought to especially benefit from this struggle since traditional security measures tend to have difficulties against such attacks.

The rapid expansion of Internet-of-Things environments also has created a vast new attack vector with totally different security concerns. These environments often use a combination of old systems with new technology, creating security gaps that are difficult to avoid, with IoT attacks increasing by 400% YoY only in 2023. With the IoT industry forecasted to almost double by 2029⁹, the Internet-of-Things security solutions will become a more and more prevalent part of the cybersecurity industry.

Figure 7: The increasing market for Internet of Things devices also means an increasing attack surface from a cybersecurity point of view

Forecasted Internet of Things annual revenue worldwide (\$ billion)



Source: Statista, "Cybersecurity: Market data & Analysis"

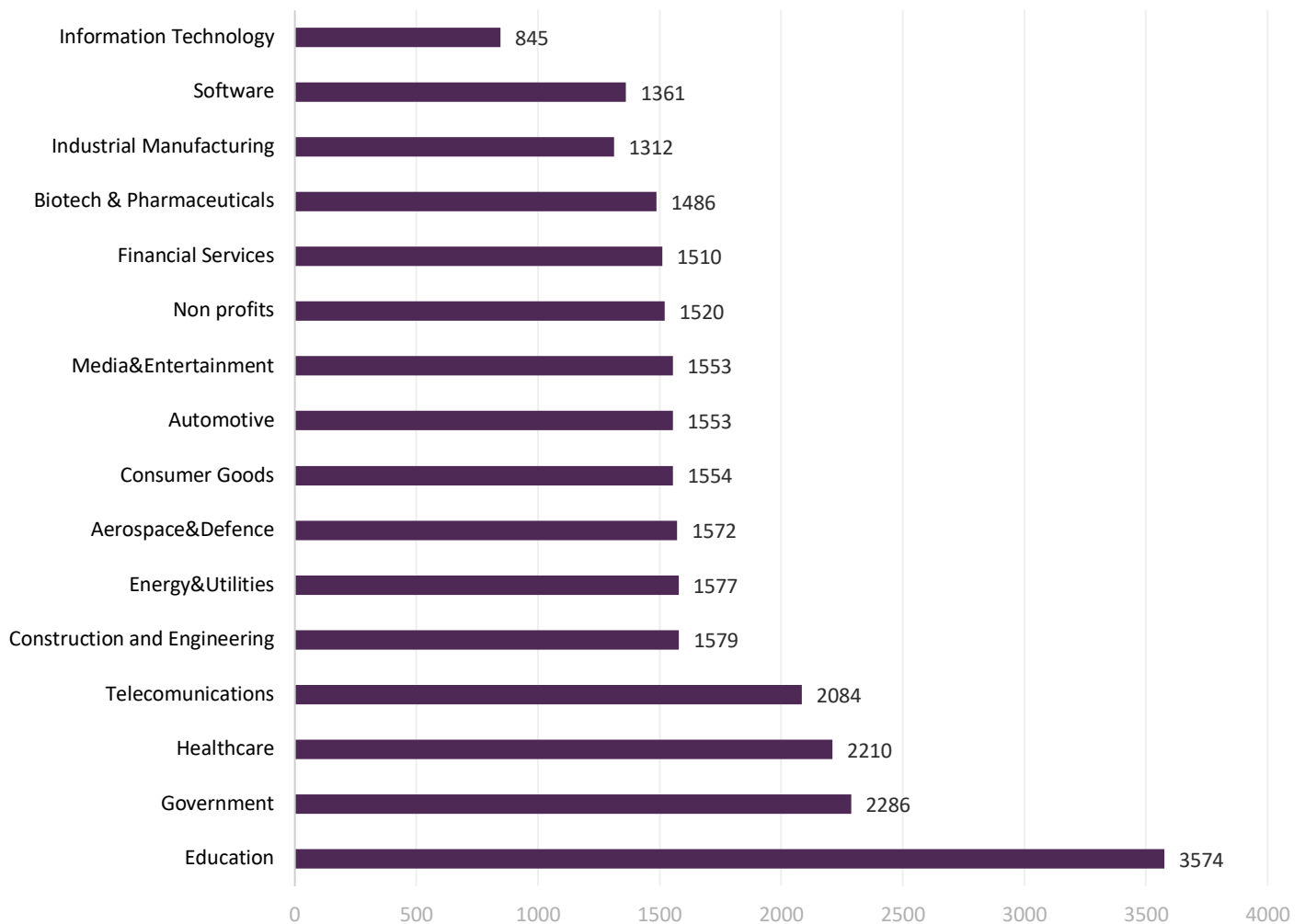
Another very long-term, but potentially catastrophic vulnerability is the emergence of quantum computing, which poses critical security concerns for the cryptography methods we have today. While consumer-viable quantum computing products might still be years away, the idea becomes more and more realistic, especially with the recent Microsoft Majorana 1 chip development, many hackers employ

⁹ Statista, "Cybersecurity, market data & analysis"

a strategy of collecting data now to decrypt it at a later point in time. There are already early adopters of quantum-resistant solutions in the defense sector and firms offering this kind of tools are seeing a constantly increasing interest, even though the technology is in its early stages.

Figure 8: Education, Government and Healthcare continue to be the industries most affected by cybercrime

Global weekly attacks per organization by industry in 2024



Source: Check Point Research "The State of Cyber Security 2025"

Tech Trends

AI and Machine Learning

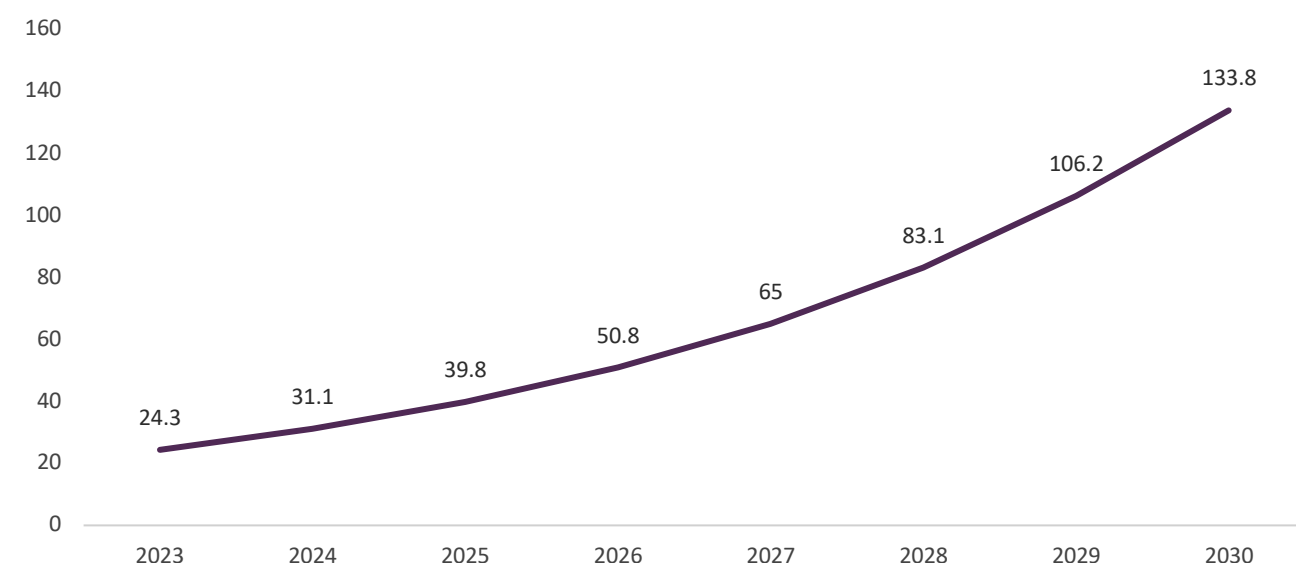
One of the most significant trends in the cybersecurity industry now is the implementation of Artificial Intelligence, with the market projected to grow at a 24% CAGR for the next 10 years¹⁰. Leading firms

¹⁰ Statista, "Value of the artificial intelligence (AI) cybersecurity market worldwide from 2023 to 2030"

implement sophisticated Machine Learning algorithms not only in the detection of new, unseen threats, but also in the automatic response of the systems. The main advantage of such solutions is that this technology allows the identification of threats or novel attacks from pattern recognition, rather than the traditional signature-based approaches where novelty types of attacks stay undetected. The market for such solutions also is increasingly differentiating between implementations on the surface-level and very complex platforms of deep learning that always keep improving since they are exposed to more and more data and threats. This, in turn, creates a wider and wider valuation gap between market leaders and followers.

Figure 9: The AI cybersecurity market is forecasted to continue growing at an exponential pace

Value of AI cybersecurity market worldwide 2023-2030 (\$ billion)



Source: Statista, "Value of the artificial intelligence (AI) cybersecurity market worldwide from 2020 to 2030"

Zero-trust architecture

Zero-trust architecture is a framework that has gained popularity in recent years. It is based on the idea of never trusting anything and always verifying all the activity in the network. This architecture is on the rise since organizations increasingly have more decentralized offices, with more and more hybrid cloud environments where traditional perimeter-based security exposes some big security issues. From an investing point of view, this trend represents growth for multiple types of firms across different types of solutions like authentication, authorization and access control. However, since the main barrier is implementation complexity, the solution-providers who offer comprehensive zero-trust platforms are capturing market share compared to vendors who offer specific solutions, thus suggesting that market consolidation will likely happen in this product sector.

Cloud security evolution

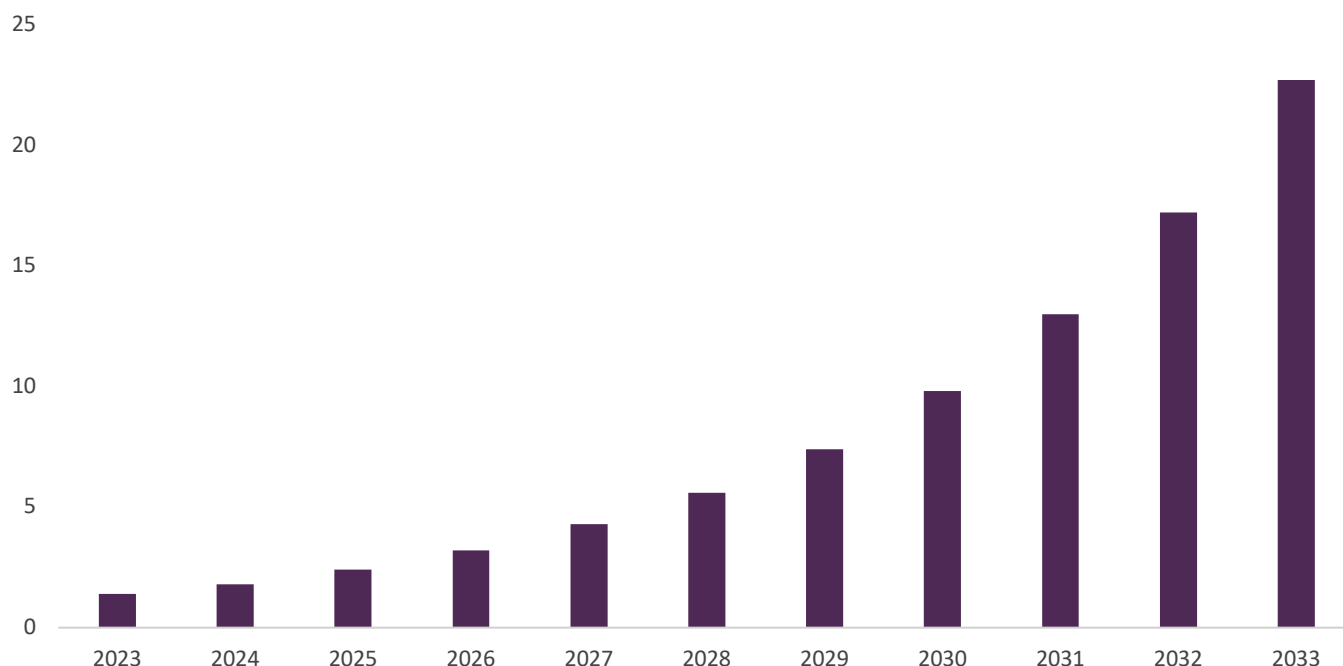
Another trend that is accelerating in recent years is Cloud Security, caused by the fast migration of corporations to multi-cloud environments, with estimates that by 2027, 70% of enterprises will use cloud

platforms, up from less than 15% in 2023¹¹. This evolution has affected the cybersecurity industry through the convergence of different security “domains” into one unified Cloud-Native Application Protection Platforms (CNAPP), reflecting the demand of comprehensive solutions for complex cloud architectures. From an equity research perspective, as organizations continue to employ a cloud-first approach, we expect that vendors who secure the cloud infrastructure without impeding business agility will outperform.

Quantum computing implications

The impending threat of quantum computing destroying current cryptography methods has catalyzed significant investments in quantum-resistant cryptography, with the market forecasted to grow at \$22.7B by 2033, up from the \$1.4B in 2024¹². This fast growth is mainly explained by the increasing need of organizations to prepare for “harvest now, decrypt later” attacks described in the previous section. This is confirmed by the National Institute of Standards and Technology who is responsible for creating security standards, releasing in 2024 the first 3 finalized Post-Quantum Encryption Standards. From an investing perspective, probably the best positioned firms to capitalize on this growth are the specialized cryptography and security infrastructure firms. For investors, the most interesting opportunities are found in the firms who have practical quantum-resistant implementations that are both technologically sound and address the complexity of migrating data to such solutions.

Figure 10: The Quantum Cryptography market is forecasted to increase in size at an accelerated pace
Value of Quantum Cryptography market worldwide 2023-2033 (\$ billion)



Source: Market.us, "Quantum Cryptography Market"

¹¹ Gartner, "The Expanding Enterprise Investment in Cloud Security"

¹² Market.us, "Quantum Cryptography Market"

Customer Dynamics

The market mainly serves B2B companies. Regarding B2B businesses, a Statista survey measured that in 2023 companies increased their allocated budget and reallocated it towards the usage of external IT resources, with a primary focus on AI and Cybersecurity, as a move to both raise IT protection, thus creating more efficient and safer internal processes. A McKinsey report states that in 3 years from now, companies' technological budget will be directed more towards third-party products and services and consequently decreasing internal labor. This highlights how leading companies are ahead of the curve and are able to leverage economies of scale and access cutting-edge technologies more effectively than internal IT departments can achieve on their own.

Moreover, AI is becoming even more blended into cybersecurity products, driving customer demands to features that combat or offset AI-related risks. Securing AI is now a stand-alone cyber-market segment that is poised to grow to \$255 million by 2027, from \$122 million today, with a total addressable market of \$10 billion to \$15 billion (McKinsey). Specifically, companies which already deploy AI mostly look for models to increase AI observability, to govern AI systems and to ensure data protection. These 3 traits are the ones steering customers' demands. Overall, to classify different customers' needs, companies are steering cybersecurity spending to outside vendors, with cloud security the biggest source of external spending, followed by engineering products, network and audit and compliance. The market is at an inflection point on best-of-breed offerings - that is, the best offering in a specific, narrow niche - versus best-of-suite offerings, which are complete, all-in-one solutions. For some segments, customers prefer the best individual vendors for each product on the market; for other segments, customers prefer to use the best product suite on the market. Providers can therefore try to cater to both types of customers, building best-of-suite bundled offerings around standout best-of-breed offerings.

Investment Analysis

The cybersecurity sector has seen a significant resurgence, with increased venture capital and private equity activity, fluctuating public market performance, strong return on investment metrics, and notable consolidation trends.

Investment in cybersecurity nearly doubled in 2024, reaching \$8.51 billion compared to \$4.46 billion in the previous year¹³. This surge reflects growing global emphasis on security and technological advancements (S&P Global). One of the most notable transactions was Wiz's \$1 billion Series E funding, which elevated its valuation to \$12 billion and positioned the company for expansion and acquisitions (Capstone Partners). More recently, Alphabet announced Wiz's \$32 billion acquisition March 18, 2025, marking its largest deal, providing cloud-agnostic security solutions and whose revenue is projected to generate \$1 billion by 2025. This acquisition enhances Google Cloud's cybersecurity capabilities, creating synergies to better compete with AWS and Azure and still requires regulatory approval, is expected to drive long-term growth in Google Cloud's offering¹⁴. Similarly, Island, a startup specializing

¹³ Private Equity International, "Cybersecurity sparks back to life"

¹⁴ AP News, "Google to buy cybersecurity firm Wiz for \$32 billion in the biggest deal in company's history"

in secure enterprise browsers, raised \$250 million in venture capital, bringing its market valuation to \$4.8 billion, with plans to use the funding for product development and workforce expansion¹⁵.

Public markets have shown mixed performances for cybersecurity firms. Okta experienced a strong breakout, supported by its partnership with Amazon Web Services (AWS), surpassing analyst expectations in the fourth quarter. The company's sales through AWS Marketplace reached \$1 billion over four years, solidifying its market position¹⁶. CrowdStrike also performed well despite previous operational disruptions, receiving a buy rating from BTIG analyst Gray Powell, who projected a 16% stock price increase with a target price of \$431, driven by anticipated revenue growth¹⁷. However, not all software companies fared well. ServiceNow, Salesforce, and Adobe faced stock declines due to concerns over government spending cuts and the slow realization of artificial intelligence benefits. Analysts suggest that efficiency improvements could drive a potential recovery for these firms¹⁸. The cybersecurity sector has demonstrated impressive ROI metrics. Google's acquisition of Wiz for \$32 billion in March 2025 turned Index Ventures' initial \$3.5 million investment into a \$4.3 billion windfall, marking a 250-fold return and highlighting the lucrative potential of cybersecurity investments¹⁹. Similarly, private equity firm Thoma Bravo acquired cybersecurity AI company Darktrace PLC for \$5.21 billion in an all-cash deal, further emphasizing the sector's high valuations and returns²⁰.

Future Outlook

Long-term challenges

The cybersecurity industry is facing a consistent shortage of workforce. Even though there is an increasing number of universities offering cybersecurity programs and companies offering certification pathways, the worker supply is still much lower than the demand. The workforce gap was estimated to be 4.8 million, up 19% year over year and forecasted to continue such growth. This will make some companies operate with understaffed cybersecurity teams, meaning that critical security operations may be delayed or mismanaged. This will also drive higher security costs and will concentrate the talent in the major tech hubs, which can lead to further regional shortages.

The increasing complexity of the systems used by companies also poses a potential long-term challenge. Since organizations adopt and integrate multiple third-party services, Internet of Things products, multi-cloud environments and so on, the potential attack surface keeps widening, also requiring more and more specialized personnel and tools. Traditional security measures that worked in the past prove to be inefficient in this increasingly fragmented environment, creating dangerous security gaps. The expansion in usage of AI, quantum computing advancements and newer technologies will only compound on the complexity already existing, forcing the industry to transition to new protocols and methodologies.

¹⁵ Wall Street Journal

¹⁶ Investors.com

¹⁷ Barron's

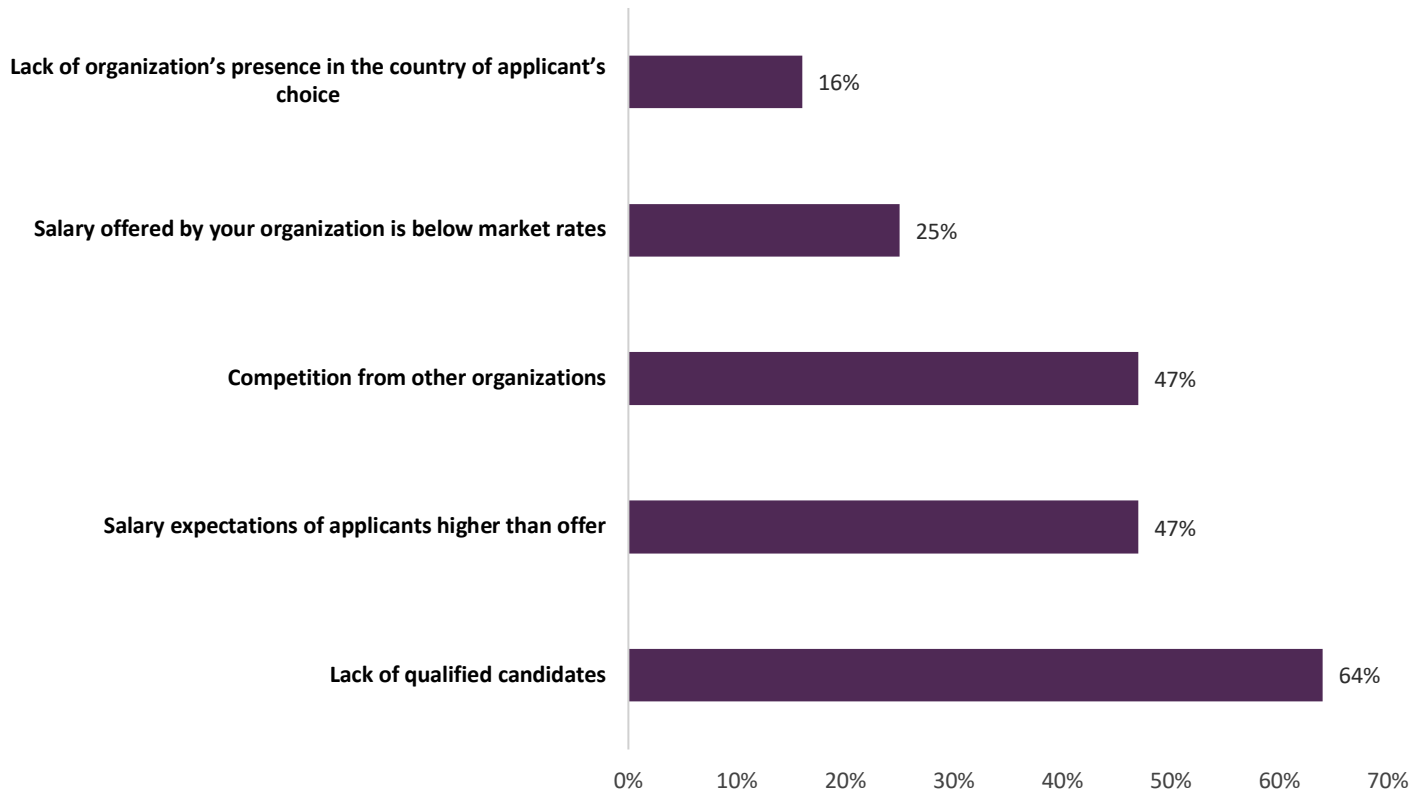
¹⁸ MarketWatch

¹⁹ Wall Street Journal

²⁰ S&P Global

Figure 11: Lack of qualified candidates is the biggest challenge in filling cybersecurity positions

Biggest challenges in filling cybersecurity positions



Source: BCG, Global Cybersecurity Forum, "2024 Cybersecurity Workforce Report", Survey Results

Long-term opportunities

Probably one of the biggest opportunities in the industry is the consolidation into comprehensive platforms, since the fragmentation we experience today is probably going to be unsustainable long-term. Exactly because of the growing complexity of informational systems, there is a strong demand for companies that offer solutions for threat detection, identity management and cloud protection into one product. This means that smaller companies should try to position themselves in very specialized niches to be more appealing acquisitions targets, while bigger companies could take advantage of this trend by developing an M&A strategy for the gaps they have in their portfolio and develop integration plans for future potential acquisitions.

Another opportunity that will be explored in the next years will be the increasing demand for compliance and risk management solutions. Since governments across the world implement continuously stricter regulations concerning data protection, AI usage or critical infrastructure, the companies are faced with complex compliance requirements, which demand specialized expertise and technologies. This regulatory-driven demand should also be particularly resilient during economic downturns, creating a stable, predictable revenue stream for companies that offer solutions for these compliance challenges.

Predicted industry evolution

We are expecting to observe a very strong consolidation trend over the next 5 years, where big players will pursue aggressive acquisition strategies to build comprehensive solutions and platforms, since many small vendors lack any differentiation in segments crowded by many market participants. We think that in turn, small and mid-market companies will be forced to specialize in specific technological niches.

We are also expecting the security service providers to undergo a transformation from the basic monitoring and detection services to a more consultative type of security that combines technology implementation, operational support and advisory services. We are also expecting these service providers to develop deep expertise and highly customizable solutions for specific industries like healthcare, financial services or critical infrastructure. Additionally, the boundaries between network security, endpoint protection and access management will continue to be blurred, being replaced by security models based more on behavior and risk-based access control.

Bibliography

Fortune Business Insights. "CYBERSECURITY MARKET ANALYSIS - 2032." Cybersecurity Market Size, Share & Industry Analysis, vol. 6, no. 1, 2025, p. 160. Fortune Business Insights, <https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165>.

Lindemulder, Gregg, and Matt Kosinski. "What is cybersecurity?" IBM, 12 August 2024, <https://www.ibm.com/think/topics/cybersecurity>.

SailPoint. "Types of cybersecurity." SailPoint, 30 September 2023, <https://www.sailpoint.com/identity-library/five-types-of-cybersecurity>. Accessed 30 March 2025.

Thornhill, John. "Cyber security companies are thriving — even when they fail." Financial Times, 31 October 2024, https://www.ft.com/content/db6a3baa-5d0d-4bbd-a23e-7ea5b3c3c5f7?utm_source=chatgpt.com. Accessed 30 March 2025.

Grand View Research. Cyber Security Market Size, Share & Trends Analysis Report By Offering (Hardware, Software, Services), By Security (Endpoint Security), By Organization Size (Large Enterprises), By Deployment (Cloud), By Solution, By End Use, By Region, And Segment Forecasts, 2025 - 2030. Grand View Research, 2025, <https://www.grandviewresearch.com/industry-analysis/cyber-security-market>.

Fortune Business Insights. "Asia-Pacific Cyber Security Market." *Fortune Business Insights*, www.fortunebusinessinsights.com/asia-pacific-cyber-security-market-107434.

MarketsandMarkets. "Middle East and Africa Cybersecurity Market Worth \$36.2 Billion by 2028 – Exclusive Report by MarketsandMarkets." PR Newswire, www.prnewswire.com/news-releases/middle-east-and-africa-cybersecurity-market-worth-36-2-billion-by-2028---exclusive-report-by-marketsandmarkets-301774833.html.

Statista. "Value of the Cybersecurity Market in Latin America." Statista, www.statista.com/statistics/1180184/value-cybersecurity-market-latin-america/.

Statista, "Cybersecurity, market data & analysis", Statista, <https://www.statista.com/outlook/tmo/cybersecurity/worldwide>

Gartner, "The Expanding Enterprise Investment in Cloud Security", <https://www.gartner.com/en/newsroom/press-releases/2024-06-05-the-expanding-enterprise-investment-in-cloud-security>

Markets.us, "Quantum Cryptography Market", <https://market.us/report/quantum-cryptography-market/>

This research material has been prepared by Minerva Invest. Minerva Invest specifically prohibits the redistribution of this material in whole or in part without the written permission of Minerva Invest. The research officer(s) primarily responsible for the content of this research material, in whole or in part, certifies that their views are accurately expressed and they will not receive direct or indirect compensation in exchange for expressing specific recommendations or views in this research material. Whilst we have taken all reasonable care to ensure that the information contained in this publication is not false or misleading at the time of publication, we cannot guarantee its accuracy or completeness, and you should not act on it without first independently verifying its contents. Any opinion or estimate contained in this report is subject to change without notice. We have not given any consideration to and we have not made any investigation of the investment objectives, financial situation or particular needs of the recipient or any class of persons, and accordingly, no warranty whatsoever is given and no liability whatsoever is accepted for any loss arising whether directly or indirectly as a result of the recipient or any class of persons acting on such information or opinion or estimate. You may wish to seek advice from a financial adviser regarding the suitability of the opinions mentioned herein, taking into consideration your investment objectives, financial situation or particular needs, before making a commitment to any investment. This report is published solely for informational purposes, and it does not constitute an advertisement nor is it to be construed as a solicitation or offer to buy or sell any securities or other financial instruments. No representation or warranty, either expressed or implied, is provided in relation to the accuracy, completeness or reliability of the information contained herein. The research material should not be regarded by recipients as a substitute for the exercise of their own judgement. Any opinions expressed in this research material are subject to change without notice.

© 2025 Minerva Investment Society