RESEARCH

analysys mason

# CYBER SECURITY:

## SELLING TO SMALL AND MEDIUM BUSINESSES

# Contents

# Introduction

## Welcome to our first collection of articles looking at security, with particular focus on the small and medium-sized business (SMB) market (that is, firms with up to 1000 employees).

Many vendors give less attention to SMBs than to large enterprises. SMBs can be harder to serve, spend less, are more price-sensitive and often value ease of use over the performance or features of a solution. However, we believe that SMBs occupy an exciting area of the market; indeed, spend on security continues to grow as firms look to improve their protection. We forecast that SMBs' spend on security worldwide will almost double between 2019 and 2024 (from a starting point of USD50 billion). Limited vendor attention means that this market is not well-understood and is often poorly served, but it offers a lucrative opportunity for providers who do get their product right.

The articles featured in this brochure give a flavour of our security research. They cover the following topics.

- **Cyber-security vendors' revenue is growing steadily, helped by acquisitions and strong demand.** This article explores the trends in the revenue generated by leading cyber-security vendors and selected telecoms operators that compete in the cyber-security space.
- **Acquisitions are a standard way for cyber-security service providers to expand capabilities and presence.** This provides a review of some of the major acquisitions during 2018 and 2019, and the motives behind them.
- **Business survey 2019: almost 25% of small businesses feel that their cyber-security protection is inadequate.** Many SMBs are aware of the problems with their current protection (and, arguably, many more have problems that they are unaware of), but they do not know how to fix them. These issues create opportunities for vendors and service providers
- **Business survey 2019: cyber-security vendors need to change their approach to win in middle-income markets.** Companies in all countries have similar security requirements, but their capacity to meet these requirements differs by income level. Security providers need to consider what this means for their strategies if they want to succeed outside of rich, high-income countries.
- **Sophos should become a more stable and stronger competitor thanks to its acquisition by Thoma Bravo.** A change of ownership for Sophos does not change the SMB security landscape, but it should help Sophos to pursue a longer-term agenda.
- **Broadcom's purchase of Symantec's enterprise unit will create opportunities for other cyber-security players.** Broadcom's strategy for Symantec will be to cut costs, reduce the size of the product portfolio and target the largest 2000 firms globally, all of which will open opportunities for competitors.

As well as our research, Analysys Mason's consulting division helps clients in all geographies and parts of the value chain to develop their approach to security. Our assignments range from rapid reviews of existing plans to full strategy development. Please contact us for more details on our research programmes or our consulting capabilities.

We send a monthly newsletter highlighting our latest business services research to around 6000 people. Please email me if you would like to be included on the mailing list.

**Tom Rebbeck**
Research Director, Research at
tom.rebbeck@analysysmason.com

# Cyber-security vendors' revenue is growing steadily, helped by acquisitions and strong demand

Igor Babić, Analyst, Research

The revenue of major cyber-security vendors grew at an average rate of 15% in 2018, largely due to acquisitions and the strong demand for cyber-security services. However, this revenue growth was far from uniform; for example, Splunk's revenue grew by 37.7%, while Symantec registered only 0.3% revenue growth. Revenue Europe and Asia grew faster than that from North America, and revenue generated through subscriptions grew faster than that from products and hardware. This explains the large variation in revenue growth to some extent.

This article explores the trends in the revenue generated by leading cyber-security vendors and selected telecoms operators that compete in the cyber-security space. It draws upon Analysys Mason's Cyber-security vendors' revenue tracker.

**All of the leading cyber-security vendors are experiencing revenue growth, albeit at very different year-on-year rates**

The average year-on-year (YoY) revenue growth rate for the ten cyber-security vendors shown in Figure 1 was 15% in 2018. The three telecoms operators that report security revenue achieved higher year-on-year revenue growth rates than some of the vendors shown, but did so from relatively small bases.

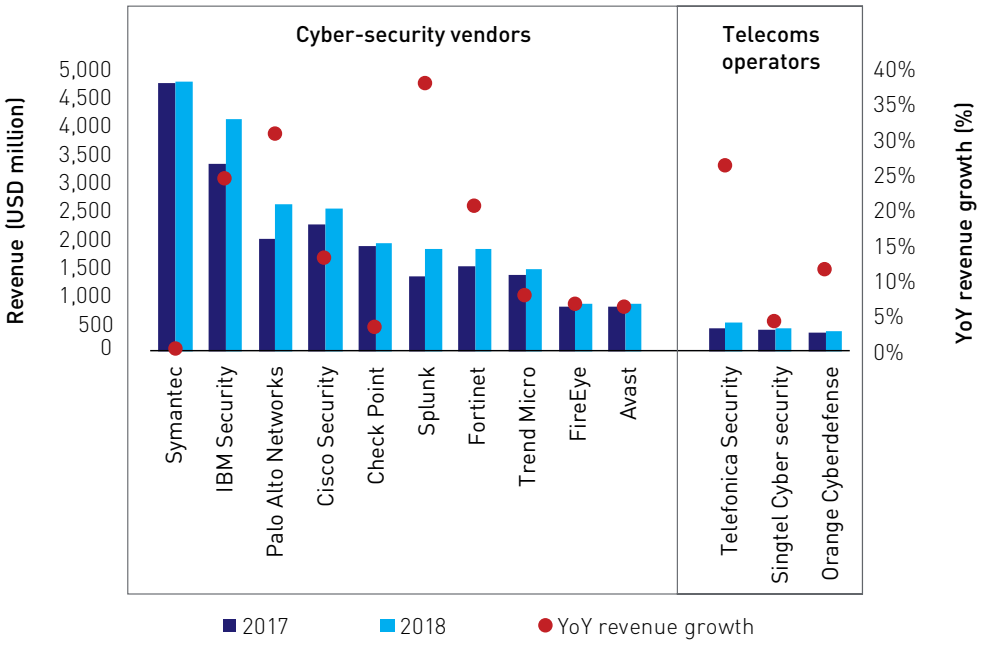


**FIGURE 1:** REVENUE GENERATED BY THE MAJOR CYBER-SECURITY VENDORS AND SECURITY REVENUE GENERATED BY TELECOMS OPERATORS, 2017 AND 2018 [SOURCE: ANALYSYS MASON, 2019]

Symantec, the largest cyber-security vendor in Figure 1 (in terms of revenue), had the lowest revenue growth rate of the players included in this article at just 0.3% in 2018. This was due to a decline in its 'Enterprise Security' sales; revenue from this segment decreased by 12.1% (from 54.9% to 49.5% of the vendor's total revenue). Conversely, its 'Consumer Digital Safety' revenue increased by 9.1% YoY in 2018. Symantec announced plans to cut around 8% of its global workforce due to this slow-down in sales to business customers.

Splunk, on the other hand, achieved the highest revenue growth rate of the vendors shown in Figure 1 at 37.3% in 2018. Splunk is focused on security information and event management (SIEM), as well as the monitoring and analysis of IT operations and IoT device data, and it increased its total number of customers from around 15 000 to over 17 500 in 2018. It also acquired Phantom, a security orchestration, automation and response (SOAR) specialist, and VictorOps, a company focused on collaborative incident management. Splunk's approach to working with channel partners, including managed service providers (MSPs), systems integrators, resellers and professional services firms, was a major contributor to its revenue growth in 2018. Splunk's partner bookings increased by 63% YoY and its channel partners brought in 76% of the new customers. The vendor's focus on expanding its product portfolio and updating its existing products also resulted in an increase in average customer spend in 2018.

IBM and Palo Alto Networks, the second- and third-largest cyber-security vendors in Figure 1 (in terms of revenue), also achieved high revenue growth rates in 2018. IBM's security revenue benefited from a strong growth in demand for the vendor's SIEM (QRadar) and SOAR (Resilient) offerings, following the company's acquisition of Resilient Systems for a reported USD100 million in 2016. The main revenue growth engines for Palo Alto Networks are acquisitions and cross-selling. The vendor acquired three companies in 2018 and a further three in 2019 (as of June), for a total of around USD1.6 billion. Palo Alto Networks was initially focused on firewalls, but in recent years, it has expanded its portfolio to cover various other enterprise security fields, including endpoint, public cloud and SaaS security. This, helped by the vendor's acquisitions which brought in some of this expertise and a number of customers, created cross-selling opportunities that are being exploited.

The cyber-security revenue of all three telecoms operators featured in Figure 1 grew in 2018; Orange and Telefónica achieved double-digit growth rates. Telefónica's revenue grew the most quickly (and from the largest base) out of all three operators and has continued to grow in 2019. In 1Q 2019, it grew by 34.6% YoY on the back of the opening of a new security operations centre in the UK and the sustained increase in the number of business customers.

We expect that Orange will roughly double its security revenue in 2019 as a result of its acquisitions of SecureData and SecureLink. These acquisitions will also accelerate the implementation of the operator's strategy to become a pan-European leader in cyber security. Singtel's security revenue growth rate was relatively low at 4.1% in 2018, but the demand for the operator's managed security services was strong, particularly in the Asia–Pacific region. Its security revenue suffered from the continued decline in demand for Trustwave's legacy payment card industry data security solutions, which are facing commoditisation.

Upon reviewing the detail of the cyber-security vendors' revenue landscape, we can see the following trends.

- Revenue from Europe, the Middle East and Africa (EMEA) typically grew the fastest in 2018, outpacing that from Asia–Pacific and North America. For the vendors that report their regional revenue splits, revenue from EMEA grew by 19% on average, compared to 15% for that from Asia–Pacific and 10% for that from North America.
- Revenue from subscriptions (sometimes including licences) grew by 30% on average in 2018; this represents a much faster growth rate than was seen for revenue from products and hardware. Palo Alto Networks had the highest reported subscription revenue of the vendors tracked, and this grew by 30.7% in 2018.
- No clear trend emerged on the split of revenue between business and consumer security products/services. For example, F-Secure's 'Corporate Security' revenue grew by 32.8% in 2018 to form the majority of the company's total revenue (just over 50%), while its 'Consumer Security' revenue decreased by 2.6% in the same period. Avast and Symantec saw the opposite trend, while revenue from both the business and consumer customer segments grew for Trend Micro in 2018. These results were mainly influenced by the individual offerings from each vendor, and the geographies that were primarily served.

The full details of the tracked revenue of the cyber-security vendors that are mentioned in this article are available in Analysys Mason's Cyber-security vendors' revenue tracker.

**Questions?**
Please feel free to contact Igor Babić, Analyst, Research at igor.babic@analysysmason.com

# Acquisitions are a standard way for cyber-security service providers to expand capabilities and presence

Igor Babić, Analyst, Research

Most major cyber-security vendors acquired smaller security service providers during 2018 and 1Q 2019 in order to expand their portfolios and market reach. Telecoms operators also made M&A in the cyber-security space during this period. The main difference between the acquisitions carried out by these two company types is their purpose; vendors tend to acquire technology, while operators acquire people and consulting capabilities.

This article explores the acquisition activity of leading cyber-security vendors and telecoms operators that are competing in the cyber-security space. It draws upon Analysys Mason's Cyber-security-related M&A tracker.

**Both cyber-security vendors and telecoms operators are using acquisitions to expand their cyber-security capabilities**

Cisco spent the most on acquisitions in 2018 and 1Q 2019 out of the vendors covered in Analysys Mason's *Cyber-security-related M&A tracker*. This is mainly due to its acquisition of Duo Security, a unified access security and cloud multi-factor authentication specialist, for USD2.35 billion (Figure 1). Duo Security generated over USD100 million in annual recurring revenue in 2017 and employed around 700 people at the time of the acquisition. It had reportedly raised a total of USD121.5 million prior to the acquisition.

Palo Alto Networks spent the second-largest amount on acquisitions in 2018 and 1Q 2019. It completed four cyber-security-related acquisitions during this period, and spent over USD1.1 billion in total (it acquired a further two companies in May 2019 for a total of around USD500 million). Its biggest acquisition was of Demisto (completed in March 2019), a security orchestration, automation and response specialist founded in 2015, for which Palo Alto Networks paid USD560 million. This acquisition will improve Palo Alto Networks's analytics and automation capabilities and will enable the vendor to accelerate its Application Framework strategy (which, in turn, will allow customers to deploy security innovations more quickly, through a suite of APIs).

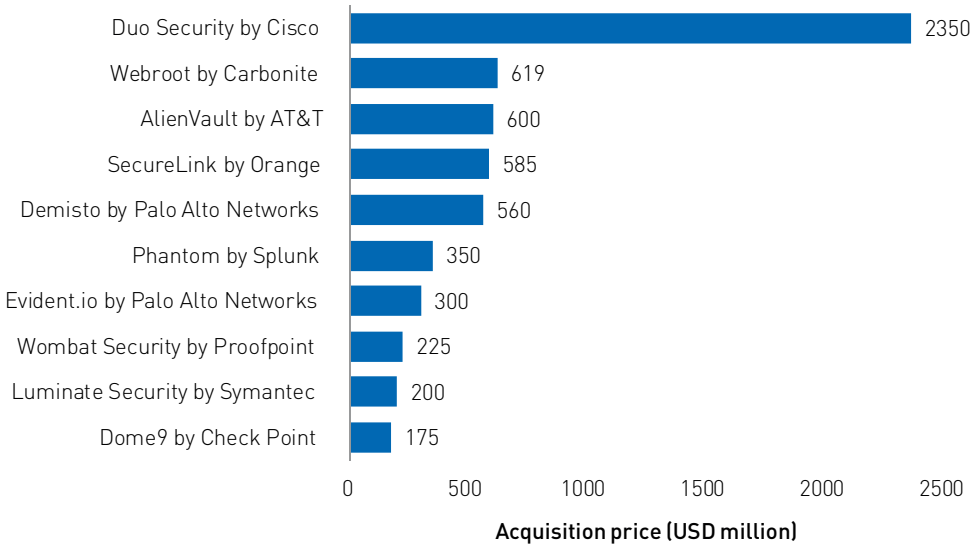


**FIGURE 1:** TEN MOST-EXPENSIVE CYBER-SECURITY ACQUISITIONS (WHERE THE AMOUNT PAID WAS DISCLOSED OR WHERE RELIABLE ESTIMATES ARE AVAILABLE), 2018 AND 1Q 2019 [SOURCE: ANALYSYS MASON, 2019]

Figure 2 illustrates how much each acquirer spent per employee to acquire the listed companies. The variation in these valuation multiples tells us a lot about the motives behind these acquisitions. Companies that were acquired mainly because they have developed unique and valuable technologies have higher per employee valuation multiples than more-established businesses that are primarily focused on providing consulting services. For example, the main reason behind Palo Alto Networks's acquisition of Redlock was to obtain Redlock's Cloud 360 AI-driven threat defence platform. Similarly, Symantec acquired Luminate Security primarily because of Luminate's Secure Access Cloud software-defined perimeter technology.

Telecoms operators have also made M&A deals in the cyber-security space. Orange spent nearly USD750 million in 2019 on its acquisitions of SecureData, a UK-based company providing integrated cyber-security solutions and consulting services, and SecureLink, a specialist in business solutions for secure remote access headquartered in the Netherlands. Both companies are well-established and focus primarily on consulting rather than technology development, explaining their position in Figure 2. Orange has added around 880 employees to its Cyberdefense business through these two acquisitions; it has extended its presence in Europe and has expanded into South Africa. Orange Cyberdefense generated USD358 million in revenue in 2018 (that is, prior to these acquisitions); SecureData generated USD57 million and SecureLink USD282 million during the same period. Orange will therefore roughly double its security revenue as a result of these acquisitions.

AT&T acquired AlienVault in 2018 for an estimated USD550 million–USD650 million and added around 300 employees as a result. AlienVault has reportedly raised a total of USD116 million since its inception in 2007. This acquisition allowed AT&T to significantly expand its cyber-security capabilities, and in 2019, the operator formed AT&T Cybersecurity, a standalone unit led by AlienVault's ex-CEO.

Orange's and AT&T's recent activities are not typical of operators (the acquisitions of AlienVault and SecureLink are the largest cyber-security acquisitions by operators since Singtel's USD810 million acquisition of Trustwave in 2015); most other operator cyber-security acquisitions have been far smaller. For example, Proximus acquired two companies in 2017 and 2018; one specialised in security analytics and vulnerability management and the other in providing managed security services. Each company had between 20 and 30 employees at the time of acquisition. KPN acquired malware protection specialist DearBytes (85 employees) in 2017 and TDC acquired Secu (11 employees) in 2019, a company focusing on vulnerability management services.

### The main difference between the acquisitions carried out by cyber-security vendors and those executed by telecoms operators is their purpose

All acquisitions in the cyber-security space enable the acquirer to expand its capabilities to some extent, but those carried out by vendors are more often executed to obtain technology or IP that can then be implemented into the vendors' offerings (as well as to acquire highly specialised talent). Acquisitions carried out by telecoms operators, on the other hand, are more often focused on gaining access to market segments that the operators are not already addressing sufficiently with their current offerings. For example, AT&T's acquisition of AlienVault enabled the operator to better target SMEs, Orange's two acquisitions in 2019 expanded the operator's cyber-security services geographical footprint and Proximus's acquisition of ION-IP in 2018 enabled the operator to expand its service portfolio in the Netherlands and increase the number of cyber-security vendors that it partners with. The aim of operators' acquisitions is often also to increase the cyber-security value chain coverage of their services (for example, through acquiring a company with managed services or software development capabilities).

More details regarding the acquisitions of the companies mentioned in this article are available in Analysys Mason's Cyber-security-related M&A tracker.

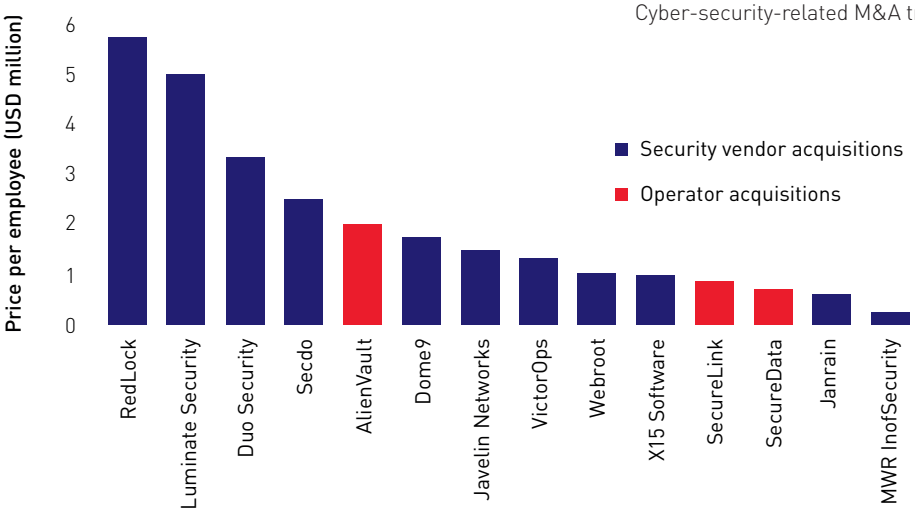


**FIGURE 2:** ACQUISITION PRICE PER EMPLOYEE (FOR THE CASES WHERE THE NUMBER OF EMPLOYEES AND THE ACQUISITION PRICE WERE BOTH REPORTED) [SOURCE: ANALYSYS MASON, 2019]

**Questions?**
Please feel free to contact Igor Babić, Analyst, Research at igor.babic@analysysmason.com

# Business survey 2019: almost 25% of small businesses feel that their cyber-security protection is inadequate

Tom Rebbeck, Research Director, Research

The cyber-security market for micro, small and medium-sized businesses (SMBs) is large, and rapidly growing. Analysys Mason estimates that enterprises with fewer than 1000 employees will spend around USD50 billion on security solutions in 2019 and that this will grow at an average rate of 13% between 2019 and 2024.

However, the market may not achieve this growth unless security vendors do a better job of servicing it. Vendors that want to succeed in the SMB market need to do more to explain the security risks that small companies face and increase awareness of products that can help these companies mitigate such risks.

Our recent survey of around 3000 businesses worldwide shows that the smaller a business, the larger the relative impact of a cyber attack. Despite this, small companies are not well served by security vendors.

### Cyber attacks have a relatively larger impact on smaller businesses

High-profile cyber attacks on large businesses such as British Airways or Equifax may make headlines, but rarely have severe long-term consequences for the business. In contrast, a cyber attack can threaten the existence of a small business. According to our survey, the average cost per employee of all attacks in the past 12 months was over USD400 for a micro business, compared to costs of USD25 for a large business (see Figure 1). (All data is self-reported and should be treated with caution.)

Security incidents are also relatively common for smaller companies. In our survey, 32% of micro businesses and 39% of small businesses reported that they have experienced a security-related incident in the last 12 months. These figures are lower than for larger companies (61% of large companies had some sort of incident in the last 12 months), but given that larger companies have more of everything (people, PCs, servers etc.), this difference is unsurprising. Again, if we compare the data on a per employee basis, smaller companies are more vulnerable than larger ones.

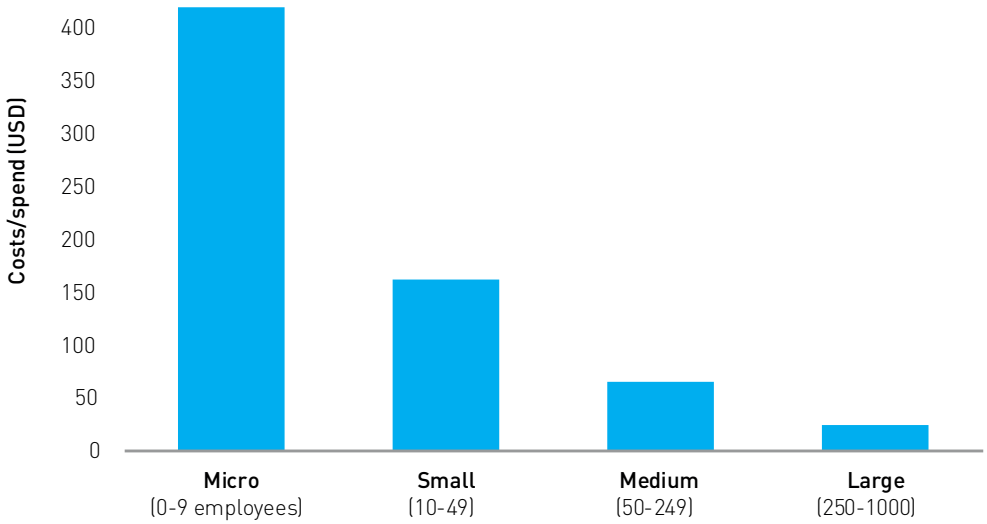


**FIGURE 1:** ESTIMATED COST OF SECURITY-RELATED INCIDENTS EXPERIENCED IN THE LAST 12 MONTHS, BY BUSINESS SIZE, PER EMPLOYEE[1] [SOURCE: ANALYSYS MASON, 2019]

This vulnerability is reflected in how smaller companies feel about their level of protection. Only 77% of micro businesses said that they felt fairly or extremely well-protected against cyber-security attacks and threats from external parties (compared to 90% for large businesses). The remaining 23% of micro businesses felt either somewhat or not satisfactorily protected, compared with just 10% of large businesses.

### Security vendors are not serving smaller businesses well

Few micro or small businesses have dedicated security personnel. Security is often the responsibility of an office manager, or even of the company owner. This makes it more difficult for security vendors to target the right person than when targeting larger organisations. However, this should not be mistaken for a lack of interest in security; our survey shows that the security priorities of smaller businesses (for example, protecting customers' data, ensuring business continuity) are almost identical to those of larger organisations.

The lack of specialist security staff and limited budgets are considered to be barriers to the development of security capabilities by surveyed businesses of all sizes. However, smaller businesses were more likely than larger ones to cite the lack of awareness of new security vendors and their products as a challenge (see Figure 2). Large and medium-sized businesses identified the lack of awareness of new security vendors and their solutions as the least of their challenges out a list of 12 options.

### Vendors should see this large, growing and underserved market as an opportunity

Vendors might regard smaller businesses as unattractive business propositions for many reasons: spend per company will be low relative to larger organisations; prospects can be hard to find and expensive to serve; price may be more important than technical capabilities in decision making, as may ease of use.

For vendors that are willing to tackle this market though, these negatives create an opportunity. As our survey reveals, even the smallest enterprises have expressed interest and increasing awareness of the need to improve security. A security breach is likely to cost at least a few thousand dollars, and for a small business with tight cash flows, that amount could represent the difference between surviving or not. Despite this (or perhaps because of it), smaller enterprises are less likely to feel well-protected than their larger counterparts.

Vendors that want to sell to micro and small businesses need to:

- highlight the impact of a security breach
- show how their products can help to mitigate the risks
- make it easy for businesses to adopt their services.

Vendors should experiment with self-serve options, freemium models and free trials that can be used to demonstrate the threats that businesses are facing.

[1] Questions: "Has your company experienced any of the following IT security-related events in the last 12 months?"and to companies that suffered a security-related incident "How much would you estimate that the incident(s) cost your company (including direct losses as well as costs incurred to recover from the breach(es) and restore the lost information, legal costs to your business, and costs of repairing your business' reputation)?". n = 2983.

[2] Question: "Which of the following are challenges to your company having a highly effective cyber-security capability?". n = 2983.

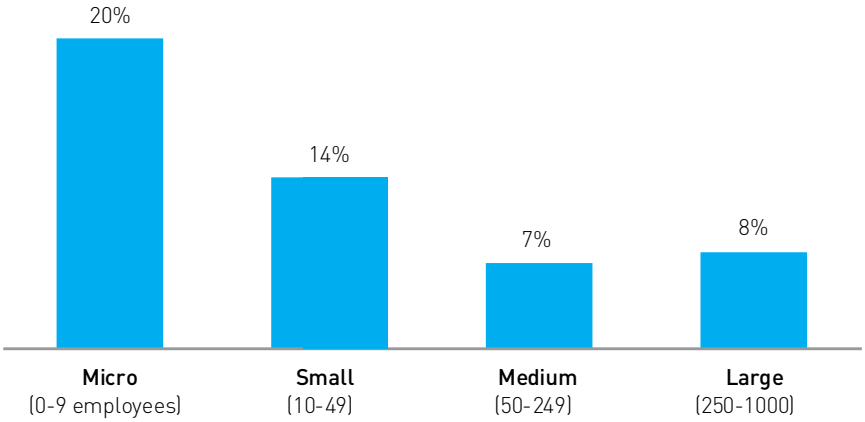


**FIGURE 1:** PERCENTAGE OF BUSINESSES THAT CITED THE LACK OF AWARENESS OF SECURITY VENDORS AND THEIR PRODUCTS AS A CHALLENGE[2] [SOURCE: ANALYSYS MASON, 2019]

**Questions?**

Please feel free to contact Tom Rebbeck, Research Director, Research at tom.rebbeck@analysysmason.com

# Business survey 2019: cyber-security vendors need to change their approach to win in middle-income markets

Igor Babić, Analyst, Research

Analysys Mason's recent survey of almost 3000 small and medium-sized businesses (that is, companies with fewer than 1000 employees) worldwide shows that businesses in middle- and high-income countries have similar cyber-security requirements, and share similar views on the threat landscape.[1]

Despite this, the challenges that these businesses face in developing their security capabilities vary considerably. Vendors that want to grow in middle-income markets (such as India and Indonesia) need to understand that the prices and complexity of their standard solutions are significant barriers to adoption. They should address this problem by adapting their offerings.

### Businesses in middle- and high-income countries have similar views on what will affect their cyber-security plans

Businesses in both high- and middle-income countries perceive the need to protect their customers' privacy and data as the main factor that will have an impact on their security plans in the next 12–18 months. This comes as no surprise; 32% of businesses in middle-income countries and 22% of those in high-income countries experienced a security incident involving theft of data during the last 12 months, according to our survey.

Businesses in these two country groups share similar views regarding the factors that will affect their short-term cyber-security plans (see Figure 1).

### The security-related challenges that businesses in middle- and high-income countries face are markedly different

Our survey also asked about the barriers that businesses face in developing their cyber-security capabilities.The results were starkly different by country income level (see Figure 2).

A lack of awareness of vendors and the products available in the market is the biggest problem for businesses in the UK and the USA. In all of the middle-income countries surveyed, this is the least significant barrier for the adoption of security solutions. In these countries, factors under vendors' control

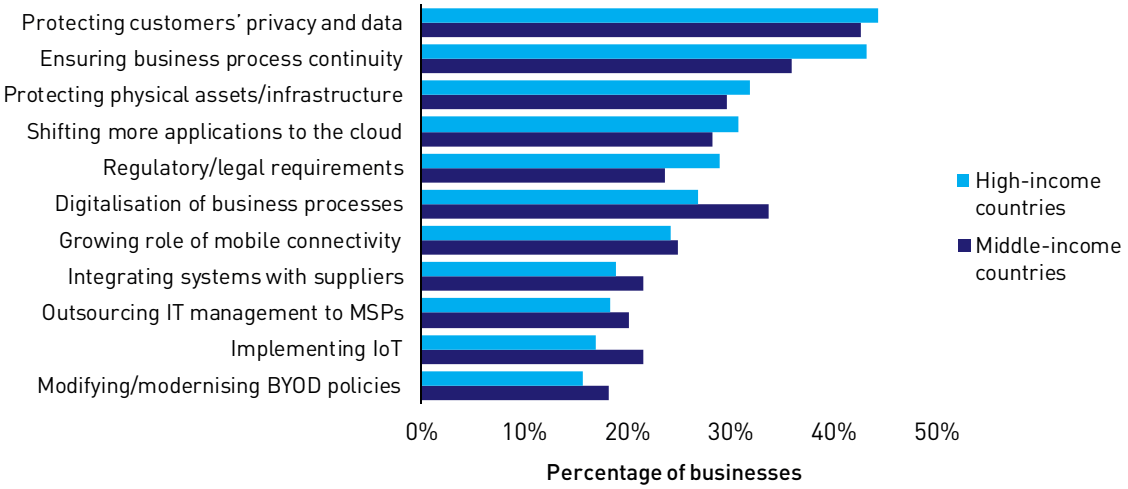


**FIGURE 1:** FACTORS THAT WILL AFFECT BUSINESSES' SHORT-TERM CYBER-SECURITY PLANS, AVERAGES FOR HIGH- AND MIDDLE-INCOME COUNTRIES[2,3] [SOURCE: ANALYSYS MASON, 2019]

– such as solution pricing, solution complexity, the guidance provided and vendors' ability to provide optimal solutions – are all perceived to be more important barriers.

A lack of specialist security staff is a problem for businesses in both middle- and high-income countries; but again, a higher proportion of the surveyed businesses in middle-income countries listed this as a challenge. It is notable that European businesses (those in France, Germany and the UK) are the least worried about this issue.

Security vendors should see the challenges that businesses in middle-income countries face as an opportunity. These businesses may be unattractive targets to vendors for many reasons – such as their security spend being lower than that of companies in high-income countries and pricing being a more important factor in purchasing decisions – but they represent a growing market that vendors can serve with existing capabilities. Few security vendors report their regional revenue splits, but from the revenue of those that do, we can conclude that revenue growth is significantly faster in the rest of the world than in North America, easily the largest region currently for many vendors.

To address the growing opportunity in middle-income markets, security vendors could consider providing lower-cost versions of their standard offerings. Solutions would need to be less complex and faster to implement, and would need to come with an appropriate level of guidance (given that around a fifth of surveyed businesses in middle-income countries reported that the lack of guidance around solutions was a challenge, and a quarter stated that they lack specialist security staff). Vendors could also experiment with freemium models in such markets, allowing businesses to use specific features of their solutions free of charge. If businesses are satisfied with the level of service offered for free (particularly in terms of simplicity to use), they may be easier to convert into paying customers.

For more information about the topics discussed in this article, see Analysys Mason's *Business survey 2019: cyber-security trends in high- and middle-income countries* report.

[1] Middle-income countries: those with a gross national income (GNI) per capita of between USD1026 and USD12 375. High-income countries: those with a GNI per capita of above USD12 375.
[2] Question: "Which of the following business goals and developments will have an impact on your cyber-security plans over the next 12-18 months?". n = 2983.
[3] MSP = managed service provider; BYOD = bring your own device.
[4] Question: "Which of the following are challenges to your company having a highly effective cyber-security capability?". n = 2983.
[5] The survey results for these four countries are indicative of the results obtained for middle- and high-income countries in general.

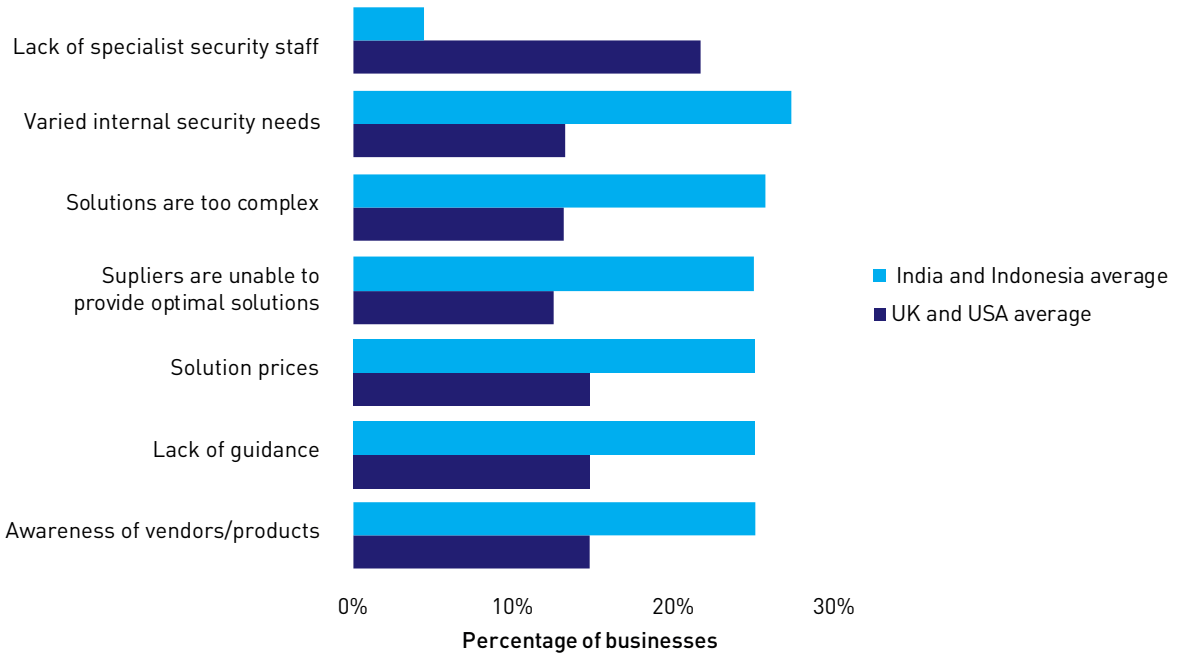


**FIGURE 2:** BARRIERS TO BUSINESSES HAVING HIGHLY EFFECTIVE CYBER-SECURITY CAPABILITIES, SELECTED HIGH- AND MIDDLE-INCOME COUNTRIES[4,5] [SOURCE: ANALYSYS MASON, 2019]

**Questions?**
Please feel free to contact Igor Babić, Analyst, Research at igor.babic@analysysmason.com

# Sophos should become a more-stable and stronger competitor thanks to its acquisition by Thoma Bravo

Tom Rebbeck, Research Director, Research


The USA-based private equity firm Thoma Bravo announced on 14 October 2019 that it was buying Sophos, a UK-based security firm. The purchase price was GBP5.83 per share; this is a 37% premium over the pre-deal price, and gives Sophos an enterprise value of GBP3.1 billion.

Private ownership should provide Sophos with the support and stability that it needs to pursue its strategy, without the distraction of the short-term concerns that are associated with being a public company. For example, during 2018, Sophos's share price was hit by investors that were unnerved by uneven revenue growth, and this may have taken management attention away from longer-term ambitions. Thoma Bravo's purchase further increases its exposure to a sector that it knows well. It will be hoping to repeat the success that it is having with other acquisitions.

**Thoma Bravo is investing heavily in technology firms that supply small and medium-sized businesses (SMBs), particularly in the cyber-security sector**

The logic of the deal for Sophos's shareholders is clear given the premium over the share price that has been offered. The motives of the buyer are more interesting.

Thoma Bravo already knows the cyber-security sector well. Its website lists 12 security firms in its current portfolio, and a further 7 previous security-related investments. Current investments include Barracuda, which it owns, and McAfee, in which it has a minority stake.

Thoma Bravo is comfortable with competition between the companies in which it has invested, unlike some other

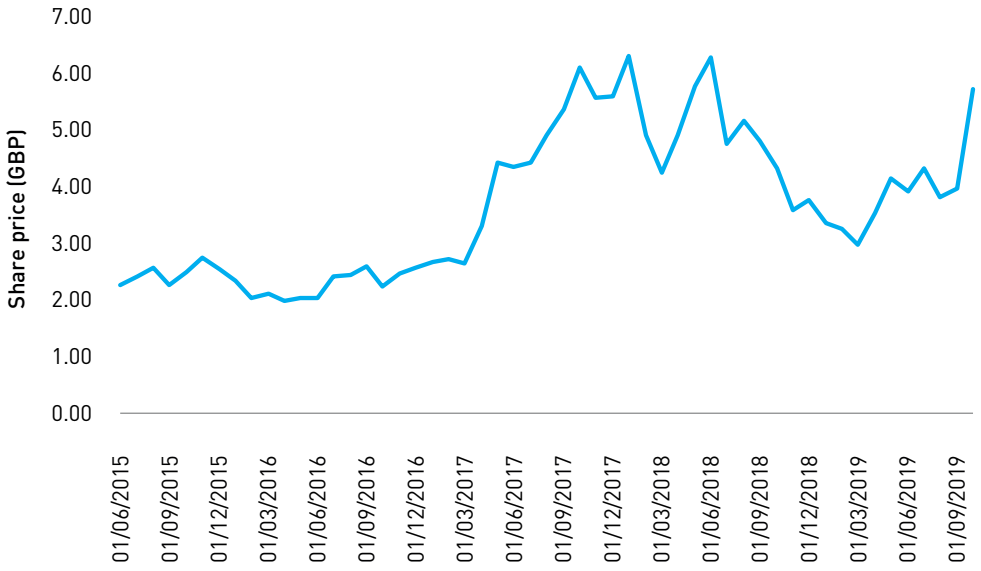


**FIGURE 1:** SOPHOS'S SHARE PRICE, JUNE 2015–OCTOBER 2019
[SOURCE: ANALYSYS MASON, 2019]

private equity firms that prefer to merge acquisitions or explore collaboration between portfolio companies. Thoma Bravo appears to have selected a market segment to focus on (technology firms that supply SMBs); it is backing several firms in this segment, rather than trying to pick (or create) a winner. Many managed service providers (MSPs) focus on the SMB market, and as such, Thoma Bravo also owns or has stakes in Barracuda, ConnectWise, Continuum and Solarwinds, all of which supply MSPs. (Sophos is also active in the MSP space, and has a dedicated MSP division.)

Sophos has a number of strengths that make it an attractive prospect, in addition to fitting Thoma Bravo's more-general interest in the security market. It is a European firm and generates most of its revenue from within the region, unlike most other major security firms that tend to be strong in North America and weaker elsewhere.

The SMB focus is also unusual for a security firm; most security vendors pay little attention to this market. Sophos has invested heavily in supporting its channel partners, which is in keeping with its SMB focus. Additionally, Sophos's core firewall and endpoint protection products are well-regarded and easy-to-use, which is valuable when targeting a market where few have specialist internal security skills. Sophos is investing heavily in improving its products further (its spend on R&D was USD144 million in FY2019; this is equivalent to 20% of its revenue).

Sophos does face challenges, however. The greatest threat to Sophos's revenue is likely to come, not from other pure-play security firms, but from other technology firms that are adding security as a feature. For example, Microsoft's security products that are bundled with Windows 10 are becoming ever more powerful and may, at least for some SMBs, provide sufficient protection.

Bundles of SD-WAN and basic firewalls are also becoming commonplace in the network security market. Sophos does have its own SD-WAN product, but this does not have the traction or market awareness of solutions from Cisco, Nokia (Nuage Networks) or VMware (VeloCloud), for example. The challenge for Sophos will be to make its bundle of security products (for example, its bundle of endpoint and network security) more valuable to customers than bundles of security solutions with other types of products (such as Microsoft's bundle of endpoint security and its operating system).

### Sophos's performance in 2018 underwhelmed investors

Sophos's results for its FY2019 (which ended in May 2019) were positive overall, and the company reported 11% year-on-year revenue growth. However, the uncertainty over its performance disappointed investors (Figure 1). Indeed, the price agreed by Thoma Bravo (GBP5.83) is more than 10% off Sophos's January 2018 peak share price of GBP6.54. Quarterly revenue fell in the first quarter of FY2019, and then again in the second quarter. Even in the most recent results, the quarterly revenue of USD180 million is less than USD5 million above the comparable quarter in 2018.

### Sophos can concentrate on longer-term goals as a private company

The Thomas Bravo deal should put Sophos in a better position to invest, both organically and through acquisitions. The declining share price meant that Sophos's management was under pressure to improve the company's short-term visibility, and this may have affected its ability to pursue a longer-term agenda. The deal with Thoma Bravo should increase Sophos's potential to follow its long-term plan.

Thoma Bravo is a supportive shareholder, as can be seen with its other acquisitions, such as Barracuda Networks. Barracuda's share price as a public company had suffered due to concerns over revenue growth (similarly to Sophos). Its share price fell from a peak of USD46.51 in April 2015 to just USD11 a year later. Thoma Bravo bought it for USD27.55 per share in November 2017.

As a private company, Barracuda has been able to grow its annual revenue from under USD400 million at the time of acquisition to approaching USD500 million in October 2019. Barracuda now has a target to reach a revenue of USD1 billion within 3 to 4 years, with growth coming through a mixture of acquisition (two bolt-on acquisitions have been completed since the Thoma Bravo deal) and continued investment in R&D.

Thoma Bravo's acquisition of Sophos will not change the cyber-security industry landscape. This deal is not trying to change the value chain for security services, unlike other recent mergers involving VMware/Carbon Black and Broadcom/Symantec. However, assuming that Thoma Bravo takes a similar approach to Sophos as it has done to its other acquisitions, the deal should help to make Sophos a more-stable and stronger competitor.

**Questions?**
Please feel free to contact Tom Rebbeck, Research Director, Research at tom.rebbeck@analysysmason.com

# Broadcom's purchase of Symantec's enterprise unit will create opportunities for other cyber security players

Tom Rebbeck, Research Director, Research

Broadcom announced the acquisition of Symantec's Enterprise division, for USD10.7 billion, on 8 August 2019. The deal is part of Broadcom's strategy to expand beyond the semiconductor business, which still generates almost 80% of its revenue, and follows earlier acquisitions of Brocade and CA Technologies.

Broadcom aims to use its established sales channels to sell Symantec products to gradually increase revenue and improve profitability by drastically cutting costs. Under Broadcom, Symantec Enterprise will focus on a narrower set of products and customers, creating new opportunities for other players in the security market.

### Symantec's enterprise performance has been troubled

Symantec operates in a growing market (Analysys Mason expects the enterprise security market to expand at around 11% each year during 2019–2024), but its enterprise revenue has been volatile, but with little or no long-term growth (see Figure 1). The enterprise division generated just over half of Symantec's total revenue in the most recent quarter, down from almost two-thirds of the revenue in 3Q 2017.

However, Symantec's profitability was of greater concern – the company reported that its enterprise division was generating just 10% of operating profit. Symantec would

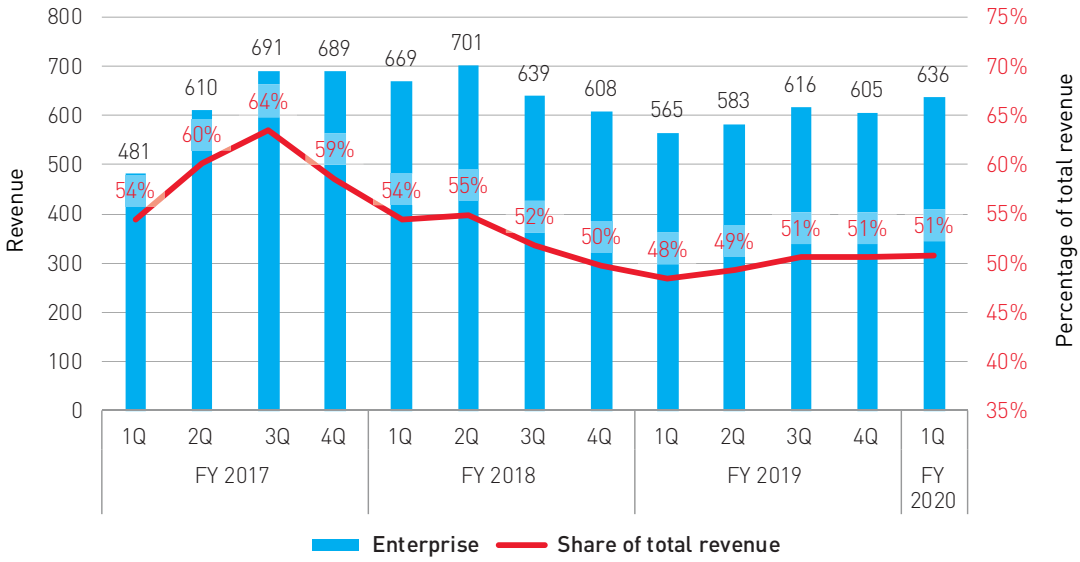


**FIGURE 1:** SYMANTEC'S ENTERPRISE REVENUE AND ITS ENTERPRISE REVENUE AS A SHARE OF ITS TOTAL REVENUE, 1Q 2017–1Q 2020
[SOURCE: ANALYSYS MASON, 2019]

have needed to invest significantly to turn the performance around. Symantec's interim CEO Richard Hill spoke during the 4Q 2019 investor call in May 2019 (that is, well before the sale) of the need to reorganise the sales process and to hire "additional direct salespeople". Instead, Symantec has opted to sell the enterprise assets and focus on the more profitable consumer business. As Hill said when announcing the transaction in August 2019, the deal would "enable our enterprise business to grow without us having to invest in fixing our go-to-market model".

### Broadcom will reuse existing sales channels and significantly reduce costs

The acquisition is part of Broadcom's ongoing move to diversify away from the semiconductor business to include more software and services. This move started when Broadcom purchased datacentre networking firm Brocade for USD5.5 billion in 2016. CA Technologies, a software development firm, was acquired for USD18.9 billion in 2018. These entities will generate just under 30% of Broadcom's total revenue when combined with annual revenue of around USD2.4 billion from Symantec's enterprise business.

The acquisitions of Brocade and CA Technologies are key to understanding the rationale behind the latest deal: Broadcom successfully improved the financial performance of Brocade, in part by increasing revenue but mostly through reduced costs, including large rounds of layoffs. It is hoping to do the same with Symantec's enterprise assets.

The new security assets will give Broadcom access to a large potential market. Analysys Mason estimates that the total enterprise security market is worth USD117 billion in 2019. Broadcom also believes that it can avoid the restructuring costs that were facing Symantec by using the sales teams and platforms developed for Brocade and CA Technologies. The strategy is to target the largest 2000 organisations worldwide.

The cost-cutting targets that Broadcom has for Symantec Enterprise are ambitious; it wants to increase annual EBITDA from around USD350 million today (a 15% margin) to USD1.3 billion (54% margin, assuming no revenue growth).

In addition, Broadcom is planning to focus Symantec's development efforts on the three areas where Symantec is best positioned today – endpoint security, web security and data-loss prevention (DLP). Investment in other areas will be reduced.

Broadcom's plans come with plenty of potential problems. It will want to increase revenue and profit while having a smaller product portfolio, after significantly reducing staff numbers (CA Technologies employee numbers were reduced by a reported 40% in the USA following the Broadcom deal). Broadcom will also deploy a new go-to-market strategy that will take time to establish – for example, existing Broadcom sales teams will need training on how to sell and support security products.

At the same time, Symantec is losing small-business customers (on the 4Q 2019 conference call, a Symantec representative said: "We've lost a lot of business in the mid- to small-business area") and losses in this market are expected to continue. Finally, Symantec is operating in a highly competitive market in which product differentiators can be hard to establish. However, churn among larger customers is low, and Broadcom will need this to remain the case if these larger customers are to act as a base on which to boost the business. It will be no easy task for Broadcom and could well generate opportunities for others.

### The deal will ease competition in some areas of the market

Broadcom will hope that the impact of the deal on existing customers is limited in the near term. The Symantec name will go to the new owner, and the current Symantec is likely to become Norton, after its better-known consumer brand. Broadcom and Symantec/Norton will continue to share threat intelligence data; one of the potential benefits of having both consumer and business customers is the large base of endpoints through which new threats can be detected. Many of Symantec's consumer and enterprise products were different, and this will also limit any impact.

The deal has broader implications for the longer term though. For companies that do not target large enterprises with the same core product set (endpoint security, web security and DLP), competition will reduce as will competition for spend by small and medium-sized businesses. However, Broadcom is likely to compete more aggressively with security companies that target the same products and enterprises as Broadcom and its sales team will be better able to position its products.

Addendum: Broadcom announced that it had sold a division of Symantec, Cyber Security Services, to Accenture, on 7 January 2020. The division employed around 300 people (out of around 4000 for Symantec) and provides managed services, including threat monitoring and analysis, to large organisations. The sale of the services unit fits with Broadcom's overarching strategy for Symantec as it helps to reduce the complexity of the Symantec's business. We also assume that the sale will help to boost Symantec's margin, as the managed services offered by the Cyber Security Services unit was likely to be lower margin than that of the products business.

**Questions?**

Please feel free to contact Tom Rebbeck, Research Director, Research at tom.rebbeck@analysysmason.com

# Cyber security research programme

## Our research focuses on helping our customers sell security solutions to small and medium-sized businesses, an underserved market

### The importance of the SMB security market

The market for cyber security solutions is growing rapidly. We forecast that worldwide business spend on these services will grow from USD57.5 billion in 2018 to USD92.3 billion in 2023 (at a CAGR of 9.9%).

SMBs are core to this growth opportunity. SMBs are often underserved by security vendors, many of which focus on large enterprises instead. However, SMBs face many of the same risks as large enterprises; indeed the impact of a security breach can be greater for smaller organisations.

### Overview of the subscription

A subscription includes:

- Access to all of our published research, including forecast reports, survey data, trackers, strategy reports and market commentary.
- Access to our analysts. Included in the subscription is an unlimited number of enquiry calls with our analysts.

### Why our research is different

The key differentiators of our research are our focus on:

- the SMB (up to 1000 employees) market segment
- go-to-market strategies and issues. We also cover technology, but are most interested in how vendors sell and support security solutions aimed at the SMB market
- Providing strategy support. Our research can help with marketing, but in keeping with our background as a strategy consulting firm, our key aim is to help our customers improve their performance.

### Who our research is aimed at

The Cyber Security research programme is designed to help all parties interested in selling to the SMB market, including:

- security vendors,
- other technology services vendors that participate in the cyber security market
- telecoms operators.

[1] Our survey was conducted in Australia, China, France, Germany, India, Indonesia, Saudi Arabia, South Africa, the UK and the USA.

| | Areas covered | Example Material |
|---|---|---|
| Market forecasts | Key cyber-security solution areas, including endpoint, mobile, network and cloud security. | Regional 5-year forecasts (e.g. for the Western Europe and Developed Asia-Pacific regions). |
| Survey reports | Adoption of security solutions, as well as spend and planned spend on them, and security-related incidents, challenges and plans. | "Cyber-security trends in high- and middle-income countries" and "Cyber-security-related views, incidents and challenges". |
| Strategy reports | Differentiators, route-to-market approaches, opportunities for security vendors and operators. | "Cyber-security services for SMEs: opportunities for operators". |
| Vendor profiles | Overviews of vendors' strategies and our assessment of their strengths and weaknesses. | Vendor profiles of Barracuda Networks, CyberArk, McAfee and Panda Security. |
| Trackers and market commentary | Revenue trends, M&A activity and key developments in the cyber-security market. | Quarterly tracker of M&A activity in the cyber-security market; commentary on the Thoma Bravo's acquisition of Sophos. |

Learn more about our Cyber Security research programme at analysysmason.com/cyber-security

analysys mason

## Stay connected

You can stay connected by following Analysys Mason via Twitter, LinkedIn, YouTube or RSS feed.

@AnalysysMason

linkedin.com/company/analysys-mason

youtube.com/AnalysysMason

analysysmason.podbean.com