New SMB working patterns are leading to a shift in cyber-security spending and routes to market

August 2020

Eileen Zimbler

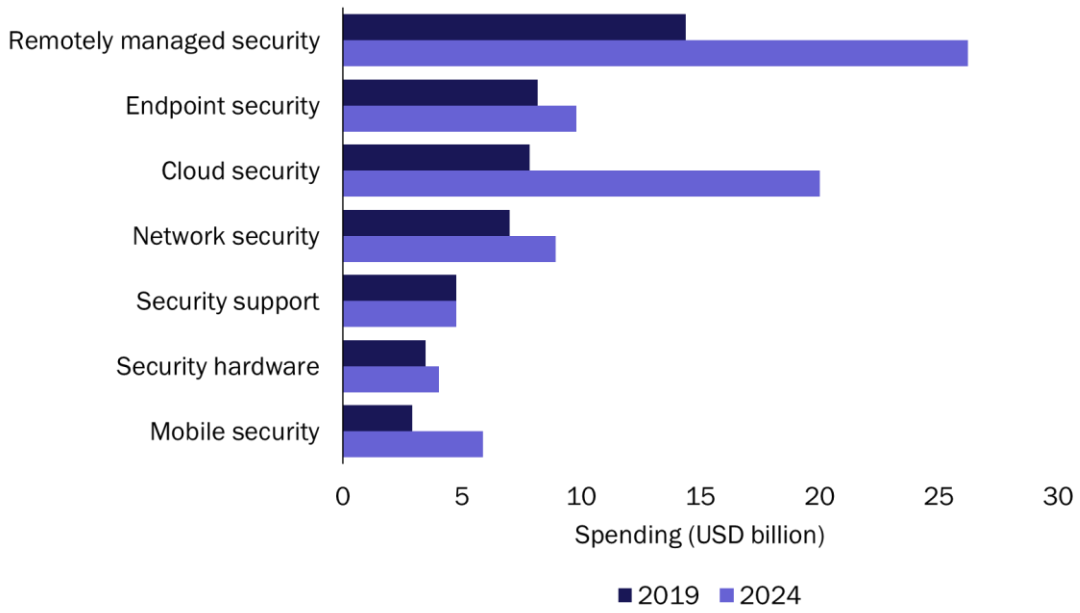
Small and medium-sized businesses (SMBs) have increased their spending on cyber security as a result of the new working patterns brought on by the COVID-19 pandemic. These new investments in security will help to offset the declines in spending caused by business failures and reduced levels of employment. Overall, increased security requirements mean that SMB spending on cyber security will continue to grow strongly, albeit at a slightly lower rate than anticipated before the crisis.

Analysys Mason's SMB Technology Forecaster predicts that the annual SMB spending on cyber security (including hardware, software and services) worldwide will grow by 10% year-on-year from 2019 onwards, and will reach almost USD80 billion by 2024.

SMB spending on cloud-based security solutions will outpace that on on-premises hardware and software

Analysys Mason's recent survey found that the majority of SMBs in the USA have changed the way in which they do business in response to COVID-19-related restrictions; the most significant change has been to expand their work-from-home programmes. This change in working habits has increased the demand for cyber-security solutions, especially for managed security services and cloud-based solutions, in order to secure SMBs' data and devices that are now located outside the office, thereby driving strong growth in cyber-security spending (Figure 1).

Figure 1: SMB cyber-security spending by solution type, worldwide, 2019 and 2024



Source: Analysys Mason, 2020

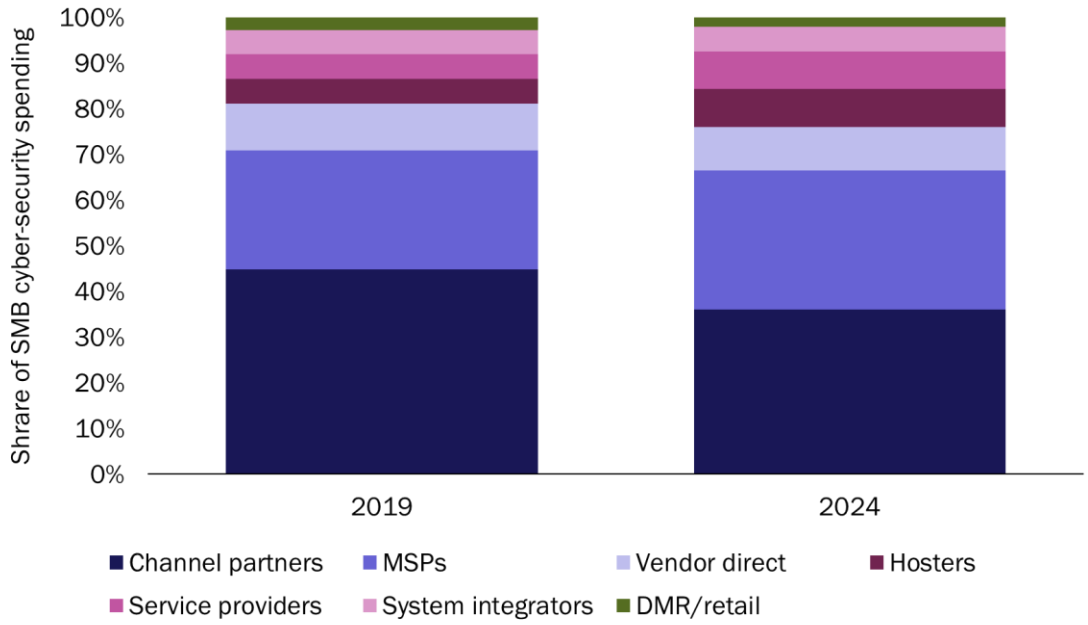
SMBs were already investing heavily in security-related solutions prior to the COVID-19 pandemic to help them to address growing concerns around protecting their customers' privacy and financial data and ensuring business process stability and continuity. Many SMBs are now reporting that they will be allocating even more of their IT budgets to cyber security. Indeed, almost a quarter of small businesses (SBs) and a third of medium-sized businesses (MBs) said that their spending on cyber security is likely to be even higher than they had originally planned after the initial restrictions on movement are relaxed. Significantly, less than 10% of the firms surveyed said that their future spending on cyber security would be lower than originally planned.

Analysys Mason's SMB Technology Forecaster predicts that much of this additional investment will be used for remotely managed security services and cloud-based solutions. Spending growth for remotely managed security services is projected to reach 13% per year between 2020 and 2024, and that on cloud-based security solutions, overall, is expected to grow at a CAGR of 15% over the same period.

An increasing share of the total spend will go to partners that are offering managed services

SMBs' purchase channels will change as they use more of their security budgets for managed security services and cloud-based solutions. The DMR/retail share of SMB cyber-security spending is expected to decrease significantly, while managed service providers (MSPs), hosters and service providers (SPs) will gain market share (Figure 2).

Figure 2: Share of SMB cyber-security spending by routes to market, worldwide, 2019 and 2024



Source: Analysys Mason, 2020

We asked SMBs about the type of support that they need to help them to navigate the new challenges caused by COVID-19 (for example, working from home, collaboration and BYOD). 30% of SBs and 51% of MBs cited offerings that could be used to upgrade their security as the most helpful.

Vendors and partners should offer cyber-security assessments as part of their sales processes. SMBs need guidance from vendors to sort out issues that are affecting their cyber security due to new work-from-home initiatives and employees' use of remote devices and potentially lax home-security protocols, which can carry additional risk to the network. Security assessments from vendors (such as Kaspersky's Security Assessment Services or Palo Alto Networks's Best Practice Assessment (BPA)) can help SMBs to evaluate the efficacy of their existing software, discover weaknesses and provide a roadmap for future cyber-security initiatives.

Security solutions vendors should emphasise scalability, as this will resonate with SMBs during this climate of uncertainty. Many SMBs have had to change the way in which they operate. 38% of the SMBs surveyed said that they have changed the way in which they deliver products and services to customers, and 64% reported having started or expanded their work-from-home programmes. These changes in business operations have added an additional layer of security risk to companies' financial and customer data, both in the short term and in the future. Being able to scale their security solutions up or down as needed will be critical to SMBs.

Service providers and channel partners should act as trusted advisers to help SMBs to achieve their cyber-security goals. SMBs were already struggling to craft and maintain cohesive and substantive cyber-security policies prior to the COVID-19 outbreak. Most SMBs lack adequate IT support to manage changing business demands and an increasingly remote workforce (as well as remote customers), and are seeking guidance from knowledgeable providers. Providing easy-to-follow guides and playbooks and personalised advice, in addition to installation support and onboarding/employee training, will be key to winning SMB business.