Security providers should help SMBs to manage their existing products before selling them new solutions

January 2020

Tom Rebbeck

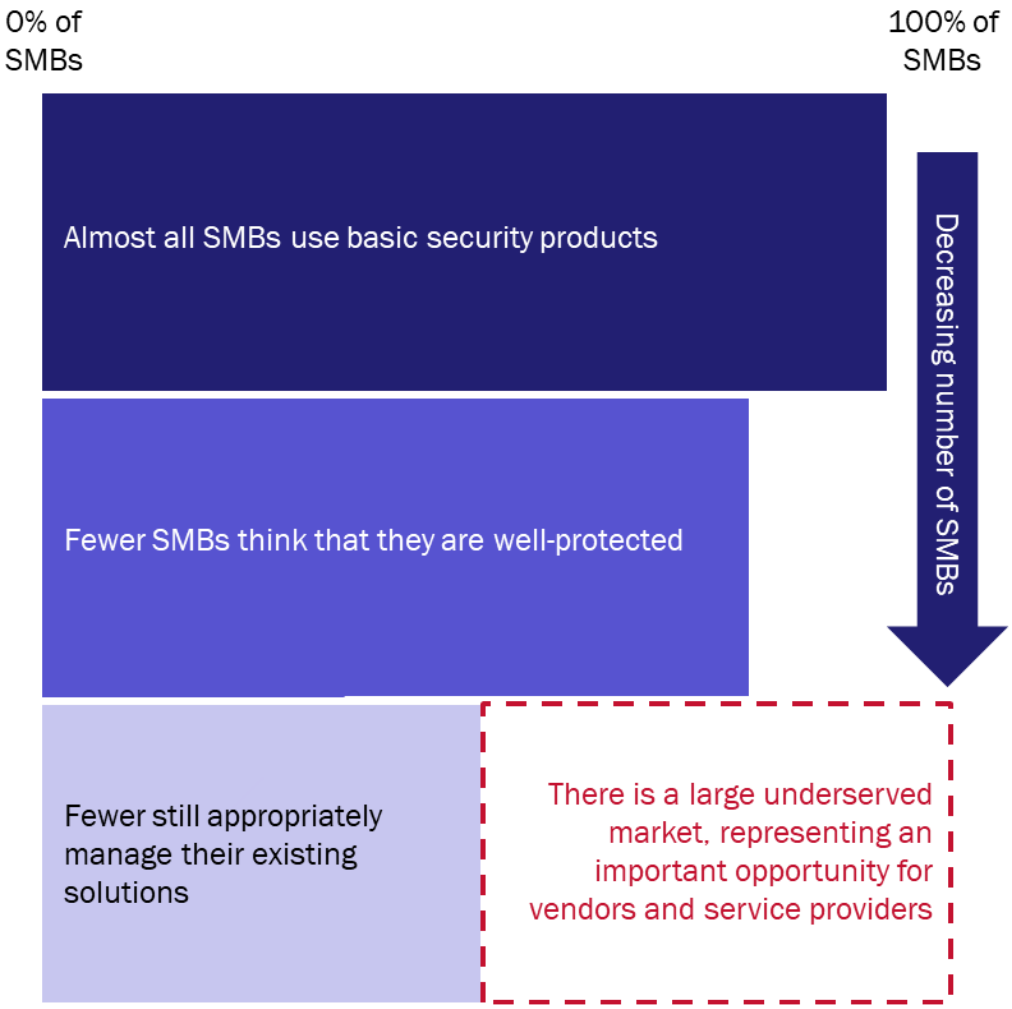
Businesses are increasingly appreciating the need for security, and most have at least basic security solutions in place to protect themselves (for example, anti-virus or email filtering). However, small and medium-sized businesses (SMBs) often struggle to find the right solution and to manage their security solutions when they are in place, even though they understand the need for security and are willing to pay for it. We estimate that only around 40% of SMBs both have suitable security solutions in place and keep these solutions up to date. This may create an opportunity for service providers; they can help clients by doing a better job of managing existing security products, and they should focus on this before trying to sell additional products.

We think that businesses are open to discussions on how their security can be improved. Many SMBs know that their existing set-up is inadequate (indeed, one in five small businesses characterised their security as such in our recent survey). They are also often aware of threats to their business and the risk that even a relatively small attack represents to their survival.

There is a difference between having basic security solutions in place and being secure

We asked a series of questions related to security in our recent survey of SMBs. We asked about security procedures and processes, as well as about which products were in place. A brief summary of the results can be seen in Figure 1.

Figure 1: Adoption of security solutions, procedures and processes by the SMBs in our survey



Source: Analysys Mason, 2020

The survey did not ask businesses explicitly whether they want to be protected against cyber threats, but it is reasonable to assume that all SMBs want to be well-protected. Most, but not all (97%) of the companies surveyed take the most basic of security products, anti-virus. Persuading the remaining 3% to do so may be challenging, but this figure represents a non-negligible number of businesses globally.

The adoption of security solutions gradually declines as cost and complexity increase; 87% of the SMBs in our survey have an email solution, 47% have a firewall and 18% have purchased SIEM. As with anti-virus, there will be some mileage in increasing these percentages and pushing penetration, but this is likely to be a challenging prospect, especially in high-income countries where the penetration is already high (that is, the market for businesses that need a firewall but do not have one is likely to be relatively small). Also, almost by definition, the more-advanced and complex solutions will only be required by a smaller subset of organisations.

More surprising than the adoption figures were the results on procedures and processes. At a high level these do not seem to signify problems; for example, 84% of the SMBs surveyed claim to have formal procedures in place for managing security and 80% think that they are well protected against threats. Based on this, we could conclude that four out of five SMBs have an adequate cyber-security strategy in place and that the opportunity for security vendors to grow their revenue from the SMB space is fairly limited.

However, examining the detail of the survey results shows that only around 43% of the SMBs surveyed update their security-related software and services frequently, that less than 40% of them conduct cyber-security assessments regularly, and that less than a third of them have documented procedures in place to act quickly in the case of a security breach. Put simply, around 60% of the SMBs surveyed pay for security solutions but do not use them properly.

This gap – the 60% of SMBs that have solutions but do not maintain them appropriately – is the key to the opportunity that service providers need to exploit.

Service providers can help their customers to get better value for money for security

Service providers and vendors should consider the following points in order to benefit from this gap.

- There is an opportunity to help SMBs to make better use of what they are paying for, for example, by ensuring that security solutions are up to date and by conducting regular security assessments. Service providers will need to demonstrate why an organisation's current procedures and processes do not suffice, and how they can be improved. Some internal IT managers may be open to these messages but others may be more resistant, especially if they feel that there is an implied criticism of their current efforts. It may be better for service providers to lead with the message that they can improve the effectiveness of the existing products rather than the more obvious push to sell additional products.

- Clear differentiators around ease of use and simple functionality are likely to resonate in this market. There is no point in having the best (or cheapest) solution if it cannot easily be kept up to date and leaves the business vulnerable.

- Linking different parts of a managed services sale is a powerful proposition. Security is not just about providing a solution that is separate from other aspects of IT. A managed services offer that takes care of basic networking equipment (for example, managing server updates) and provides connectivity and security solutions (such as firewalls) is much more compelling than separate solutions.

Our survey results show that there is an appetite among SMBs to improve their security and have better information from vendors on what solutions are on offer. Service providers have the scale and expertise to manage solutions more effectively and efficiently on an SMB's behalf, and this may be a powerful sales message. Vendors need to make sure that their products are easy to use and keep up to date, and should provide better guidance on how to use their products more effectively.