COVID-19-related remote working is driving growth in SMBs' use of and spending on cyber-security solutions

February 2021

Eileen Zimbler

Small and medium-sized businesses (SMBs) worldwide spent over USD57 billion on cyber-security solutions in 2020 and Analysys Mason forecasts that the SMB security spend will reach USD90 billion by 2025. This growth is being driven by SMBs' escalating dependence on cyber security to help to protect their customers' data, guarantee business stability, support digitalisation plans and protect the rising number of users on their corporate networks. All of these issues are becoming increasingly intensified and more difficult to manage as firms continue to struggle with the COVID-19 pandemic.

Businesses have experienced an increase in the number of data security attacks since the initial outbreak of COVID-19, and there has been a dramatic rise in the number of employees working from home. Many SMBs are reporting that at least some portion of their workforce will never return to a traditional office setting. This will make it challenging for IT departments to control who is using company PCs while they are in employees' homes, and what they are being used for. Analysys Mason recently conducted a survey of over 1800 SMBs regarding the impact that the COVID-19 pandemic has had on their business. Respondents expect that there will be a 54% increase in the proportion of staff that work from home post-crisis compared to the share that worked from home prior to the pandemic.[1]

Growth in security spending by small businesses will outpace that from other segments during 2020–2025

SMBs accounted for 52% of the USD110 billion spent on cyber-security solutions by businesses worldwide in 2020, and their share is expected to increase to 55% by 2025 (Figure 1). Analysys Mason estimates that the total spend on security-related solutions worldwide will reach USD165 billion by 2025, rising at a CAGR of 8.4% per year over the forecast period.

---

[1]   Analysys Mason's business survey on the impact of COVID-19 on SMBs worldwide in 1Q 2021, *n* = 1870.

Figure 1: Security spending by business segment, worldwide, 2020–2025
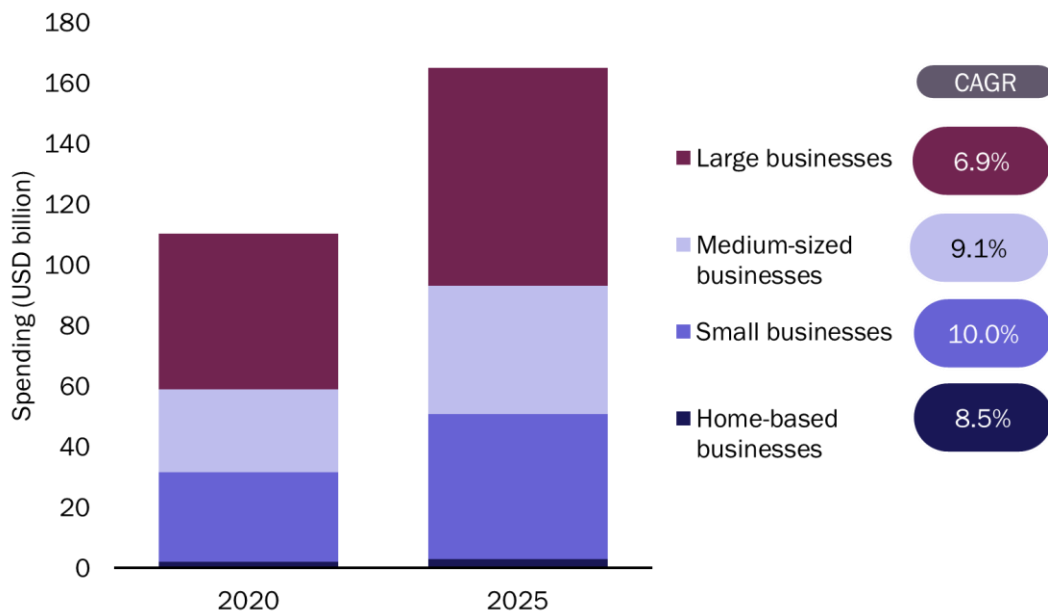
Source: Analysys Mason, 2021

Security spending by small businesses (SBs; 0–99 employees) is projected to grow more quickly than that of any other business segment, at a rate of 10% annually throughout the forecast period. Spending by medium-sized business (MBs; 100–999 employees) is expected to increase by 9.1% year-on-year during the same timeframe. Large enterprises (1000+ employees) currently account for almost half of the total security spending worldwide, but the growth of this spending will be the slowest (6.9% per year throughout the forecast period). SMBs' spending on cyber-security is growing more rapidly than that of large enterprises because many of them are adopting a range of security products for the first time, partly in response to the need to support increased levels of remote working. Large enterprises already have more established infrastructure and security solutions to support remote working.

SMBs' cyber-security investments are being heavily influenced by ever-increasing concerns about security breaches, particularly as firms contend with WFH issues and changing operational conditions due to extended COVID-19-related restrictions. About 46% of SMBs reported that they have either started using cyber-security solutions for the first time, or have increased their usage since the initial outbreak of COVID-19.[1] Over three quarters of SMBs surveyed plan to increase or maintain their current level of cyber-security usage. The majority (almost 8 out of 10) of SMBs we spoke to reported that they anticipate spending similar or greater amounts on cyber-security solutions in 2021 as they did in 2020.

SMBs' security spending with MSPs, SIs and telecoms operators will grow rapidly, but resellers and VARs will still remain important

Where SMBs buy cyber-security solutions from is heavily influenced by how much support they need to secure an increasingly remote workforce. We expect that an increasing number of businesses will look to outsource security due to their rising security needs and lack of in-house cyber-security resources. Indeed, 75% of SMBs surveyed reported that it would be helpful or very helpful if their IT/telecoms suppliers would upgrade their security solutions to cover new problems in the coming year (such as working from home, collaboration and

RESEARCH

analysys
mason

BYOD policies). SMBs' security spending with MSPs and systems integrators (SIs) is expected to grow by 13% per year over the forecast period, from USD20 billion in 2020 to USD37 billion in 2025 (Figure 2).

Figure 2: SMB security spending by route to market, worldwide, 2020–2025[2]
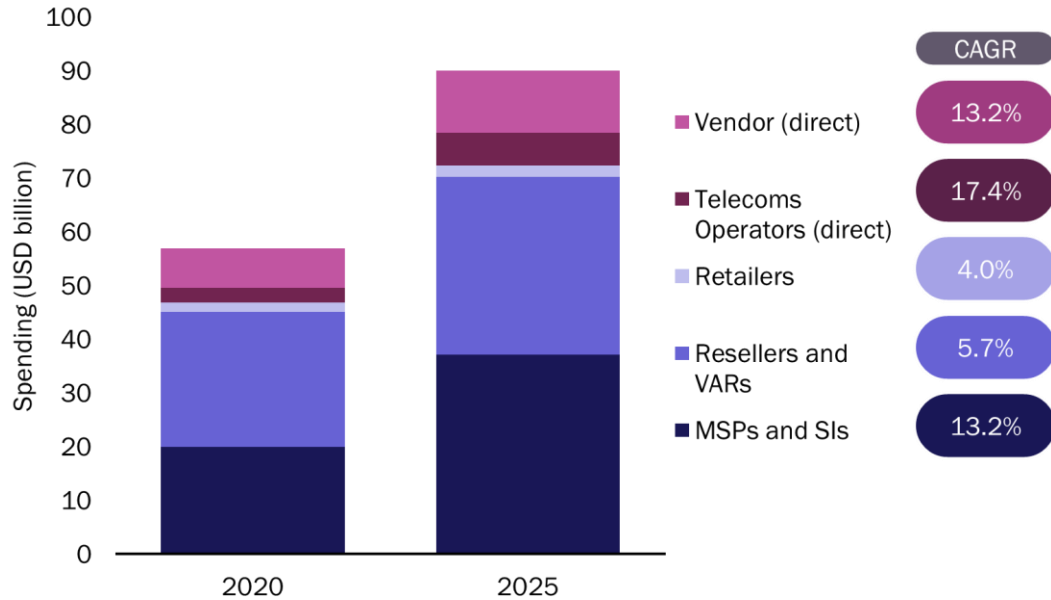
Source: Analysys Mason, 2021

Telecoms operators' direct sales represented just 5% of SMBs' spending on security in 2020, but this figure under-represents operators' role. A much larger share of security sales will come from telecoms operators' reseller partners (captured in our reseller and VARs category). The share of operators' direct sales will increase rapidly throughout the forecast period as they look to bundle security more closely with connectivity products. SMBs tend to rely on their telecoms providers as longstanding and trusted partners. Indeed, 44% of SMBs providing mobile connectivity for their employees reported that bundled mobile security is a very important aspect of their mobile service.[1]

Vendors should focus on the SMB segment and should support telecoms operators

Vendors should look to increase their focus on the SMB market relative to that on the large enterprise market. Spending in all segments will grow, but that in the SMB market will increase more quickly than that in the large enterprise segment. The move to working from home, accelerated by the pandemic, should encourage vendors to consider how well-suited their products are to this working environment. Security vendors need to offer remote installation for SMBs' employees that are currently working from home, as well as ongoing security training and support for these remote workers.

---

[2]   Note that the chart represents the channel that sells the service to the business. If a vendor sells a product through an MSP, the sale is captured under 'MSPs and SIs'. If a security product is supplied by a telecoms operator, but sold by a reseller, this sale is captured in the 'resellers and VARs' category.

analysys mason

Security vendors should consider how they can best support the telecoms operator channel. It is the fastest growing channel in terms of spending, but, as we have discussed before, telecoms operators are not always well-served by security vendors.

analysys
mason