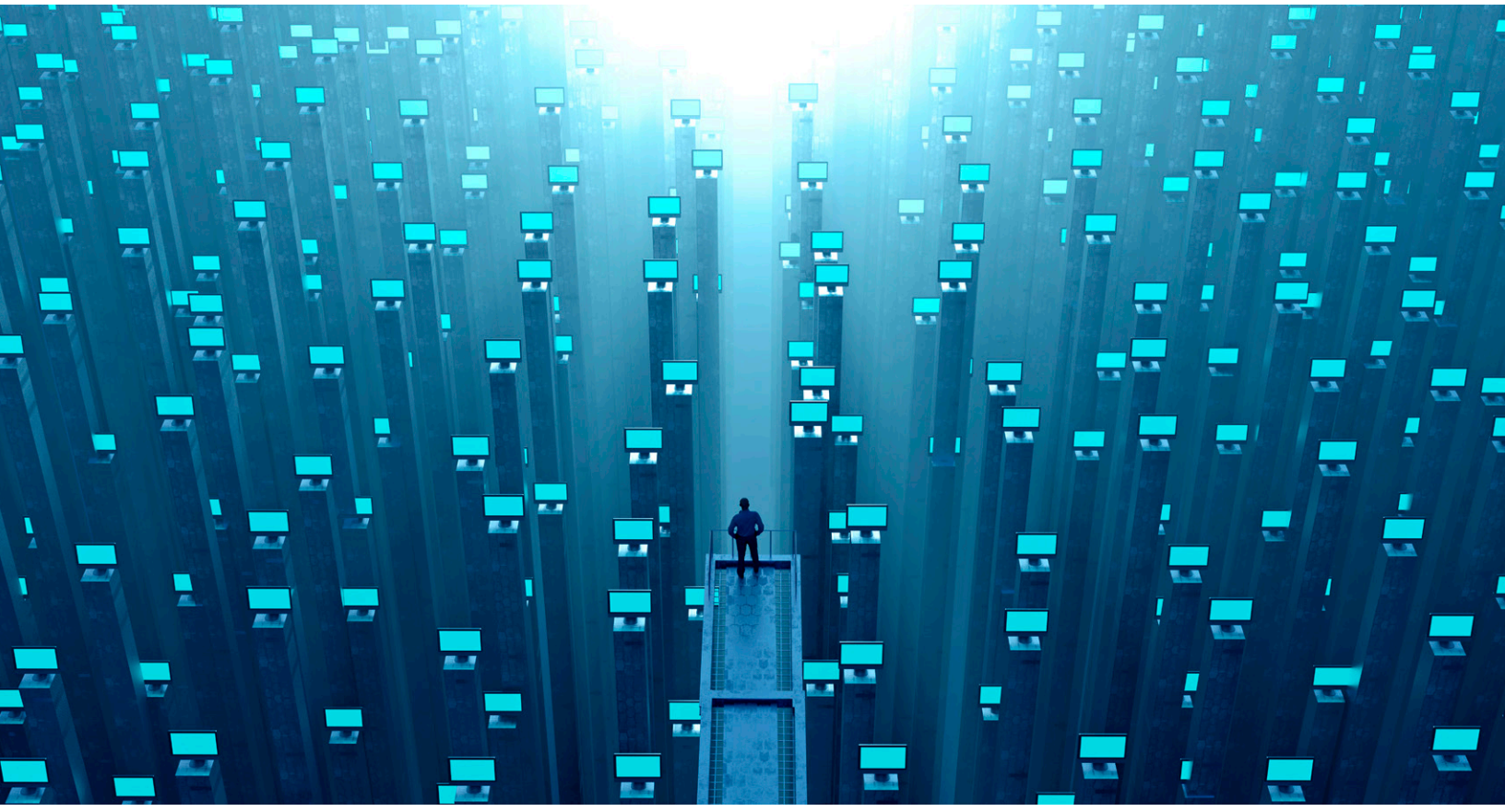
McKinsey & Company

Cybersecurity Practice

# New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers

Cyberattacks are proliferating, causing trillions of dollars of damage every year. The cybersecurity industry has a chance to step up and seize the opportunity.

*by Bharath Aiyer, Jeffrey Caso, Peter Russell, and Marc Sorel*





October 2022

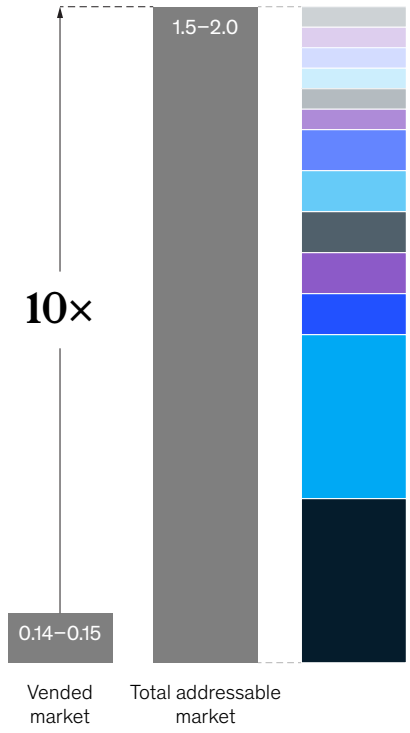
**As the digital economy grows,** digital crime grows with it. Soaring numbers of online and mobile interactions are creating millions of attack opportunities. Many lead to data breaches that threaten both people and businesses. At the current rate of growth, damage from cyberattacks will amount to about $10.5 trillion annually by 2025—a 300 percent increase from 2015 levels.[1]

In the face of this cyber onslaught, organizations around the world spent around $150 billion in 2021 on cybersecurity, growing by 12.4 percent annually.[2] However, set against the scale of the problem, even this "security awakening" is probably insufficient. A survey of 4,000 midsized companies suggests that threat volumes will almost double from 2021 to 2022.[3] According to the survey, nearly 80 percent of the observed threat groups operating in 2021, and more than 40 percent of the observed malware, had never been seen previously. These dynamics point to significant potential in an evolving market. Currently available commercial solutions do not fully meet customer demands in terms of automation, pricing, services, and other capabilities—which this article will explore in further detail. As a result, the gap today between the $150 billion vended market and a fully addressable market is huge. At approximately 10 percent penetration of security solutions today, the total opportunity amounts to a staggering $1.5 trillion to $2.0 trillion addressable market

Exhibit 1

## The global cybersecurity total addressable market may reach $1.5 trillion to $2.0 trillion, approximately ten times the size of the vended market.

**Global cybersecurity market size, 2021,** $ trillion




| Segment | Total addressable market, $ billion | Current penetration, % |
|---|---|---|
| Data protection | 50–100 | 30–35 |
| Governance, risk, and compliance | 50–100 | 30–35 |
| Email security and awareness | 50–100 | 10–15 |
| Cloud security | 50–100 | 1–5 |
| Network security | 50–100 | 15–20 |
| Identity and access management | 50–100 | 20–25 |
| Security consulting | 100–200 | 15–20 |
| Web security | 100–200 | 5–10 |
| IoT/OT[1] | 100–200 | 1–5 |
| End point security | 100–200 | 5–10 |
| Application security | 100–200 | 1–5 |
| Security and operations management | 400–500 | 1–5 |
| MSSP[2]/outsourcing | 400–500 | 5–10 |

[1]Internet of Things/operational technology.
[2]Managed security service provider.
Source: McKinsey Cyber Market Map 2022

[1] Steve Morgan, "2022 Cybersecurity Almanac: 100 facts, figures, predictions, and statistics," *Cybercrime Magazine*, January 19, 2022.
[2] Growth is compounded.
[3] *The biggest cyber security threats coming in 2022*, Coro.

(Exhibit 1). This does not imply the market will reach such a size anytime soon (current growth rate is 12.4 percent annually off a base of approximately $150 billion in 2021), but rather that such a massive delta requires providers and investors to "unlock" more impact with customers by better meeting the needs of underserved segments, continuously improving technology, and reducing complexity—and the current buyer climate may pose a unique moment in time for innovation in the cybersecurity industry.

The underpenetration of cybersecurity products and services is, on the face of it, the result of the below-target adoption of cybersecurity products and services by organizations—which suggests that the budgets of many if not most chief information security officers (CISOs) are underfunded. Cybersecurity providers must meet the challenge by modernizing their capabilities and rethinking their go-to-market strategies.

To maximize the opportunity, providers must get a grip on the factors shaping the market, the segments most likely to grow, and the services customers need. Here we set out four areas likely to be the focus of such discussions: cloud technologies, pricing mechanisms, artificial intelligence, and (particularly in the midmarket) managed services. With strategic planning in these areas, and a robust approach to implementation, cybersecurity providers can make themselves more competitive and get a slice of the $2 trillion pie.

## Growing cybermarket potential

Why does the cybermarket offer such significant potential right now? We see five key drivers.

### More attacks targeting smaller companies

From a demand perspective, fast-growing smaller organizations are exposed to proliferating digital touchpoints and ecosystem relationships. In addition, malware such as ransomware can pose an existential threat to small and midsize businesses (SMBs) and midmarket companies in a way it often doesn't to large enterprises. What might remain a silent breach at a larger organization is often a significant, overt disruption at a smaller one. For example, a Texas-based midsize steel structure manufacturer was forced into bankruptcy in May 2019 when ransomware permanently encrypted both its tooling and financial accounting software. Ransoms can be out of reach, while information retrieval and recovery services are timely and difficult. Moreover, the trust of customers can prove difficult to recover once a company has been breached. In fact, according to previous McKinsey research on the importance of digital trust, in the past 12 months nearly 10 percent of respondents reported stopping business with a supplier after learning of a data breach.

Midmarket entities are often targeted by criminals looking to exploit unsophisticated security tooling. These companies, for example, may miss threats such as EternalBlue, an exploit developed by the US National Security Agency and later used by Wannacry ransomware. Many smaller entities use a single-backup strategy, which can leave them susceptible to attacks from ransomware such as PureLocker.

The proliferation of ransomware attacks targeting SMBs and midmarket companies means that even those that don't currently employ or engage a security team have a responsibility to act. Fortunately, the SMB segment is becoming truly addressable by cybersecurity products and services for the first time, thanks to emerging economies of scale.

### The impetus from regulation

At least 45 states and Puerto Rico introduced or considered more than 250 bills or resolutions that deal significantly with cybersecurity.[4] Federal initiatives include the US National Defense Authorization Act, Executive Order 14028,[5] and the extension of the False Claims Act to include the misrepresentation of an organization's cybersecurity program and qualifications.

[4] Cybersecurity Legislation 2021, National Conference of State Legislatures, July 1, 2022.
[5] Improving the Nation's Cybersecurity: NIST's Responsibilities, May 2021.

Based upon McKinsey's client conversations, federal cybersecurity contracting requirements are trickling down to thousands of SMB and midmarket contractors. The US Securities and Exchange Commission (SEC) is discussing new rules on breach notifications. Compliance challenges grow more onerous as ecosystems proliferate. The Department of Defense's Cybersecurity Maturity Model Certification (CMMC), for example, underscores the critical importance of holistic cybersecurity, much of it beyond the reach of SMBs and the mid-market unless they get help from vendors.

Rules around the world are equally stringent. The European Union's General Data Protection Regulation, for example, may levy fines of up to 4 percent of global turnover against companies that fail to protect their customers.[6]

**CISOs are as serious as ever about closing the (log) visibility gap**

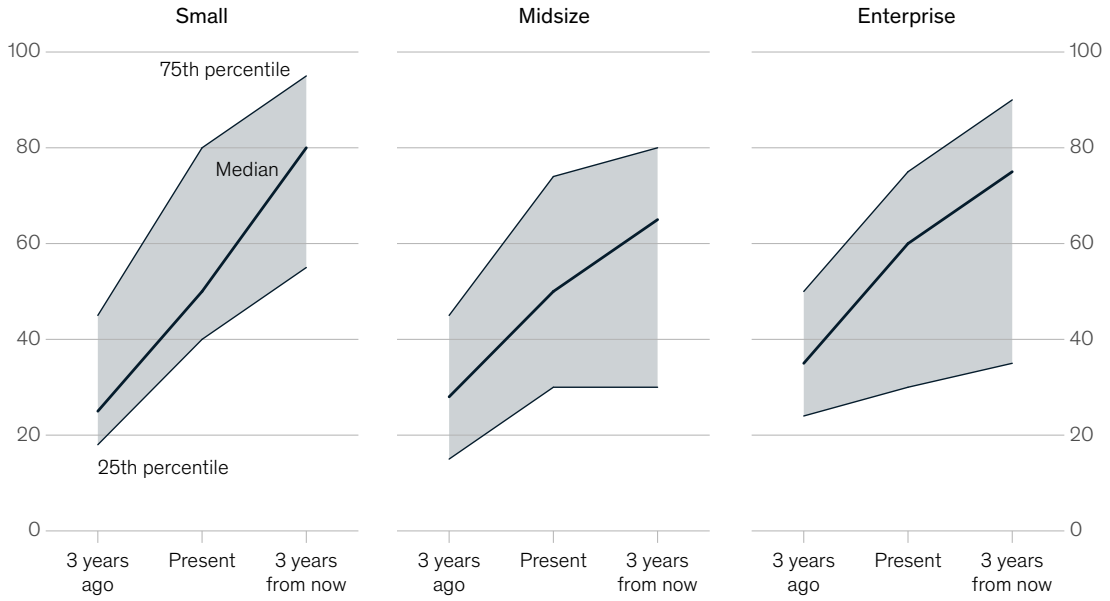
Moves to ramp up log processing are critical because just three years ago the average enterprise saw only 30 percent of what was happening. Finding more needles in the haystack will probably require more commitment—in particular, in areas such as AI, which can spot cyberthreats and malicious activities. For providers, AI will force a rethinking of technology and how they bring it to market.

Over the past three years, companies have boosted their share of total log volume visibility from about 30 percent to about 50 percent on average and are pushing toward 65 to 80 percent over the next three years (Exhibit 2).[7] SMBs and the midmarket have been slightly more active than larger enterprises, and future growth in visibility use cases is predicted

Exhibit 2

## Chief information security officers expect enterprise visibility and log consumption to rise, but performance will vary.

**Share of total log volume monitored across enterprise network by company size,**[1] %




[1]Question: What percentage of total log visibility would you estimate your security operations center SIEM (security information and event management) currently has in total across the enterprise network? N = 173.
Source: McKinsey Cyber Market Map 2022

[6] An earlier version of this article incorrectly stated that the European Union's General Data Protection Regulation may levy fines of up to 2 percent of global turnover, when 2 percent only represents the possible fine for "less severe" violations. The "most severe" violations may fine up to 4 percent of revenue.
[7] McKinsey Cyber Market Map Survey.

# A global cybersecurity talent shortage means that IT leaders often have little choice but to do business with third-party service partners.

to be stronger among these smaller companies. SMBs expect to widen their deployment of end point detection and response (EDR) tooling, to use single panes of glass that ingest and monitor their cloud environments, and to rely on managed-service partners (such as providers of managed detection and response services) for more sophisticated activities.

A surprising aspect of the current market landscape is the significant extent to which the slowest-moving enterprises are trailing their faster-moving peers. Bottom-quartile enterprises report lifting their log volume visibility by just 6 percent over the past three years and forecast a meager 5 percent rise in the next three. By comparison, the best performers, particularly in the SMB segment, increased their log coverage by between 25 and 35 percent in the past three years and plan to accelerate those efforts over the next three.

**Talent shortages and service offerings**

An existing global cyber-talent shortage, compounded by the intensification of digital threats like ransomware during the COVID-19 pandemic, has created further growth opportunities for service providers as CISOs and talent partners struggle to fully staff their organizations. Structural dynamics are also boosting demand for vended solutions. As companies build out their protections, buyers increasingly expect products to come bundled with offerings that ensure both short-term services (for instance, implementation) and long-term ones (ongoing security).

The bottom line? Across all segments, forecasted changes in allocated security spending is increasing as a percentage of services between internal and third-party services. So long as talent remains a problem, outsourced services will be essential for companies that need to support strong security outcomes.

**Higher levels of customer engagement**

Until recently, many organizations that required cyber protection were not fully engaged with the challenges they faced. Often, they saw the cost and complexity of action as greater than the need for it. Now, with attacks becoming more frequent, the risk–benefit equation has changed. With security and privacy concerns being elevated to the C-suite across industries, geographies, and enterprises whatever their size, both providers and investors have opportunities. We see potential for innovation in prices and bundles, geographic coverage, target customer groups, integration, and off-the-shelf analytics.

## Providers can excel on four fronts

To gauge the market opportunity, McKinsey used a bottom-up model: an assessment of key players and validation against industry logic and our conversations with clients. We also surveyed 500 cybersecurity buyers and interviewed 50 market-leading vendors. The combined insights, tracked in McKinsey's Cyber Market Map, show that spending on products and services from vendors is set to rise 13 percent annually up to 2025—a significant

uptick from 10 percent growth over the past three to five years. Key changes to previous market forecasts include not only faster growth, with services increasing much faster than products, but also a significant opportunity in the SMB segment.

For providers, the message is clear. Current market dynamics give them a chance to boost their penetration of both existing accounts and the unvended space. This growth will be spurred by an evolving threat landscape and talent shortages—a gap of at least 600,000 in the United States alone.[8] To maximize the opportunity, we see potential for action on four fronts.

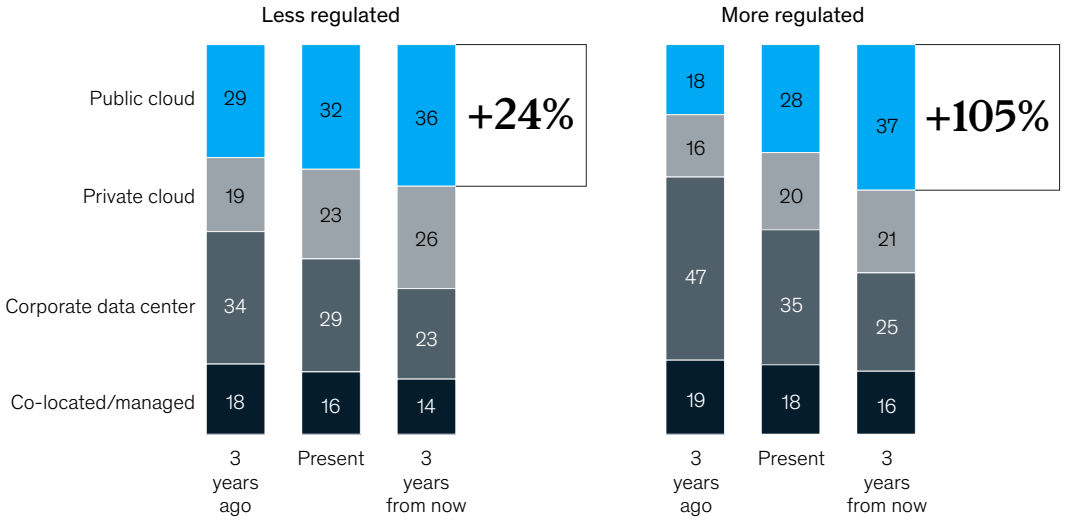
**Ride the coattails of the cloud transformation**
Public-cloud migrations will continue to define enterprise technology strategies for the next several years (Exhibit 3). Providers (especially product providers) should thus consider not only accommodating but also specializing in hybrid and multicloud architectures.

Where cloud providers offer cybersecurity solutions, the tooling on offer in many cases is not a comprehensive substitute to the capabilities of cybersecurity specialists—at least in the enterprise segment. Organizations that adopt multicloud strategies or maintain critical on-prem workloads will in all likelihood persistently need best-of-breed solutions. The challenges that vendors are expected to help resolve include ease of implementation, day-to-day ease of use, integration and coverage across environments, and agility and flexibility in attack environments. If information about an attack detected in one cloud provider environment is not conveyed immediately to other cloud environments, for example, that lapse would amount to a tooling failure.

Exhibit 3

## Highly regulated industries are migrating to public cloud four times faster than less regulated industries.

**Share of total workloads by disposition,** %




Note: More-regulated industries include banking, insurance, government; less-regulated industries include manufacturing, software, media, and education.
Figures may not sum to 100%, because of rounding.
Source: McKinsey Cyber Market Map 2022

[8] Olivia Rockeman, "Hackers' path eased as 600,000 US cybersecurity jobs sit empty," Bloomberg, March 30, 2022.

In many security-related markets, characterized by large numbers of tools, entire categories of orchestration players (such as those that orchestrate security and the identity of users) have been created to simplify the combination of parallel processes. Antifraud programs, for instance, require so many different sets of tooling to manage different geographies that a new category has emerged to manage workflows. In another example, in the cloud, orchestration coordinates workflows and the deployment and management of data across multiple public and private clouds, software-as-a-service (SaaS) providers, managed data centers, and on-prem infrastructure enterprises. All of these demands for increased visibility are potential entry points for providers.

Finally, regulation also creates a cloud-related opportunity for providers. Highly regulated verticals are migrating to the cloud about four times more quickly than low-regulated verticals are. This could help unlock new markets, particularly in highly regulated Europe, and be a key differentiator for multinationals that must navigate complex cross-border data flows, local regulations and data sovereignty, and geopolitical issues that spike cyber and data risk.

**Create a pricing model for the midmarket**

Many cyber solutions are mispriced for SMBs. Larger organizations can pre-pay or buy in bulk to obtain volume discounts, but many SMBs and midmarket companies are less able to negotiate hard for these services. Large enterprises have an abundance of metrics, historical data, and reference points. SMBs and midmarkets, however, often lack information on how much they and others have spent. Consumption-based pricing models (for example, per gigabyte) can add flexibility but also risk: if an organization doesn't know what good security looks like, will it burn through its budget just looking for needles in haystacks? Instead, customers increasingly reward vendors that use outcome-based or more "plannable" pricing models, such as per workload.

One cause of the pricing mismatch is simple economies of scale. SMBs and midmarket companies have a smaller base of employees over which to spread cyber-tooling costs, so they face a decision: either pay a disproportionate price per employee—by a factor of three to five or more than larger companies do, depending on the tooling category—or forego some security controls entirely.

## Organizations that adopt multicloud strategies or maintain critical on-prem workloads will in all likelihood persistently need best-of-breed solutions.

**Better automation, AI, and machine learning**

The steepest innovation curve is for developing the brains of next-gen products and managed security services. Fully autonomous intelligent cyber-defense platforms (for example, end-to-end automated SIEM/SOAR[9] detection and response pipelines) are challenging to engineer and validate to the point where they are fully trusted by operators. Providers should therefore strive to enable high-fidelity assisted intelligence that makes human analysts more efficient be it through leveraging advanced analytics or building tight integrations with other security platforms (Exhibit 4).

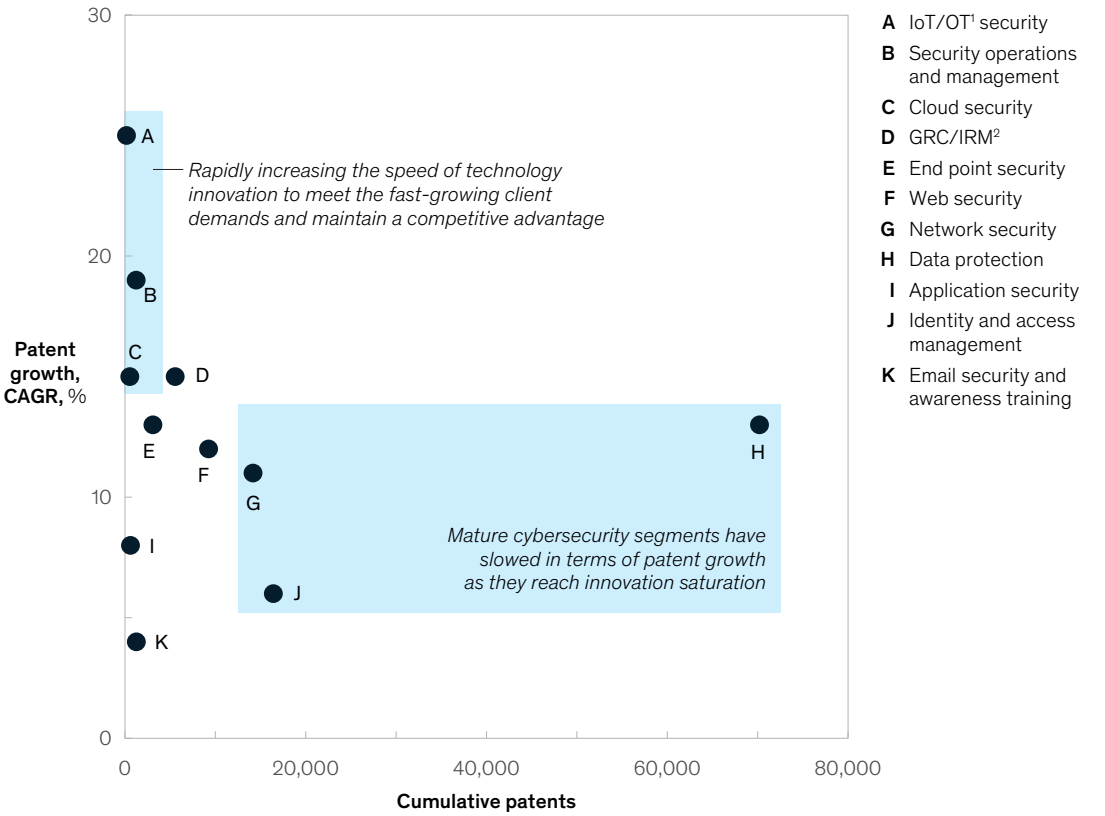
Many next-gen algorithms for AI and machine learning (ML), while not yet ready for autonomy, are getting close. Rule libraries are increasingly refreshed from open sources and built on common standards, such as Yara. Eventually, one human being, operating as a remote or virtual resource to serve multiple companies, will reduce the cost of MDR solutions and boost the margins of providers.

To reach this target state of optimized low-cost services, managed-service providers can focus on the brains of next-generation security products by concentrating innovation in areas such as data

Exhibit 4

## An expanding attack surface is driving innovation in cybersecurity.

**Cybersecurity patents by type, 2017–21**




[1]Internet of Things/operational technology.
[2]Governance, risk, and compliance/integrated risk management.
Source: Innography; McKinsey analysis

[9] Security orchestration, automation, and response (SOAR) and security, information, and event management (SIEM).

source integration and neural/logic engines. Enhancing and building data source integrations could yield indirect revenue opportunities and widen access to larger ecosystems—for example, as part of an open extended detection and response (XDR) concept. Spreading investment in neural/logic engines across both cutting-edge AI and static rules libraries will ensure that R&D efforts are measurably productive.

**Expand managed services and create a midmarket-friendly solution**

Demand for full-service offerings is set to rise by as much as 10 percent annually over the next three years. Providers should thus seek to develop bundled offerings that take advantage of hot-button use cases. And they ought to focus on outcomes, not technology.

A potentially rewarding approach would be to adopt co-creative models with managed-service providers (MSPs) to build workbench solutions. This would require investments in R&D and development tooling (for example, APIs) that allow MSPs to connect your platform to theirs rather than the other way around. Partnering will make it possible to create centers of excellence, which will lead to faster implementation and more efficient operations. The resulting improvement in customer outcomes will feed into the performance metrics of providers, and a more robust service layer will create a runway to master product market fit.

Rather than the common laundry list approach, vendors should adopt a clear MSP partnership strategy. Where necessary, they should invest in building collaborative sales capabilities with their partners. (In several cyber-partner programs, 20 percent of the partnerships generate 80 percent of the partners' revenues.) Finally, vendors must articulate industry-specific use cases with tweaks to their products' user interfaces and user experiences, as well as potential MSP and partner channel sales and marketing.

Winning companies will work with SMB-focused channel partners and optimize their marketing. That approach could involve partnerships with small-business software providers (such as tax prep software and cloud email and storage) and with vertical SaaS providers (such as payroll management and point-of-sales services). In some cases, it will make sense to replatform offerings as lighter-weight SaaS-first solutions, catering to buyers already deep in the trenches of SaaS transformations in other enterprise applications and platform realms.

---

The continuing digitization of the global economy, ever-increasing numbers of cyberattacks, and regulatory pressure on companies to protect their data present cybersecurity providers with a compelling opportunity. Amid talent deficits and the desire to boost log visibility, SMBs and midmarket players in particular are focused on implementing more advanced solutions.

With billions of dollars of revenues set to flow into the market in the next three years, providers should seize the moment. That means optimizing engagement with the cloud, developing a pricing model for the midmarket, embracing innovation, and expanding managed-service offerings to create midmarket-friendly solutions. In short, it means finding productive combinations of product, price, and services that vendors can tailor to target segments and are flexible enough to scale. If the industry can meet these priorities, it can start to create the momentum that will increase its penetration across segments and put the $2 trillion prize in play.

**Bharath Aiyer** is an associate partner in McKinsey's Southern California office; **Jeffrey Caso** is an associate partner in the Washington, DC, office; **Peter Russell** is a consultant in the New York office; and **Marc Sorel** is a partner in the Boston office.

The authors wish to thank Hannah Chen, Bartlomiej Kazimierski, and Kevin Telford for their contributions to this article.

Designed by McKinsey Global Publishing