# Mid-market security: operators should try to do more than simply sell security services to existing customers

*February 2020*

**Tom Rebbeck**

Most operators want to increase their business revenue, and security is an obvious area of focus. Indeed, cross-selling security solutions to existing connectivity customers is a common strategy. Pursuing such a strategy will provide a small incremental revenue uplift and help to defend the core business, but it will not be transformative. Operators may need to consider more aggressive strategies such as those being pursued by other operators, both big (such as AT&T and Orange) and small (such as Claranet and Exponential-e).

This article is based on a recent report that profiles the activities of 12 operators that are selling security solutions to the mid-market.[1]

## The mid-market is an attractive space for operators

The mid-market is good for telecoms operators that want to sell security products for several reasons.

- It is a large market that is growing quickly. The overall mid-market spend on security is expected to almost double between 2019 and 2024 from a base of USD10 billion.
- Operators are well-placed to access this spend because most already have direct relationships with hundreds if not thousands of mid-market companies.
- Mid-market companies often need managed services because few have internal security expertise.
- Mid-market companies have expressed a willingness to turn to operators for security expertise.
- The security requirements of these companies are complex, meaning that their spend is large, but not too complex, meaning that operators do not need a large portfolio or security team to serve them.

Moving into security is also a defensive measure for operators. In time, most companies in the mid-market will adopt SD-WAN: a product with strong security elements. SD-WAN also integrates well with other security products such as firewalls, cloud security solutions (for example, Zscaler) and web gateways. Operators' competitors are already providing SD-WAN with additional security components and are reducing operators to being simply internet access suppliers. Operators may need to offer security products to defend their connectivity position.

1 We define the mid-market as the market formed of companies with roughly 250–1000 employees.

# Operators are taking three broad approaches to mid-market security

Operators' approaches to the mid-market security opportunity can be placed into three broad categories (Figure 1). These range from cross-selling security to connectivity customers ('connectivity-first') to leading with security and having connectivity as the add-on ('security-first').

The middle category, with a balanced approach between connectivity and security, is interesting and is gaining attention. Operators in this category have separate security divisions and are selling security solutions to existing customers, but are also chasing new, non-connectivity customers, often in countries where the operator has little or no network presence.

***Figure 1: Operators' approaches to selling security solutions to mid-market companies***

| | Connectivity-first | Combined | Security-first |
|---|---|---|---|
| **Description** | Operators offer a limited set of security products that are closely linked to the core connectivity offer (e.g. firewalls, anti-DDoS).<br>Target customers are mostly existing connectivity customers. | Operators build out a broad set of security products. Sales are mostly to existing connectivity customers, but there is a growing focus on selling products independently from connectivity. | Operators develop a highly sophisticated security offering with which they lead. Connectivity is added on later. |
| **Examples** | Most large European operators (BT, KPN and Telia). | Larger global operators (AT&T, Orange and Telefónica) and B2B specialists (Exponential-e). | Specialists (Claranet) and operators with a limited business base (Zain). |
| **Advantages of this approach** | • Relatively simple products requiring limited investment<br>• Strong fit with existing products, sales and brand | • Increased revenue opportunity<br>• Meets most/all security needs of customers | • Independent of the connectivity offering<br>• Can have clear differentiators |
| **Disadvantages of this approach** | • Limited revenue opportunity<br>• Limited differentiation<br>• Customers still rely on other security providers | • Complex to build, sell and support<br>• Brand not associated with security<br>• Internal collaboration can be challenging<br>• Professional services elements can be low-margin | • Requires significant investment<br>• Complex to build, manage and sell advanced security products |

Source: Analysys Mason, 2020

# Operators need to consider how to go beyond simple cross-selling

An operator's security strategy will largely be driven by its existing internal capabilities. Operators will be limited to gradually adding products to their portfolios unless big acquisitions are made. This approach may appeal to customers: connectivity customers may be more comfortable letting their operator prove itself with simpler, network-related products initially. SD-WAN provides a convenient platform upon which managed security products can be added.

However, many operators will want to offer more products to a wider set of customers in the longer term. This will allow them to capture a greater security spend and to defend their connectivity revenue. Vying directly against pure-play security service providers should also force operators to make their offers more competitive rather than relying solely on cross-selling opportunities, and this should help all of their security customers.

The move to becoming a more advanced security provider may lead to organisational problems for operators. The trend is for operators to have a separate security division with its own management and (often aggressive) targets. AT&T, Orange and, most recently, Telefónica have implemented this structure. The arguments behind having a separate division are strong: security is a very different from connectivity in terms of sales and support processes, cultures and employee pay scales.

These separate divisions are being set up just as the boundaries between connectivity and security are blurring. Furthermore, the main opportunity in security for telecoms operators (especially incumbents) comes from cross-selling to existing connectivity customers. Having a separate security division is probably necessary for operators with large ambitions for security, but they will need to have strong links back to the connectivity business to make the most of the opportunity.

## A longer-term vision should help operators to shape their short-term strategies

Operators are well-placed to address the large and growing mid-market security opportunity. The first step (that is, gradually adding more services) is obvious and is already being taken by many. However, most operators should develop a longer-term vision for security with the aim of creating a standalone division that is not restricted to selling to existing connectivity customers. A clear longer-term strategy should also help operators as they make their initial steps.