Mobile security vendors can maximise their revenue by improving offerings and partnerships to target SMBs

March 2023

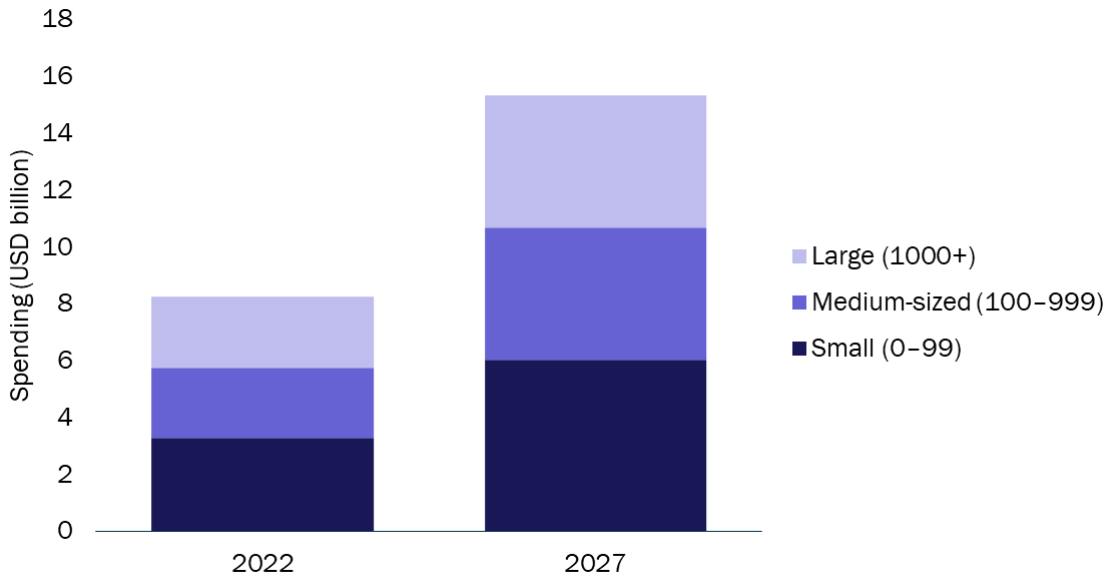
Jiachen Zhang and Lucy Brooker

Effective mobile cyber security is a top priority for small and medium-sized businesses (SMBs). The shift to hybrid working has increased the number of mobile devices that perform important business tasks and access sensitive business assets that SMBs are keen to secure.

SMBs' spending on mobile security is expected to increase at a CAGR of 13% from 2022–2027

Analysys Mason's SMB Technology Forecaster shows that SMBs' spending on mobile security worldwide will increase rapidly between 2022 and 2027. SMBs' total spending on mobile security is expected to almost double from USD5.7 billion to USD10.7 billion worldwide in the 5-year forecast period. We predict that SMBs will continue to account for most of the spending in the mobile security market, approximately 69% of the total market between 2022 and 2027.

Figure 1: Spending on mobile security solutions and services by business size (number of employees), worldwide, 2022 and 2027



Source: Analysys Mason

SMBs' spending on mobile security solutions is driven by the following factors.

- **The increasing demand for mobile security by SMBs.** Business decision makers are more concerned about cyber threats than ever. According to our recent survey, around 30% of SMBs are planning to

upgrade or start using mobile threat defence and mobile device management solutions in the next 12 months.

- **The increasing number of security treats on mobile devices.** SMBs are becoming more vulnerable as more mobile devices are signing on to business networks and accessing sensitive data. For example, Lookout's Global State of Mobile Phishing report showed that 21.45% of enterprise and 53.07% of personal mobile devices had encountered phishing attacks in 2022.

- **The growing number of 'bring-your-own' devices.** As employees increasingly use their personally owned devices for work purposes, it is becoming essential to enforce security procedures and policies consistently.

- **Insufficient awareness about security among employees.** Employees may be connecting to public Wi-Fi, clicking on unverified links or downloading unsecure content/apps.

- **Complexity with mobile device management:** A consistent security strategy is challenging to implement give the wide range of apps and devices that are available.

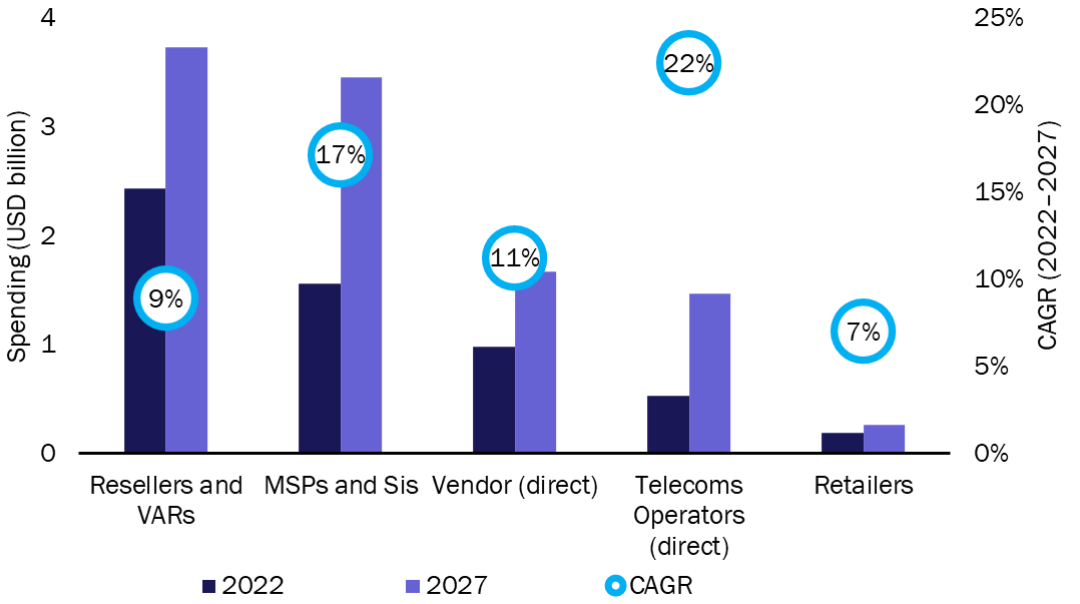
Vendors need to address the mobile security-related challenges that SMBs face

Vendors need to provide specific support to SMBs to attract their business. Many SMBs are yet to see the importance of adding mobile security to their IT budgets. They also lack expertise in mobile security or the ability to hire specialist security employees. SMBs are still learning about user behaviour and mobile device security and are seeking security-related support from their IT, telecoms or technology suppliers operators. Vendors should offer advice and support so that SMBs can implement and maintain comprehensive mobile security measures.

SMBs also want to purchase mobile security solutions through their preferred channels. MSPs and telecoms operators are expecting strong demand from SMBs for IT solutions in 2023 and this will be particularly the case for cyber-security applications.

Resellers and value-added resellers (VARs) accounted for the largest share of SMBs' spending on mobile security in 2022, but we predict their growth to slow down (Figure 2). The highest rate of growth for SMBs' spending will be among telecoms operators and managed service providers (MSPs); spending through these channels is expected to grow at CAGRs of 22% and 17% respectively, between 2022 and 2027.

Figure 2: SMBs' spending on cloud-based mobile security solutions by channel, worldwide, 2022 and 2027



Source: Analysys Mason

Mobile security vendors need to focus their offerings and build partnership opportunities to capture SMBs' increasing spending

Vendors should improve their understanding of how MSPs and operators sell to SMBs, tailoring their channel partner programmes to the needs of operators and vendors. Solutions should be easy to use and manage, enabling flexible integration with other security solutions that SMBs already use.

Security vendors should drive increased collaboration across the ecosystem while improving their SMB offerings as follows.

- Vendors should build partnerships with other vendors to offer integrated, complete security solutions. For example, Check Point Software Technologies and Samsung Electronics (Samsung Knox MSP) partnered for the first time in February 2023 to create an integrated mobile security solution that protects organisations from mobile cyber attacks.

- Vendors should do more to educate SMBs on the risks that mobile devices may bring to their businesses and the importance of securing the devices. One way would be to implement joint initiatives with operators and MSPs to increase SMBs' awareness of the need to include mobile device security solutions as part of a robust IT security strategy.

- Vendors could simplify their solutions for ease of implementation, integration and management. They could work with operators and integrate their offerings with operators' existing products and services, offering bundled security solutions, and providing them with more flexible pricing plans. Vendors could also offer free trials, discounts and partner incentives to increase brand recognition and capture market share.

- Vendors should continue to provide affordable, flexibly-priced and scalable security solutions that will suit SMBs' needs and budgets. Training and ongoing support are also essential. Vendors can help SMBs to stay up to date with the latest mobile security threats and vulnerabilities by providing regular updates and alerts.

Mobile security vendors will need to do more to provide specific support in their offerings and partnership strategies to better target the SMB market and benefit from the increased spending on mobile security.