Security-as-a-service solutions offer operators the chance to boost enterprise revenue

May 2017

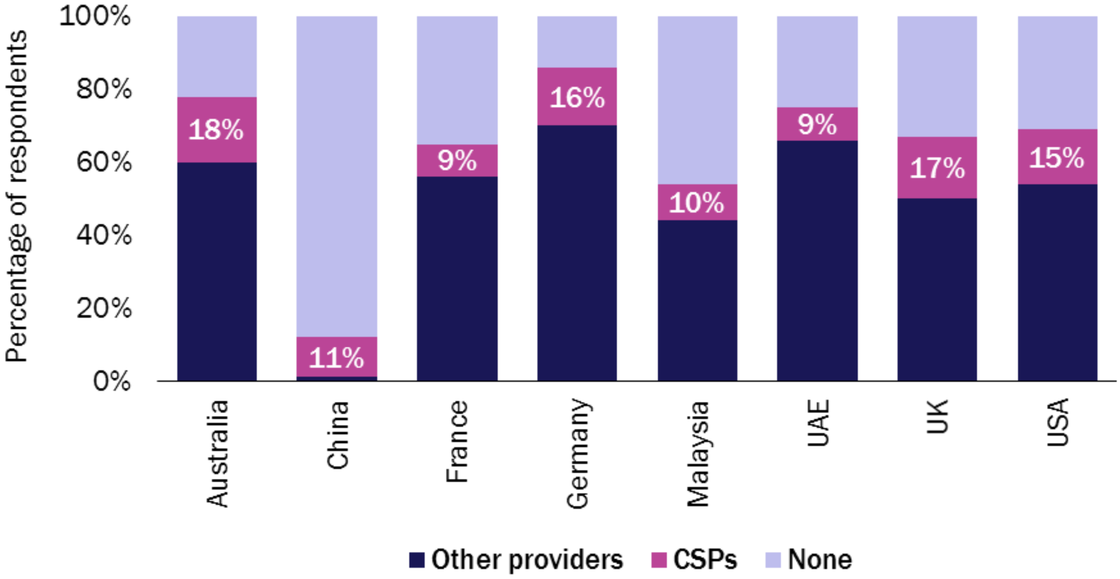
Patrick Donegan

Deutsche Telekom and M1 (Singapore) are among the first telecoms operators to launch security-as-a-service (SECaaS) solutions for small and medium-sized enterprises (SMEs). Operators have clear incentives for offering such applications, including increased revenue. However, operators must ensure that SMEs understand the risks of **not** buying security solutions, keep costs down and offer applications that are easy to use. This article is based on our recently published report, *Cyber security services for small and medium-sized enterprises: opportunities for CSPs*, and explores how operators should approach this opportunity.

Demand for cyber security is growing at a time when operators need new sources of enterprise revenue

Operators have a clear rationale for investing in SECaaS – operators are seeking new sources of revenue and demand for security solutions is growing. Enterprise revenue is flat or declining for most telecoms operators in high-income countries. SMEs are increasingly threatened by cyber crime and many have underinvested in protecting themselves. The market for cyber-security services for SMEs is expected to grow, but operators are only taking a small share of this market in most countries (see Figure 1).

Figure 1: Enterprise adoption of cyber security solutions by country and provider[1]



Source: Analysys Mason

[1] Results based on Analysys Mason's survey of 1600 enterprises.

Operators bring important assets to the SECaaS market

Operators bring two critical attributes to the SECaaS market. Firstly, and perhaps most importantly, they have existing customers of connectivity services. Secondly, the operators have scale; scale with which to negotiate attractive pricing from security technology vendors and the scale with which to generate a decent RoI by selling SECaaS sales to large numbers of customers.

However, operators face risks as well as opportunities in this market. SECaaS solutions for SMEs are highly replicable, and there should be little or no need for customisation. In contrast, security services for large enterprises often need to be highly customised, which can require specialist resources and drain margins.

Serving SMEs comes with margin risk. Most large enterprises have IT and cyber security professionals to implement and operate security solutions, but SMEs do not. This can result in SMEs calling customer support for assistance in understanding and optimising their solution. It can be challenging for operators to manage margins for security services for which operators can only charge a couple of euros or dollars per user. To counter this problem, telecoms operators must develop SECaaS solutions that are easy for SMEs to use. Any on-site configuration needs to be automatic; manual configuration can be an option but not a requirement. The user interface also needs to be simple to use, for example via a self-service portal. Telecoms operators that are faced with a trade-off between large gains in ease of use or minor gains in the level of security provided, must prioritise ease of use for customers.

Operators can help build demand among SMEs for security solutions

Operators need to lead in communicating the specific threats that SMEs face. Media reporting of cyber crime inevitably focuses on the impacts on large organisations or high-profile individuals. SMEs can think they are not likely to be targeted, or that the consequences of any attack will be limited. SMEs also lack awareness of the specific legal obligations on them to protect third-party data arising from forthcoming data protection regulations such as the General Data Protection Regulation (GDPR) in the EU.

A compelling SECaaS offering must also leverage the potential of virtualised infrastructure solutions. The cost of proprietary vendor hardware has traditionally been a barrier to investing in SME security for both operators and SMEs. Traditional security solutions required SMEs to make sizeable, often prohibitive, upfront investments in dedicated on-premises hardware. In addition, staff training, and the on-site operation and maintenance of the proprietary hardware had opex associated with them. Until recently, an operator looking to invest in a SECaaS proposition found itself similarly constrained. The model often implied a sizeable initial capex investment in the hope of generating enough sales to generate an acceptable RoI. The transformation towards software-controlled networking provides a platform for a more flexible pay-as-you-grow cost model for the operator, the benefits of which can then be extended in part or in full to the SME customer.

A rich portfolio of SECaaS services is key to success for operators

Security priorities vary considerably from one SME to the next. To truly scale, operators need a portfolio that is broad enough to cater for both basic and advanced SME security requirements. Some larger SMEs might want the kinds of 24/7 monitoring from a security operations centre (SOC) that are usually associated with large corporates.

In order to position themselves as protecting the SME before, during and after an attack, telecoms operators should consider reselling value-added services such as cyber security insurance or executive training in leading recovery from the impact of a major cyber attack.

Operators that want to target SMEs need to be open to leveraging new channels to market. Operators are used to working with private sector-run business organisations and confederations, institutes and the like, to reach their large and small business members, including their IT and communications directors. Operators also need to be open to partnering municipal authorities that are investing in cyber-security services for small businesses such as the Mayor of London's London Digital Security Centre (LDSC) in the UK.