McKinsey & Company

Risk & Resilience Practice

The cybersecurity provider's next opportunity: Making AI safer

New technology means new challenges—and new solutions—for cybersecurity providers.

by Justin Greis and Marc Sorel
with Julian Fuchs-Souchon and Soumya Banerjee

November 2024

The rapid advancement of AI and generative AI (gen AI) is fundamentally transforming the cybersecurity landscape, presenting both opportunities and challenges for cybersecurity providers. As more organizations in both the private and public sectors use AI to enhance their operations, they risk inadvertently introducing new cyber-related threats. This is creating a significant and growing demand for advanced cybersecurity solutions.

AI is also being used by bad actors as a tool to fuel more sophisticated cyberattacks and increase their volume, as exemplified by the rise in AI-enhanced social engineering and the substantial financial impact of data breaches. For example, gen AI has enhanced social-engineering techniques, in which attackers generate highly realistic phishing emails or deepfakes to trick employees into sharing sensitive information or credentials. In 2023, the total cost of cybercrime had more than doubled since 2015.[1]

While companies' response time to cyber-related risks has generally decreased over the past several years, it still takes organizations an average of 73 days[2] to contain an incident, highlighting the ongoing difficulty of containing breaches. Combined with an expanding attack surface (that is, more devices and technologies that could be breached or exploited), an increase in threat actor sophistication, a lack of skilled cybersecurity workers, and a wave of new regulations, organizations are increasingly leaning on third parties to help them manage cyber risk.

Helping companies address these risks represents a significant opportunity for providers of cybersecurity solutions, but capitalizing on that opportunity requires considerable investment in innovation and new paths to market.

In addition to securing the general use of AI, using AI to help improve security is also an opportunity for cybersecurity providers. According to our research, customers say today's cybersecurity solutions often fall short of meeting demands in terms of automation, pricing, services, and other capabilities. Helping organizations manage this risk in a cost-efficient manner is a big opportunity for cybersecurity providers, but they will need to understand AI technology and embrace it within their offerings. Innovation also remains critical in traditional cybersecurity products as the market continues to evolve, requiring providers to shift their marketing strategies to meet customers where they are seeking solutions.

AI is expanding what is already a $2 trillion opportunity for cybersecurity providers. In fact, with a large and increasing number of customers wanting to shift workloads from public cloud back to private cloud,[3] organizations will incur new costs, making the capturable value for cybersecurity providers even greater.

As more organizations use AI to enhance their operations, they risk inadvertently introducing cyber-related threats. This creates a significant and growing demand for advanced cybersecurity solutions.

[1] "Why we need global rules to crack down on cybercrime," World Economic Forum, January 2, 2023.
[2] *Cost of a data breach report 2024*, IBM, 2024.
[3] Emil Sayegh, "The evolving cloud landscape: How private clouds are reshaping the tech industry," *Forbes*, November 7, 2023.

Earlier this year, McKinsey surveyed and interviewed more than 200 cyber leaders worldwide, gaining valuable insights into how the cyber market is evolving, including a deep dive into the impact of AI on cybersecurity. Below we examine trends shaping the cybersecurity market and strategic implications for cybersecurity buyers, investors, and providers.

Attacks are increasing, with or without AI

In the face of increasing—and increasingly sophisticated—cyberattacks, organizations spent approximately $200 billion on cybersecurity products and services in 2024, up from $140 billion in 2020.[4] The vended cybersecurity market is expected to grow 12.4 percent annually between 2024 and 2027, outstripping historical levels of growth as organizations look to quell threats. At the same time, organizations are gradually spending more on third-party products than internal labor; about 65 percent of cyber budgets today represent third-party spending, and only 35 percent represent internal labor (Exhibit 1).

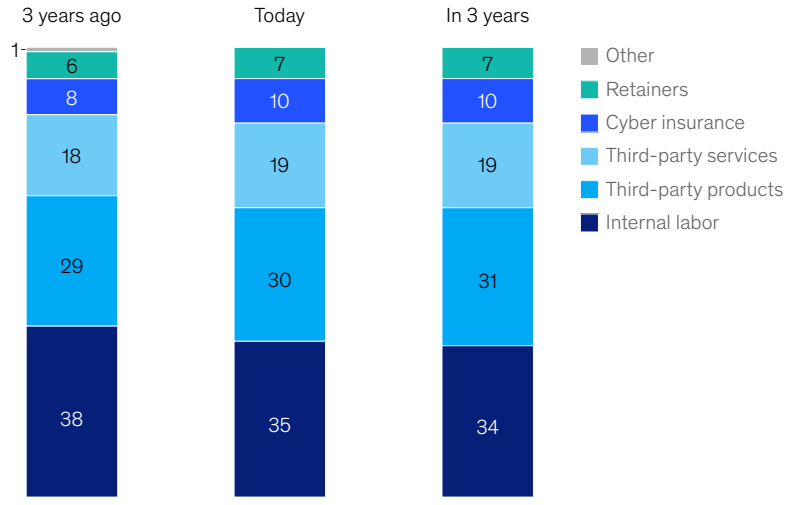
Put another way, there is a trend toward bigger budgets and spending on third-party vendors. This is driven not only by the rising number of breaches but by the cost of complying with newly introduced, strict regulations such as the Securities and Exchange Commission's rules in the United States[5] and the NIS 2 Directive in the European Union.

Organizations can harness the power of AI to help keep pace with attackers. Top cybersecurity providers are already using AI, with 17 of the top 32 cyber suppliers now offering advanced-AI use cases. However, established vendors are not the only ones introducing AI solutions. Investment

Exhibit 1

Companies spend more of their cybersecurity budgets on third-party products and services than they do on internal labor.

Average cybersecurity spending, by type, 2024, % of total cybersecurity budget



Note: Figures may not sum to 100%, because of rounding.
Source: McKinsey Cyber Market Survey, Mar 2024 (n = 200)

McKinsey & Company

[4] McKinsey Cyber Market Survey, March 2024.
[5] "Cybersecurity risk management, strategy, governance, and incident disclosure," US Securities and Exchange Commission, 2023.

in AI-powered cybersecurity start-ups has surged, particularly for application security and data protection start-ups. More than 70 percent of cybersecurity buyers at large organizations across most industries are “highly willing” to invest in AI-enabled cybersecurity tooling, though enthusiasm to adopt differs by industry. Customers are also looking not only to enhance cybersecurity capabilities with AI but also to secure other AI use cases within their organizations.

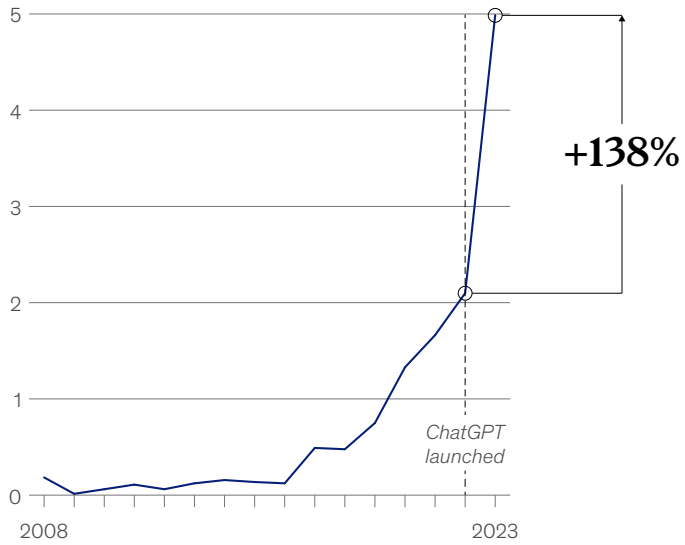
A growing attack surface is leading to higher risk exposure

The cybersecurity landscape today is fraught with familiar threats. Phishing, business email compromise, and stolen credentials are leading to breaches that are costing organizations an average of $5 million per successful incident. AI and gen AI have added a new level of danger to traditional attacks, making them harder to detect using traditional means. (Exhibit 2).

Exhibit 2

Cyberattackers continue to use generative AI to accelerate phishing as their primary method of attack.

Annual number of phishing sites detected, million



Source: *State of the Phish Report,* Proofpoint, 2023

McKinsey & Company

AI-enhanced advances also make it easier to exploit a growing attack surface, in turn introducing new risk exposure (Exhibit 3). AI-based attacks can target the traditional perimeter (for example, endpoints, servers), the modern perimeter (for example, identities, applications), and the expanding perimeter (for example, social media, data, collaboration tools). There is a growing number of devices, identities, and tools across perimeters, ranging from roughly 7 to 30 percent.

These attacks have already exploded in volume. Since the proliferation of gen AI platforms, starting in 2022, phishing attacks have risen by 1,265 percent. In short, bad actors have not only ramped up their ability to find vulnerabilities but also launched an unprecedented new wave of attacks.

Regulatory regimes and talent gap as key market drivers

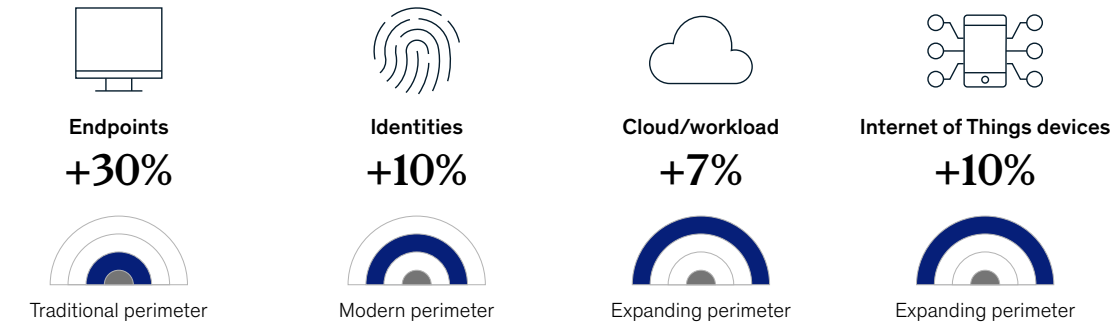
Amid this growing threat, a regulatory landscape is rapidly evolving to ensure that organizations remain resilient and are responsible stewards of customer data. Rule makers have zeroed in on secure development, data protection, reporting, and resilience. Beginning in 2023, the United States introduced several new regulatory frameworks, including Executive Order 14110[6] and CIRCIA.[7] Outside of the United States, the European Union has proposed the Cyber Resilience Act and has instituted the NIS 2 Directive and DORA[8] frameworks. To remain or achieve compliance with such regulations requires a growing cost to organizations, driving demand for cybersecurity products and services. For instance, compliance with the European Union's NIS 2 Directive is expected to increase cyber budgets by up to 22 percent in the first years following its implementation. Already, cyber regulatory risk remediation constitutes an average of more than 10 percent of cyber budgets.

The cybersecurity industry will need to fortify its talent base and resources to meet both increased threats and regulatory demands. Workers trained in cloud security, AI, and zero-trust[9] (for example,

Exhibit 3

The cyberattack surface is expanding, leading to additional risk exposure.

Expected increase in risk exposure in the next 3 years, select examples, %



Source: McKinsey Cyber Market Survey, March 2024 (n = 200)

McKinsey & Company

[6] Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence, October 30, 2023.
[7] Cyber Incident Reporting for Critical Infrastructure Act (proposed).
[8] Digital Operational Resilience Act 2022. DORA was published in the EU's Official Journal on December 27, 2022, and entered into force on January 16, 2023. It will apply in full on January 17, 2025.
[9] In this security system design, all entities—inside and outside the organization's computer network—are not trusted by default and must prove their trustworthiness.

ZTNA[10]) implementation are and will be the biggest need (Exhibit 4).

For those charged with keeping organizations safe, these new AI-based threats pose an unprecedented challenge—they are more sophisticated, unrelenting, and shifting. They are also growing exponentially.

How cybersecurity providers can capture the $2 trillion opportunity

Providers can take a series of steps to address increasing threats and seize the opportunity they present (Exhibit 5). In our work with clients and with the information collected in the survey, we have identified four clear pathways that providers can follow.

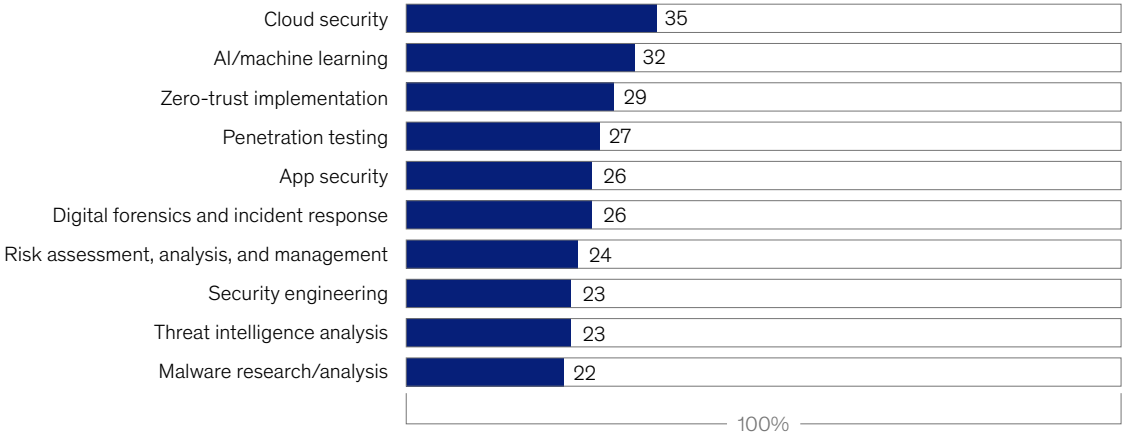
Develop AI-infused cyber products and new offerings to secure AI applications

Given the recent advancements in AI, existing cybersecurity providers are working hard to integrate AI into their existing security products. More than 90 percent of cybersecurity AI capabilities are expected to come from third-party providers.[11] As AI and gen AI have rapidly advanced during the past 12 to 18 months, most leading cyber providers have already announced AI upgrades to their existing product suite. Our survey results show that cloud security, security operations (SecOps), and endpoint security are among the market segments that will benefit the most from AI use cases. Most current AI-infused cyber products are focused on SecOps threat detection and incident response, and there are market opportunities and expectations for AI

Exhibit 4

The cybersecurity industry's biggest talent gap is in cloud security and AI/machine learning.

Share of cybersecurity professionals reporting skills gap at organization, %



Source: *Cybersecurity Workforce Study 2023*, ISC2

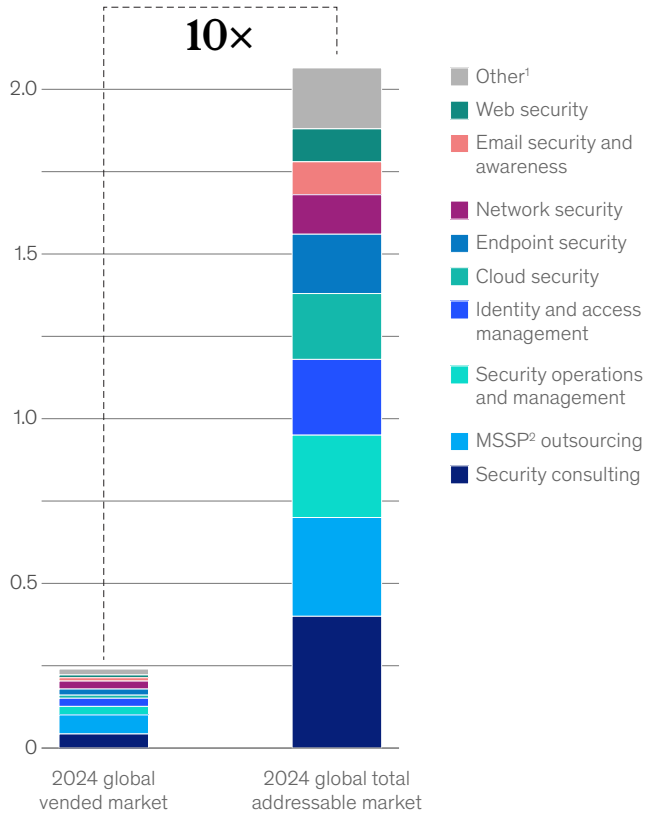
McKinsey & Company

[10] Zero Trust Network Access is a security service that allows secure access to applications, data, and services by verifying users and devices before granting access.
[11] *Securing generative AI*, IBM, 2024.

Exhibit 5

The global addressable market for cybersecurity could reach approximately $2 trillion.

Global cybersecurity market value, 2024,
$ trillion



[1]Includes governance, risk, and compliance; data protection; application security; Internet of Things; operational technology; and AI security.
[2]Managed security service provider.
Source: McKinsey Cyber Market Map, 2024

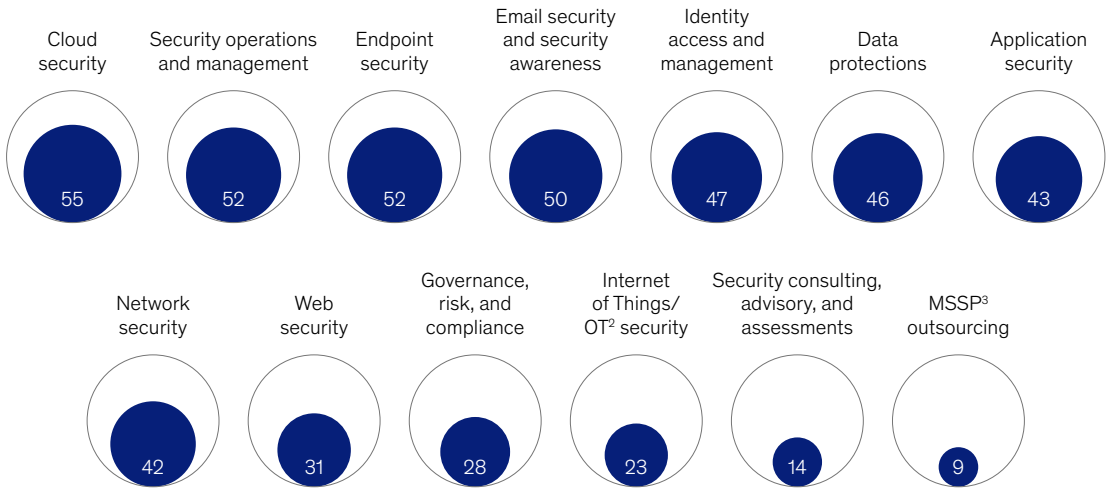
McKinsey & Company

use cases in cloud and endpoint security. Gen AI for SecOps threat detection includes suggesting and writing detection rules and queries for security information and event management by assisting in sifting through large data sets to uncover hidden threats or recommending actions to security-operations-center analysts. Providers have reported to us time savings of up to 20 to 25 percent. Also on the horizon are promising AI use cases and features such as everyday AI assistants for (nonsecurity) employees to autofill security questionnaires and reports. Providers also revealed that gen AI for autofilling security questionnaires can add time savings of up to 80 percent. For providers, the upgrades can add increased product performance and, as they will be able to increase their prices for an AI-infused product offering, a return on investment (Exhibit 6).

Exhibit 6

Generative AI is expected to significantly benefit many segments of the cybersecurity market.

Market segments that will significantly benefit from generative AI,[1] % of respondents



[1]Question: In your experience, which cybersecurity capabilities would significantly benefit from generative AI (eg, more automation through copilots, more threat detection, or faster response)?
[2]Operational technology.
[3]Managed security service provider.

McKinsey & Company

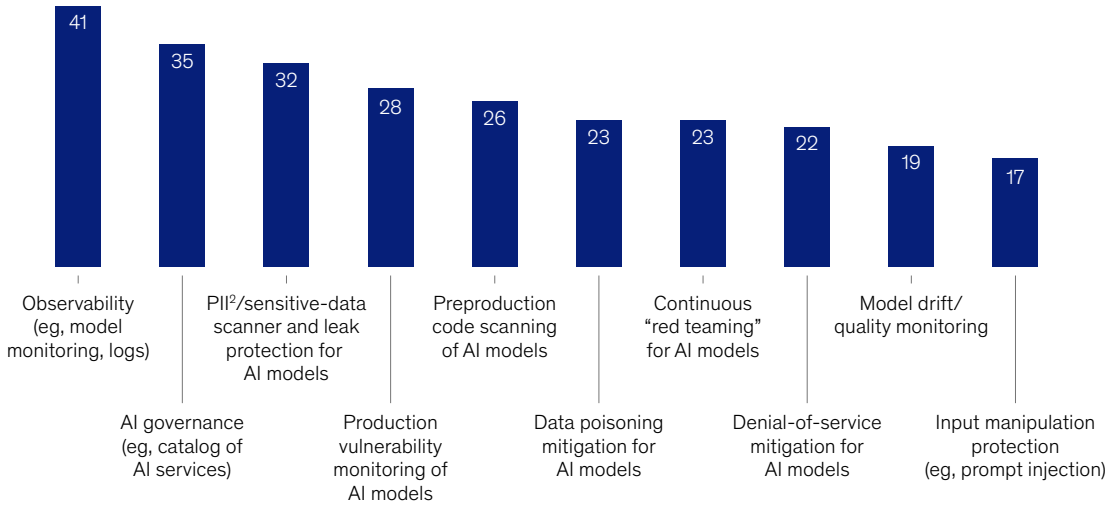
Besides the need to upgrade existing security offerings, corporations are seeking to build and integrate AI into various areas of business. Securing these new AI systems is high on the agenda for many companies. Our survey finds that vulnerability in cybersecurity is one of the top three most-cited risks of AI adoption, and many companies are prioritizing the safety of these new systems. After observability and governance, sensitive-data scanning, vulnerability monitoring, and code scanning are the top security AI use cases and will require investment. Nearly all customers (more than 97 percent) anticipate spending more on outside vendors to secure AI use cases, and 52 percent say securing AI systems will increase vendor costs by more than 5 percent (Exhibit 7). In our Cyber Market Map, 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.

Customers are looking to secure AI use cases primarily through existing vendors, but they are willing to seek out new vendors if existing vendors cannot sufficiently secure in-house AI systems.

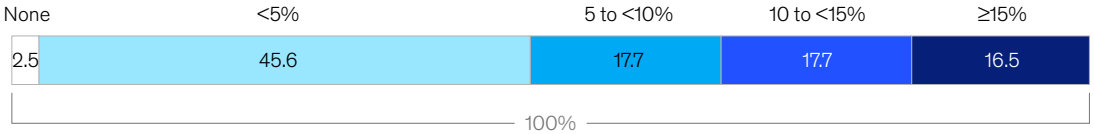
Exhibit 7

Organizations have clear needs and allocated budgets to address cybersecurity-related AI risks.

Top AI security capabilities customers are looking to adopt,[1] % of respondents selecting option as a top 3 capability



Additional third-party spend needed to secure AI use cases,[3] % of respondents



[1]Question: Which AI security capabilities is your organization looking to adopt?
[2]Personal identifiable information.
[3]Question: How much additional costs will you expect to incur to secure these AI use cases (if any)? Please answer as a % relative to existing cost of relevant vendor products/services.
Source: McKinsey Cyber Market Survey, March 2024 (n = 200)

McKinsey & Company

In short, providers that can secure AI and tailor offerings to priority customer use cases will have a competitive advantage (Exhibit 8).

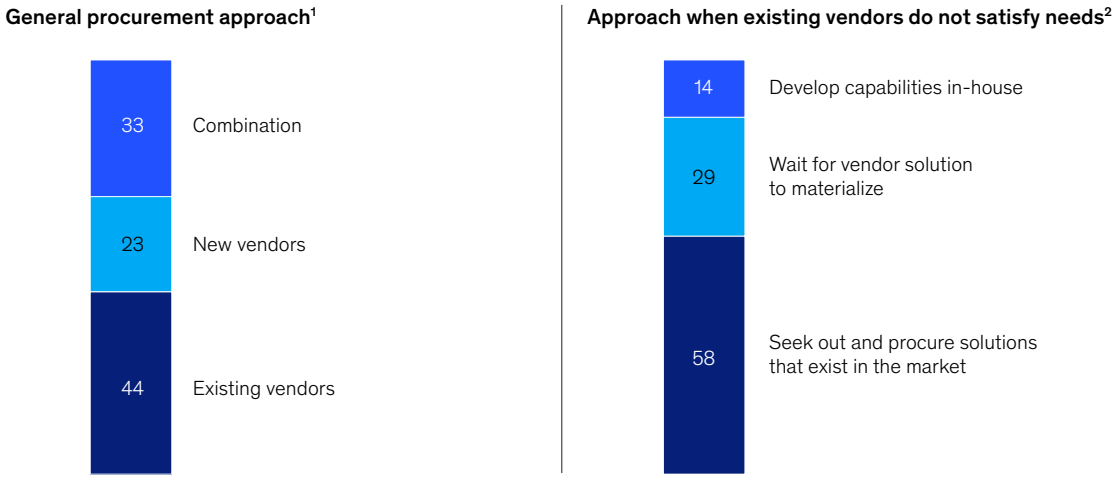
Adapt a go-to-market approach to evolving market dynamics

Evolving market dynamics are changing the way cybersecurity providers reach potential customers. Today, nearly 15 percent of cybersecurity spending comes from outside the chief information security office (CISO), and non-CISO cyber spending is expected to grow at a 24 percent CAGR over the next three years (Exhibit 9). This has changed from a decade ago, when almost all cybersecurity spending came from the CISO organization. Providers will need to increasingly cater to non-CISO customers, with most non-CISO cyber spending coming from buying centers responsible for cloud, product, network, and audit and compliance.

Exhibit 8

Customers will give current vendors first opportunity to secure AI use cases but won't wait long to seek other options if needs aren't met.

Approach to securing AI/generative AI use cases, % of respondents



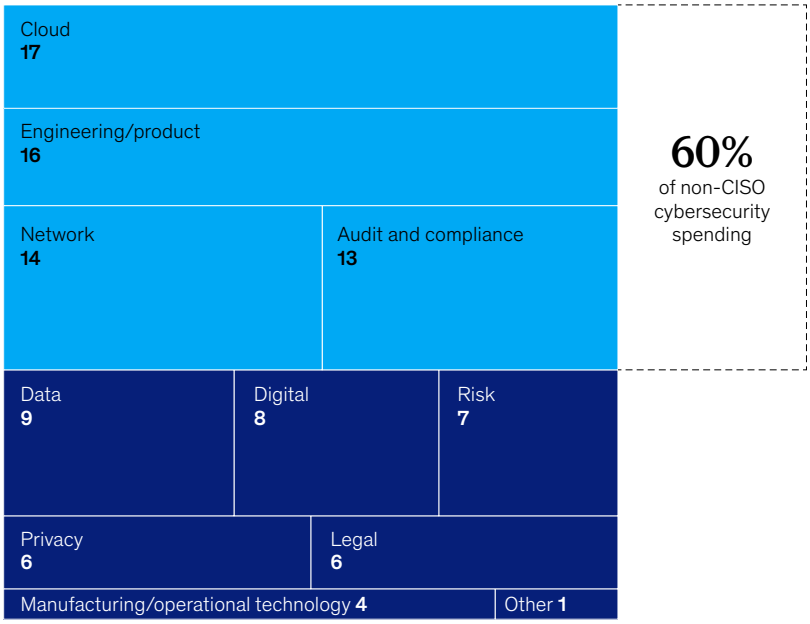
Note: Figures may not sum to 100%, because of rounding.
[1]Question: To what extent do you expect to secure AI/generative AI use cases through existing vendors vs new tools?
[2]Question: For capabilities not satisfied by existing vendors, which of the following actions are you planning to take?
Source: McKinsey Cyber Market Survey, Mar 2024 (n = 200)

McKinsey & Company

Exhibit 9

Companies are steering cybersecurity spending to outside vendors, with cloud security the biggest source of external spending.

Average source of cybersecurity spending outside chief information security office (CISO),[1] %



Note: Figures do not sum to 100%, because of rounding.
[1]Question: In your best estimation, how much of your cybersecurity spend comes from outside of your CISO organization? Where does that non-CISO cyber spend come from?
Source: McKinsey Cyber Market Survey, March 2024 (n = 200)

McKinsey & Company

Second, while most cyber sales and marketing dollars are historically spent on direct-sales and digital-sales campaigns, customers are now leaning into education and reputation to help them find providers. Customers are using industry reports, referrals, and industry analyst consultations in their decision making. They are also turning to service providers and value-added resellers when purchasing solutions.

Finally, customers that do buy cybersecurity services say improving cybersecurity maturity scores and risk ratings are big factors in their decision. These metrics are also valuable when customers want to communicate the impact to stakeholders.

Adapting the go-to-market strategy to these changing market dynamics can help companies capture a larger piece of the pie.

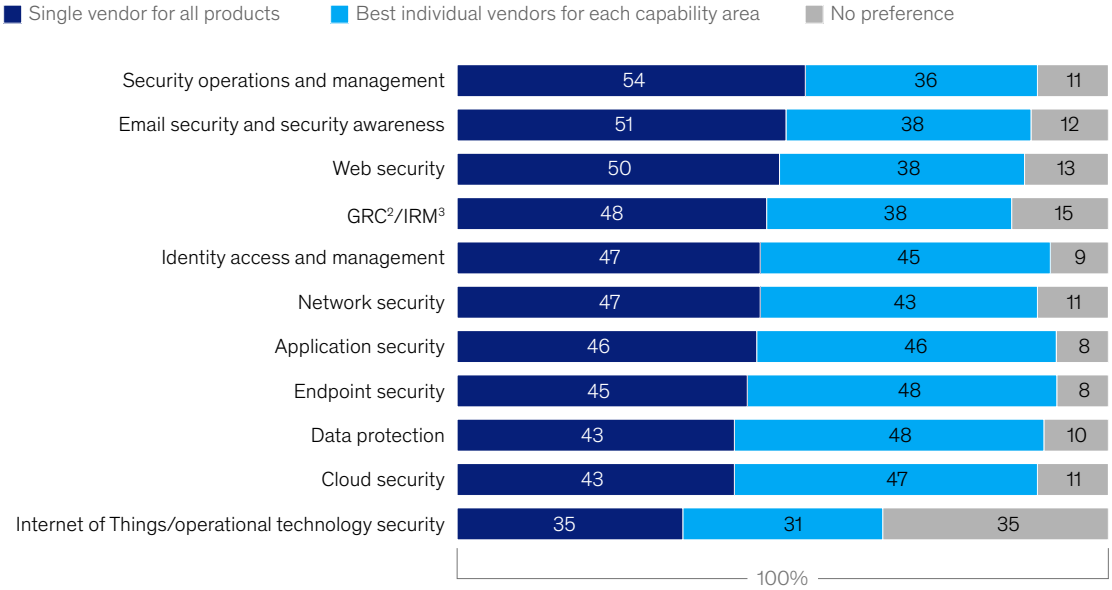
Create all-in-one offerings for highest-priority customer use cases

Our survey suggests 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. In practice, most customers are still using a broad array of cybersecurity products, with larger organizations using as many as 50 to 200 of them. Some are shifting to vendors that provide the biggest suites, but many still rely on best in class. Providers can therefore try to cater to both types of customers, building best-of-suite bundled offerings around standout best-of-breed offerings (Exhibit 10).

Exhibit 10

The cybersecurity market is at an inflection point on 'best of breed' vs 'best of suite.'

Cybersecurity vendor preferences, by capability,[1] % of respondents



Note: Figures may not sum to 100%, because of rounding.
[1]Question: In the future, will your company prioritize finding a single vendor for all of your products (ie, "best of suite") vs the best individual vendors for each capability area (ie, "best of breed")?
[2]Governance, risk, and compliance.
[3]Integrated risk management.
Source: McKinsey Cyber Market Survey, March 2024 (n = 200)

McKinsey & Company

For example, if a provider has a best-of-breed offering today, it can look to develop best-of-suite offerings through acquisition, the development of new products, or the bundling of existing ones. It can also look to build best-of-suite offerings through partnerships such as enterprise resource planners and customer relationship planners. Practically, providers can create these best-of-suite offerings around common cross-segment packages today.

While providers are turning to best-of-suite bundled offerings, there is also a shift toward consolidation. In three years, customers expect to use fewer vendors for network and endpoint security. At the same time, there has been a steady decline in the number of new cybersecurity companies formed since 2017, suggesting a maturing market ripe for consolidation.

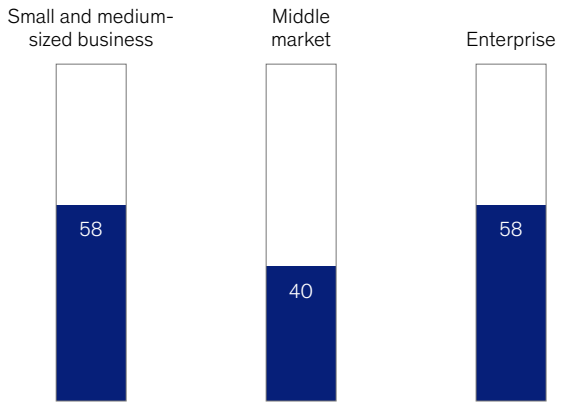
Prioritize innovation beyond AI

Beyond AI, there continues to be customer demand for innovation, especially for zero-trust capabilities. Zero-trust architecture has the potential to increase adoption rates over the next three years, with the highest potential demand in middle-market companies (Exhibit 11). Providers can increase zero-trust adoption for middle-market customers by assuaging customer concerns that legacy systems and fragmentation inhibit zero-trust adoption within a company's environment.

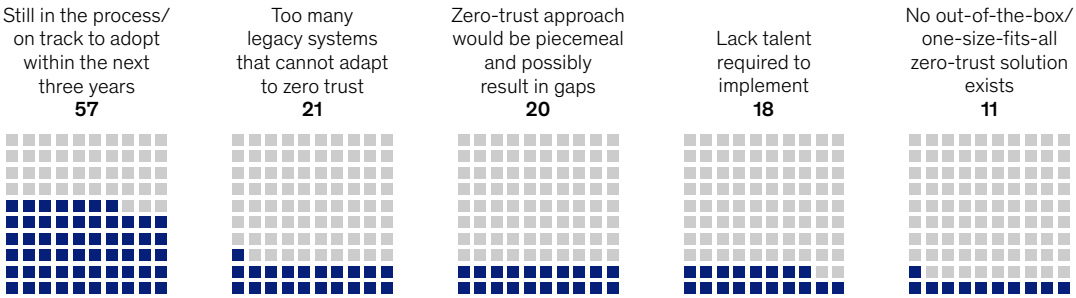
Exhibit 11

Zero-trust architecture has the potential to be more widely adopted, especially in middle-market companies.

Zero-trust architecture adoption,[1] by company size,[2] % of respondents



Top 5 reasons for not adopting zero-trust architecture,[3] % of respondents whose organization has not adopted zero-trust architecture (n = 56)



[1]Question: Do you have a zero-trust architecture today?
[2]Small and medium-sized business = <500 employees (n = 12); middle market = 500–4,999 employees (n = 52); enterprise = ≥5,000 employees (n = 48).
[3]Question: Why hasn't your organization adopted zero trust?
Source: McKinsey Cyber Market Survey, March 2024 (n = 200)

McKinsey & Company

Extended detection and response (XDR) products are also popular immediate solutions in that they provide security across all parts of an organization: endpoints, network, cloud, and more. XDR providers tend to differentiate on their telemetry, as customers look to efficient high-fidelity curated signals compared with comprehensive but tedious, resource-intensive monitoring of logs. Customers are expecting to see about a 25 percent increase in log visibility in three years, and providers that can deliver more advanced telemetry could capture a larger share of the pie. Quantum security—which refers to defense against powerful quantum-computing attacks—is seen as a more medium-term priority. While quantum is further out on the adoption curve, most industries say quantum is less than five years away from being part of their cyber budget, with software and consumer and retail the most likely to adopt. Identification of where encryption keys are stored and automated recycling of encryption keys are two promising use cases where quantum is expected to play a role.

Cyber insurance is also gaining significant momentum and attention, especially after the recent global outages. While cyber-insurance firms have significantly improved their assessment and loss ratio on cyber-insurance coverage, nearly 50 percent of companies that have cyber-insurance coverage do not feel adequately covered by it, according to the survey. There is a significant opportunity, therefore, for cyber-insurance firms to improve their insurance coverage at the right price point in the cyber market.

As the cyber market expands, providers must keep pace

Cybersecurity has always been a dynamic field of moving targets and threats. The emergence of AI and gen AI presents a new challenge for companies while also amplifying existing threats. Organizations in need of cybersecurity to meet the moment are looking to providers to help ensure that these new and fast-developing technologies are manageable and that their institutions and clients remain safe.

Just as the environment has changed, cybersecurity investors and providers need to shift as well. They must rethink and innovate their products while also reshaping their approach to reaching customers.

Providers can assuage their clients' concerns and harness the dynamic changes already taking place to grow their own businesses and positions in the marketplace. To do so, they can tailor their offerings, revise how they communicate and market themselves to customers, create products that appeal to nontraditional buyers of cybersecurity services, and, finally, keep innovating on all fronts.

Justin Greis is a partner in McKinsey's Chicago office, **Marc Sorel** is a partner in the Boston office, **Julian Fuchs** is a knowledge expert in the Stuttgart office, and **Soumya Banerjee** is an associate partner in the New Jersey office.

The authors wish to thank Anatoly Brevnov, Bharath Aiyer, Elisa Becker-Foss, Jeffrey Caso, Kevin Telford, Nick Curcio, and Wolfram Salmanian for their contributions to this report.

This article was edited by David Weidner, a senior editor in the Bay Area office.

Designed by McKinsey Global Publishing