RESEARCH STRATEGY REPORT

CYBER-SECURITY SERVICES FOR SMALL AND MEDIUM-SIZED ENTERPRISES: OPPORTUNITIES FOR CSPs

PATRICK DONEGAN and TOM REBBECK

analysysmason.com

analysys mason

About this report

This report analyses the opportunity for communications service providers (CSPs) to sell security-as-a-service (SECaaS) solutions to small and medium-sized enterprises (SMEs).

The SECaaS model provides CSPs with an opportunity to:

- boost declining revenue from the enterprise sector
- reduce churn
- enhance their brand.

The report provides recommendations for CSPs, and outlines a framework that will help network security vendors to understand the SECaaS market for SMEs from a CSP perspective.[1] It also:

- details the elements of a CSP SECaaS proposition for SMEs
- includes case studies of network security offerings from two operators, Deutsche Telekom and M1 (Singapore)
- lists key vendors of network security solutions for SMEs.

It is based on:

- Analysys Mason's research on SECaaS
- a series of interviews and discussions with stakeholders in the SECaaS market, including CSPs and vendors.

[1] Network (or cyber) security consists of the steps necessary in hardware and software, as well as in human behaviour and processes, to ensure the confidentiality, integrity and availability of infrastructure and the applications and services that run over it.

KEY QUESTIONS ANSWERED IN THIS REPORT

- What role do CSPs play in the SME security market, and how can they use SECaaS to increase their share in that market?
- What are the main opportunities and risks?
- How can CSPs leverage their established capabilities to build a SECaaS value proposition?
- What are the key components of a successful CSP strategy in the SECaaS market for SMEs?

WHO SHOULD READ THIS REPORT

- SECaaS and managed security service provider (MSSP) groups within CSPs.
- Strategy teams and senior executives within CSPs and vendors that are defining their organisations' roles in the cyber security space.

© Analysys Mason Limited 2017

CONTENTS

EXECUTIVE SUMMARY

OPPORTUNITIES AND RISKS FOR CSPs

PORTFOLIO DESIGN

DRIVING DEMAND AND NEW CHANNELS TO MARKET

APPENDIX: DEUTSCHE TELEKOM AND M1

ABOUT THE AUTHORS AND ANALYSYS MASON

analysys mason

Executive summary

Cyber threats are an increasing risk to SMEs without adequate network security. Operators can increase revenue, reduce churn and enhance their brand by targeting this customer segment with security services.

SMEs have compelling reasons to invest in cyber security and to outsource it as a service. Evidence shows that security concerns are the greatest barrier to SMEs investing in the cloud.[1]

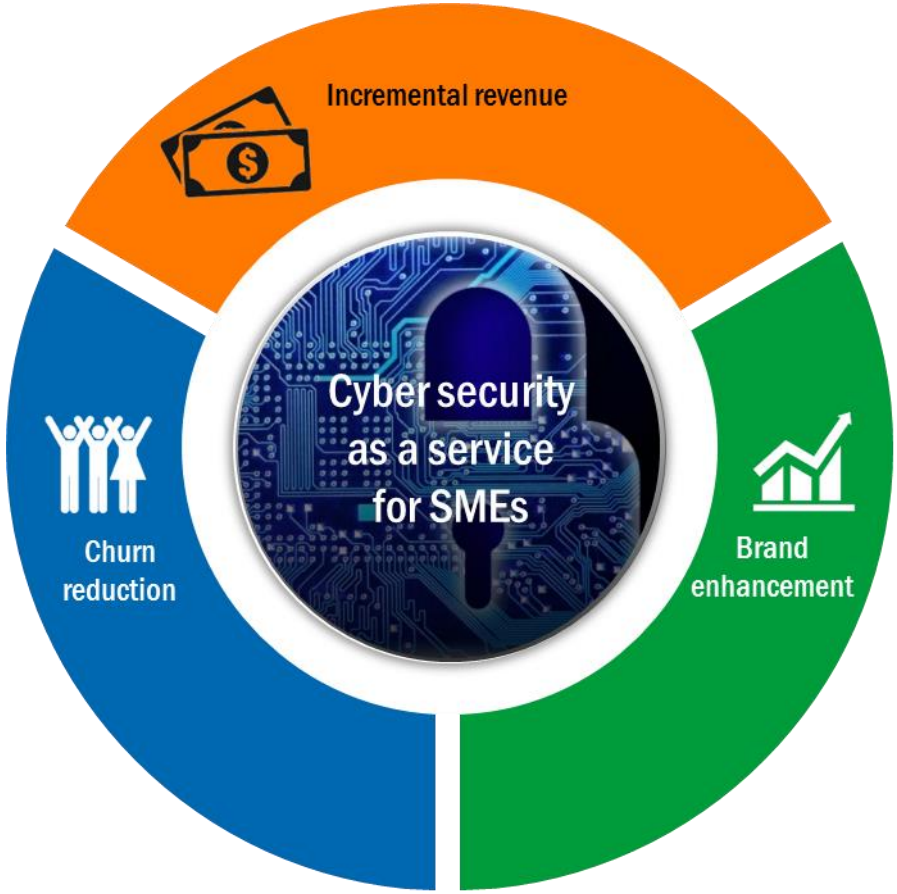
Operators are in a strong position to offer security services to SMEs because they have the scale with which to buy best-of-breed security solutions at competitive cost, bundle them in a comprehensive security portfolio, and combine them with connectivity in the cloud or on the SME customer premises.

Selling security to SMEs is not straightforward. Many will not buy services they do not understand. Cloud-based security vendors, Internet companies and a myriad of mostly small managed service providers (MSPs) are also key players in this space.

We recommend that operators:

- take the lead in communicating cyber security risk to SMEs
- design security services that are easy for SMEs to use
- use scale, trust, bundling and value-added services to differentiate themselves.

Figure 1: Supplying cyber security-related services to the SME market will have three main benefits for CSPs



Source: Analysys Mason

[1] For example, see www.cybersecurity-insiders.com/portfolio/download-cloud-security-report.

SECaaS for SMEs is an opportunity for CSPs to arrest the decline in revenue from enterprise services

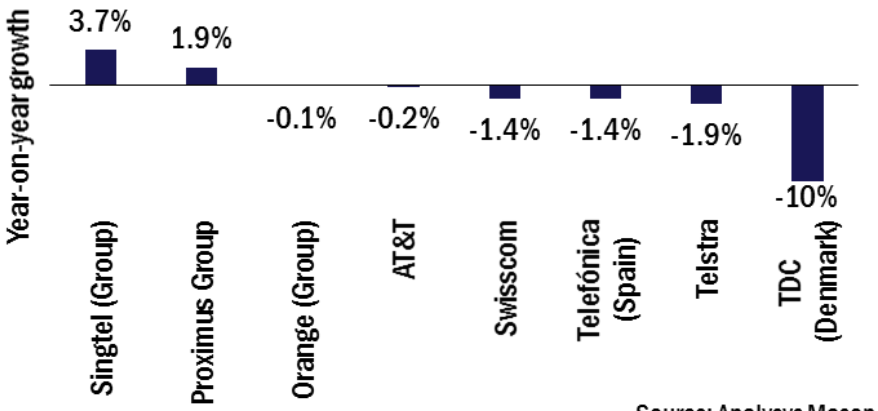
The enterprise revenue of CSPs is declining, but SECaaS represents an obvious opportunity for CSPs to fill that revenue gap.

CSPs' enterprise revenue generally declined between 2015 and 2016 (see Figure 2).

Analysis of enterprise and ICT revenue of several large operators suggests that strong ICT sales is linked to relative success in arresting – or even reversing – declining enterprise revenue.[1] Operators with robust ICT portfolios report the strongest overall enterprise revenue – AT&T, Orange, Singtel and Swisscom all performed better than the average.[2]

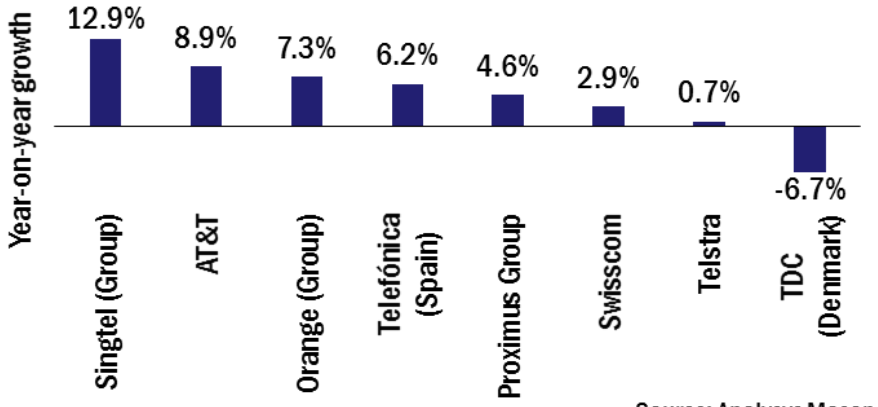
SECaaS solutions for SMEs are an almost entirely new revenue opportunity for most CSPs. If CSPs can execute on it well, selling SECaaS to SMEs could help to fill the revenue gap.

Figure 2: Change in enterprise revenue, selected operators, 2015–2016



Source: Analysys Mason

Figure 3: Change in ICT revenue, selected operators, 2015–2016



Source: Analysys Mason

[1] Definitions of enterprise and ICT revenue vary by operator, but ICT revenue usually includes new areas such as cloud and security service, and excludes traditional connectivity revenue.

[2] For more information, see *Singtel outperforms a declining telecoms enterprise market*. Available at www.analysysmason.com/Singtel-enterprise-market-Apr2017.

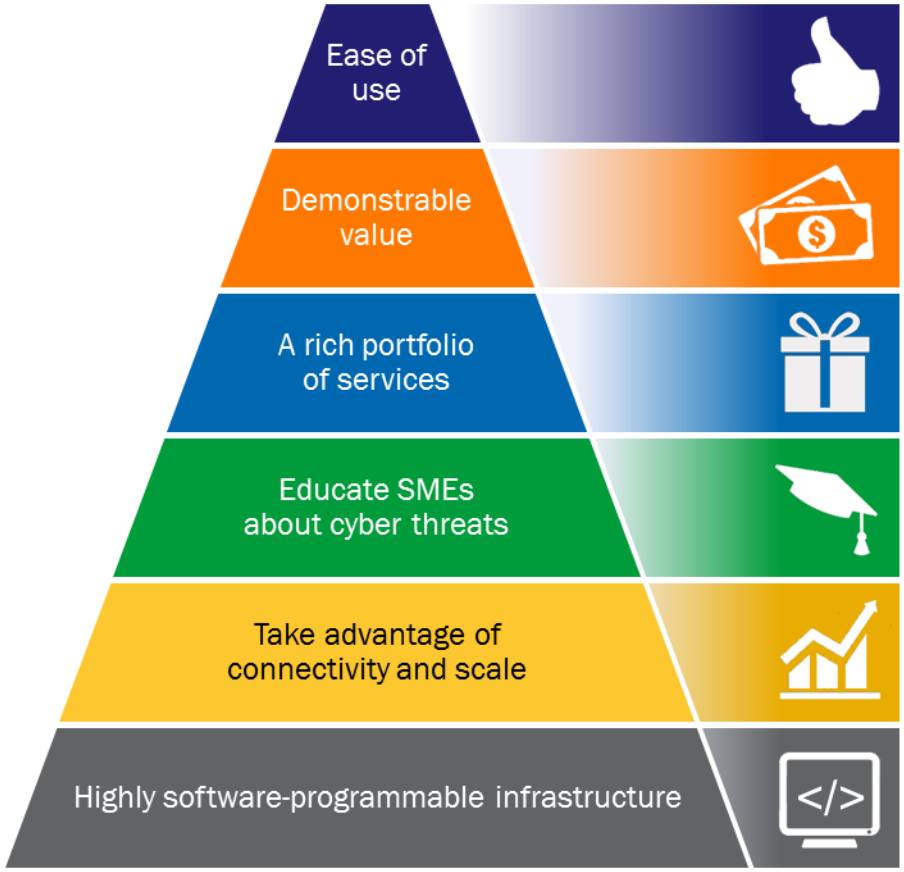
© Analysys Mason Limited 2017

We suggest that operators use six basic principles to frame their approach to SECaaS for SMEs

CSPs should leverage their inherent advantages of scale and connectivity footprint when developing a SECaaS strategy for SMEs, but should augment the strategy with capabilities built around six key principles.

- **Ease of use.** If security solutions are difficult to use, SMEs will either not buy them, or will make lots of customer care calls that will deplete margins.
- Many SMEs need to see **demonstrable value** – not theoretical value – before purchasing. A free customer trial that illustrates the unique threats to which they are subject is the best way to drive willingness to pay.
- SECaaS value propositions need a **rich portfolio of services** beginning with a firewall and evolving towards IDS/IPS, DDoS protection, malware detection and other services, including cyber insurance for when attacks get through.
- CSPs need to lead in providing **customer education** on the unique ways in which cyber threats put SMEs at risk. CSPs should actively support cyber awareness programmes run by national, regional and local government as a new, and potentially important, channel to market.
- A **highly software-controlled infrastructure** platform is critical for delivering SECaaS to SMEs. This should enable faster instantiation and updating of services.

Figure 4: Overview of six principles for CSPs to remember when designing and selling SECaaS solutions to SMEs



Source: Analysys Mason

Recommendations for CSPs

1

CSPs should lead in communicating cyber security risk to SMEs.

CSPs should drive demand by leading in communicating the specific cyber risks that SMEs face in the cloud and on their premises. Many SMEs have inadequate understanding of this. They also lack awareness of the legal obligations to protect third-party data that forthcoming data protection regulations will demand. Many SMEs will not spend more on security without a better understanding of security risks and how to manage them.

2

CSPs should prioritise ease of use when designing the security service suite.

SMEs do not want services that are difficult to use. Such services lead to customer dissatisfaction and heavy use of customer support, which will threaten CSPs' margins. Bundling security with connectivity is a good starting point. However, most SMEs also want security software delivered from the cloud as a service direct to a PC or management console. Championing ease of use also means prioritising it over marginal gains in security efficacy. Solutions that are easy to use should be easy to sell.

3

CSPs should use their scale, service bundling and reputations as local trusted providers to differentiate themselves from potential competitors.

The ability to build a comprehensive suite of security services at low cost is a key differentiator for CSPs, as is the ability to bundle those services with connectivity. Further differentiation is challenging but achievable. CSPs should consider offering options such as cyber security insurance and C-Suite training in cyber-attack crisis management. CSPs may also be able to use locally run and managed data centres as a differentiator.

© Analysys Mason Limited 2017

CONTENTS

EXECUTIVE SUMMARY

OPPORTUNITIES AND RISKS FOR CSPs

PORTFOLIO DESIGN

DRIVING DEMAND AND NEW CHANNELS TO MARKET

APPENDIX: DEUTSCHE TELEKOM AND M1

ABOUT THE AUTHORS AND ANALYSYS MASON

analysys mason

About the authors

Patrick Donegan (Senior Contributor) contributes to Analysys Mason's *Telecoms Software and Networks*, and *Enterprise and IoT* research practices. He specialises in telecoms and IT security and has worked in the telecoms sector for over 25 years. Patrick has led several custom consulting projects for leading vendor and operator clients in this area. In recent years, his research has focused on the security opportunities and threats presented by the telecoms sector's efforts to use more software-controlled networking.

Tom Rebbeck (Research Director) leads Analysys Mason's *Enterprise and IoT* research practice. He has more than 16 years of experience in the telecoms sector. He is based in our London office, but works for clients worldwide. Tom specialises in the Internet of Things (IoT) and other enterprise services, and has written widely on the role for operators as telecoms markets develop. He has worked on projects for a range of clients – including operators, regulators, industry bodies and vendors. Many of these projects have been supported by original research, such as expert interviews and customer surveys.

© Analysys Mason Limited 2017

Research from Analysys Mason

Clients across the breadth of telecoms, media and technology sectors rely on our research and analysis to inform business-critical decisions.

Consumer services programmes
- Mobile Services
- Mobile Devices
- Fixed Broadband Services
- Convergence Strategies
- Video Strategies

Network investment programmes
- Network Investment Strategies
- Network Traffic
- Spectrum

Telecoms software and networks programmes
- Software Forecast and Strategy
- Telecoms Software Market Shares

Network-focused
- Next-Generation Wireless Networks
- Service Delivery Platforms
- Service Fulfilment
- Service Assurance
- Network Orchestration
- Software-Controlled Networking

Customer-focused
- Digital Experience
- Customer Care
- Revenue Management
- Analytics

analysysmason.com/research

Digital economy programmes
- Digital Economy Strategies
- Future Comms

Enterprise and IoT programmes
- Large Enterprise Voice and Data Connectivity
- Large Enterprise Emerging Service Opportunities
- SME Strategies
- IoT and M2M Services
- IoT Platforms and Technology

Regional markets programmes
- Global Telecoms Forecasts
- Asia–Pacific
- Middle East and Africa
- European Core Forecasts
- European Telecoms Market Matrix
- European Country Reports

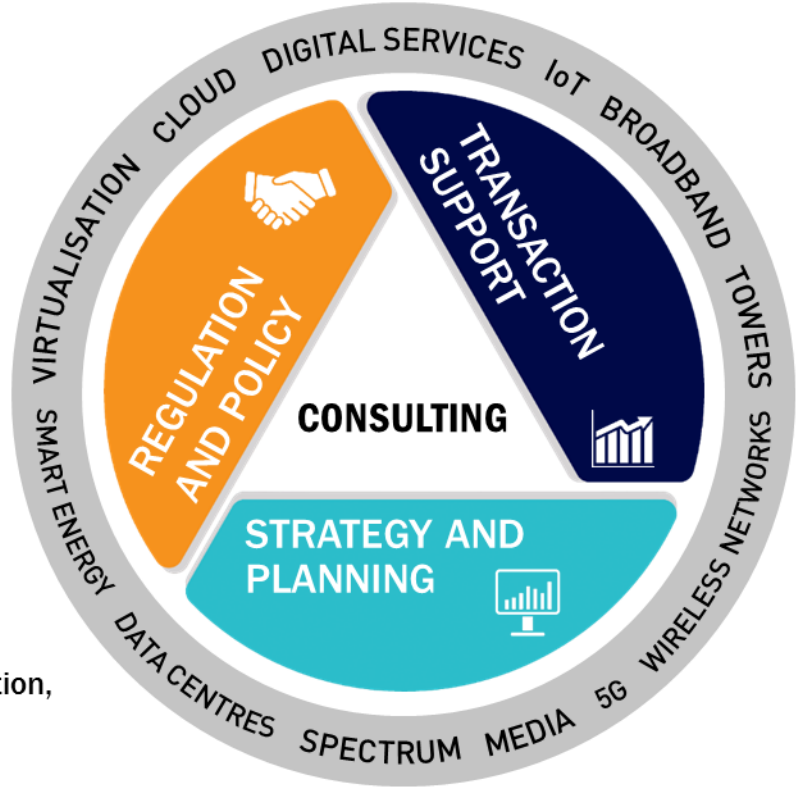
DataHub
- Data covering +80 countries and +400 operators
- +1400 forecast and +250 historical metrics
- Regional results and worldwide totals
- Operator historical data
- Compare markets and operators
- Financial values in USD, EUR or local currency
- Export data to Excel and save searches

© Analysys Mason Limited 2017

Consulting from Analysys Mason

REGULATION

- Quality of service
- Market review
- Margin squeeze tests
- Analysing regulatory accounts
- Regulatory economic costing
- Policy development and response
- Media regulation
- Expert legal support
- Radio spectrum management
- Net cost of universal service
- Radio spectrum auction support
- Postal sector policy: USO, liberalisation, costing, pricing and regulation



TRANSACTION SUPPORT

- Commercial due diligence
- Technical due diligence
- Digital services
- Mid-market finance sponsors
- Data centres

STRATEGY AND PLANNING

- Commercial expertise
- Technology optimisation
- New digital frontiers

analysysmason.com/consulting

PUBLISHED BY **ANALYSYS MASON LIMITED** IN **MAY 2017**

Bush House • North West Wing • Aldwych • London • WC2B 4PJ • UK

Tel: +44 (0)20 7395 9000 • Email: research@analysysmason.com • www.analysysmason.com/research • Registered in England No. 5177472

© Analysys Mason Limited 2017. All rights reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means – electronic, mechanical, photocopying, recording or otherwise – without the prior written permission of the publisher.

Figures and projections contained in this report are based on publicly available information only and are produced by the Research Division of Analysys Mason Limited independently of any client-specific work within Analysys Mason Limited. The opinions expressed are those of the stated authors only.

Analysys Mason Limited recognises that many terms appearing in this report are proprietary; all such trademarks are acknowledged and every effort has been made to indicate them by the normal UK publishing practice of capitalisation. However, the presence of a term, in whatever form, does not affect its legal status as a trademark.

Analysys Mason Limited maintains that all reasonable care and skill have been used in the compilation of this publication. However, Analysys Mason Limited shall not be under any liability for loss or damage (including consequential loss) whatsoever or howsoever arising as a result of the use of this publication by the customer, his servants, agents or any third party.