McKinsey & Company

Risk & Resilience Practice

Securing small and medium-size enterprises: What's next?

Small and medium-size enterprises are becoming an increasingly attractive segment for cybersecurity-technology and -solution providers.

by Bharath Aiyer, Venky Anant, and Daniele Di Mattia

March 2021

Give cybercriminals this much: they are opportunistic. When the COVID-19 outbreak led to government-ordered shutdowns in early 2020, almost overnight thousands of organizations around the world became entirely remote. But while many businesses had some experience with mobility and flexible work-from-home arrangements, few were set up to operate 100 percent remotely. Opportunistic attackers predictably wasted little time targeting insecure home networks and household smart devices. The upshot: a fourfold surge in the number of attacks[1]—everything from credential theft and email phishing scams to social engineering brute force attacks against end points—as cybercriminals sought to exploit this historic transition to find security vulnerabilities that would allow them to burrow into corporate networks.

These mounting cybersecurity threats are particularly fraught for small and medium-size enterprises (SMEs), defined as those with fewer than 500 employees. Even before the pandemic, SMEs faced challenges when it came to limited budgets and hiring skilled personnel. Now, as the pandemic continues to take its toll on the broader economy, tighter budgets are expected to also affect cybersecurity spending by SMEs.

Still, SMEs remain a market category with global cybersecurity sales estimated at more than $40 billion, one that had been growing at more than 8 percent per annum until this year.[2] But despite its size, the market remains often underserved by cybersecurity providers. While this opens a window of opportunity for savvy cybersecurity-technology and -service providers, it requires them to reassess their SME strategy, applying more efficient direct remote-selling strategies and revising their channel strategy to capture growth in the managed security service provider (MSSP) segment. Lastly, they will need to revise their specific SME pricing and packaging to better appeal to this varied customer segment.

At first blush that sounds like a lot of heavy lifting, but it's worth the effort: the ultimate prize for success could be a significant business in a segment that will exceed $50 billion during the next five years.

State of the market

The cybersecurity needs of SMEs have been relatively underserved compared with the significantly larger enterprise segment. It's also been less profitable than the consumer segment. That's a missed opportunity hiding in the open as cybersecurity and the threat of future attacks weigh equally on SMEs.

But this is a market with a diversity of needs that present specific sales and marketing challenges to cybersecurity providers. We see three distinct segments within the SME segment, largely defined by the sophistication of their IT requirements and size of IT personnel (exhibit):

- *Limited maturity* (approximately $9 billion market with about 10 percent CAGR): this segment includes most small offices—fewer than ten full-time employees (FTEs), and some small enterprises (ten to 99 FTEs), operating in low-digitization industries (for example, healthcare, public sector) and with no IT resources.

- *Semimature* (approximately $17 billion market, approximately 10 percent CAGR): this segment includes most small businesses (ten to 99 FTEs) and some medium-size enterprises (100–499 FTEs), operating in low-digitization industries (for example, industrials, transportation, utilities, services) with nondedicated to very limited IT resources and nondedicated security resources.

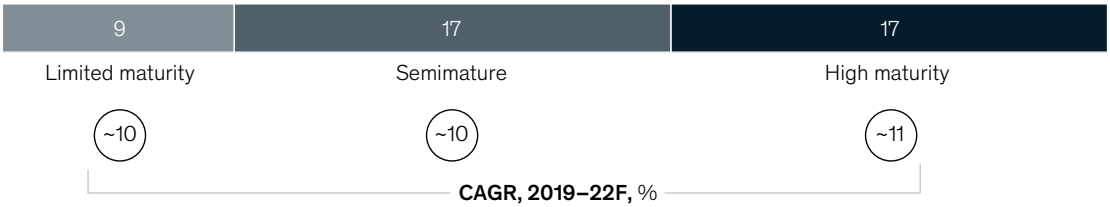
- *High maturity* (approximately $17 billion market, approximately 11 percent CAGR): this segment includes most medium-size enterprises (100–499 FTEs) and small enterprises (10–99 FTEs) in high-digitization industries (for example, financial services, high tech, telecoms and media, consumer and retail) with a small, dedicated IT department.

[1] "Fight back: How to stop cyber criminals during the pandemic," Aspen Institute, April 16, 2020, aspeninstitute.org.
[2] Gartner, International Data Corporation, and McKinsey research.

Exhibit

Small and medium-size enterprises fall into three segments of IT maturity, which will affect their cybersecurity needs.

Cybersecurity market for small and medium-size enterprises by IT maturity, 2019, $ billion



McKinsey research based on a survey of SME industry leaders reveals that different SME segments have distinct cyber needs.

— *Limited-maturity segment:* very similar to the consumer segment with approximately 90 percent cyber spend on end-point security for most companies. One in three companies with fewer than 50 FTEs is estimated to use free or consumer-grade products.[3]

— *Semimature segment:* with relatively basic product needs—usually a combination of end-point security and basic network security with potential add-ons (for example, messaging security)—these organizations are not as concerned with advanced features and prefer simple, affordable solutions.

— *High-maturity segment:* defined by more holistic security needs, these organizations tend to be close followers of enterprise trends, although with a lower willingness to pay and internal capabilities. Cyber products and services typically include more advanced security around end points, networks, messaging, and data.

Similarly, each segment takes a different approach when it comes to buying and managing cybersecurity technology and services.

— Approximately 70 to 80 percent of the limited-maturity segment is estimated to buy direct, online, or through big-box retailers. The rest rely on managed service providers (MSPs) to provide a full range of IT-managed services, including software and hardware resale and support and procured solutions, as part of the agreement.

— About half of the SMEs in the semimature segment use an MSP, with 30 to 40 percent using a value-added reseller (VAR). A smaller number, ranging between 10 and 20 percent, prefer to buy direct. MSPs in this segment sometimes outsource the security aspect to an MSSP in about 30 to 40 percent of cases, comprising 15 to 20 percent of the total segment.

— The mature segment tends to have higher in-house technical capabilities and thus has less reliance on MSPs. Security products are procured through MSSPs (40 to 50 percent), VARs (30 percent), and direct from vendors (20 to 30 percent). Those procuring direct typically are highly tech-savvy and possess significant in-house talent who can integrate products with an in-house security operations center (SOC).

— MSSPs are increasingly showing up in the mature segment and emerging as trusted third parties, given the need for integrating and selecting multiple point products across the cyber stack.

[3] "New study reveals one in three SMBs use free consumer cybersecurity and one in five uses no endpoint security at all," Response Source, February 19, 2020, responsesource.com.

The cybersecurity companies vying for ascendancy in the SME category have traditionally been enterprise point solution providers, but that might change with the emergence of opportunistic new entrants offering new approaches to cybersecurity technology and distribution.

Potential market shifts

It's rare to find cybersecurity vendors reaching beyond 30 to 40 percent market share in a product category. That fragmentation also applies to the SME category where no single vendor has a dominant position across all domains. Historically, the cybersecurity companies vying for ascendancy in this segment have traditionally been enterprise point solution providers or consumer players looking to expand their reach into what for them were new markets. In the future, that might change with the emergence of opportunistic new entrants offering new approaches to cybersecurity technology and distribution that SMEs find compelling.

On the product side, we might witness the rise of simpler, integrated, and modularized "security suites" and cloud-based platforms. Indeed, some vendors are already championing the concept of security suites more tailored for SMEs (for example, end-point detection and response/managed detection and response, next-generation firewall, cloud, email/phishing, mobile security). The idea is to reduce the complexity of implementation, deployment, and maintenance with components increasingly deployed on the cloud. There would be no on-site installation of a hardware appliance; instead, everything would be pre-integrated and managed through a central console.

On the channel side, we're already seeing a shift with MSSPs gaining steady share, both through direct contracts with SMEs and as MSPs increasingly partner with MSSPs to provide security-managed services.

In fact, the MSSP share of the SME market is estimated to grow 14 percent from $7 billion to $10 billion by 2022.[4] At the same time, VARs will be compelled to provide more managed services in order to expand their revenue and gross margins, a move that will further accelerate the growth of the managed security service sector.

Meanwhile, the growing channel trend toward direct, digital, and remote sales of software may expand to cybersecurity post-COVID-19. McKinsey research in the United States and Europe found that 30 percent of software buyers for SMEs had no field interaction across the customer-decision journey, especially for purchases smaller than $50,000. The same research found this percentage is expected to increase by over ten percentage points post-COVID-19 (April 2020 data).

[4] Gartner, International Data Corporation, and McKinsey research.

The research also found that software companies on aggregate get as much revenue from direct remote sales as from partner channels. While adoption of direct remote sales in cybersecurity has been lagging behind compared with the overall software industry—due to the higher complexity of security solutions versus other categories of software—the gap might close as security product sales shift from point solutions to packaged suites.

Implications and no regrets for all cyber vendors

Against the evolving landscape of cybersecurity providers and the needs of the SME segment, there might be ample opportunity to build an SME business at scale.

The proposition would likely resemble a simple and competitively priced "security-in-a-box" solution. This sort of modular product suite would bundle different products on a cloud-based platform targeted at the needs of the high-maturity customer segment.

The solution would be sold direct to businesses in certain geographies and customer segments, as well as to or through MSSP channel MSPs and VARs in others. Such business could be worth several hundred million dollars in revenue by 2025 if it captured a high-single-digit share of direct distribution in North America and Western Europe, and a low-single-digit share of the MSSP distribution globally.

In light of these shifts, there are three actions we believe cyber vendors should consider following:

— *Build an effective and efficient remote sale motion.* In our experience, leaders in remote selling increase demand generation by three- to fourfold if they use agile marketing practices to drive traffic and optimize online journeys, use effective machine-learning models for lead scoring/nurturing, and optimize their sales coverage and practices. Remote sales' best performers, for example, do twice as well as bottom-quartile performers. Clear roles and responsibilities are established across the funnel. Sales reps are equipped with the proper playbooks and tools to improve productivity and performance.

— *Rethink your channel program as partner business evolves.* Many vendors treat MSPs and MSSPs as if they were direct accounts or VARs. But successful vendors instead perform top-to-bottom reviews of their channel program to refocus and prioritize their resources. The goal is to wind up with fewer high-growth partners, design roles, and compensation models as they build specific enablement activities for prioritized partners. Channel program restructuring can significantly increase revenue growth—and result in doubling market share in specific territories.

— *Reconsider SME-specific pricing and packaging.* Enterprise customers have traditionally been—and will continue to be—best-of-breed buyers. SME customers, however, can be targeted with a "product bundle," a well-packaged suite that ideally offers a pre-integrated solution of products and services, competitively priced. That sort of offering will resonate with customers eager to reduce the clutter and complexity that often results from the need to integrate multiple products. Additionally, a larger ticket sale—selling a suite instead of a point solution—will make direct remote selling more economically attractive.

For cybersecurity-solution providers, the opportunity is out there. The customer challenges are clear. Although some players will continue to bring the same corporate products to the SME market, the ultimate winners will be those who address directly the specific needs of SMEs and evolve their products and distribution to do so.

Bharath Aiyer is an associate partner in McKinsey's San Francisco office, **Venky Anant** is a partner in the Silicon Valley office, and **Daniele Di Mattia** is an associate partner in the London office.

Designed by McKinsey Global Publishing