RESEARCH

analysys mason

CYBER SECURITY:

SELLING TO SMALL AND MEDIUM BUSINESSES

VOLUME II

Contents

Introduction

Welcome to our second collection of articles focused on cyber security, with a particular focus on the small and medium-sized business (SMB) market (that is, organisations with up to 1000 employees).

We believe that SMBs occupy an exciting area of the cyber-security space; indeed, such organisations are increasingly aware of the risks that they face if they are not adequately protected against cyber threats. Also, this segment of the market is rapidly growing; we forecast that SMBs' spend on cyber security worldwide will grow from USD57 billion in 2020 to USD90 billion in 2025.

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

- **COVID-19-related remote working is driving growth in SMBs' use of and spending on cyber-security solutions.** This article discusses our recently updated business cyber-security market forecasts, including the expected changes in the importance of different routes to market.
- **Vendors of cyber-security solutions need to change their approach to benefit from the operator channel.** In this article, we talk about what operators that sell cyber-security services to SMBs expect from their vendor partners, and how these partners could make themselves more attractive for co-operation.
- **Telecoms operators rated Fortinet as the best security vendor for the SMB market.** We surveyed 34 operators worldwide in 2H 2020 and asked them about their security strategies and vendor partners for the SMB market. This article explores operators' plans in this field, as well as their assessments of different vendors' strengths and weaknesses.
- **Palo Alto Networks is emerging as the lead vendor in the competitive network security market.** This article discusses the trends in the financial and operational metrics of four market-leading vendors that are mainly focused on providing network security solutions (Check Point, Cisco, Fortinet and Palo Alto Networks).
- **Business survey 2020: the COVID-19 pandemic will accelerate the cyber-security spend of SMBs in the USA.** We surveyed 400 SMBs in the USA in April and May 2020 to assess how the COVID-19 pandemic will affect (and is affecting) their demand for IT services. This article, which is based on results from this survey, examines the pandemic's impact on SMBs' adoption of cyber-security solutions and their related plans.

Analysys Mason helps clients in all geographies and parts of the value chain to develop their approach to the cyber-security market through our consulting services, as well as through our research. Our assignments range from rapid reviews of existing plans to full strategy development. Please contact us for more details on our subscription 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
Partner, Research at
tom.rebbeck@analysysmason.com

COVID-19-related remote working is driving growth in SMBs' use of and spending on cyber-security solutions

Eileen Zimbler, Senior Analyst, Research

Small and medium-sized businesses (SMBs) worldwide spent over USD57 billion on cyber-security solutions in 2020 and Analysys Mason forecasts that the SMB security spend will reach USD90 billion by 2025. This growth is being driven by SMBs' escalating dependence on cyber security to help to protect their customers' data, guarantee business stability, support digitalisation plans and protect the rising number of users on their corporate networks. All of these issues are becoming increasingly intensified and more difficult to manage as firms continue to struggle with the COVID-19 pandemic.

Businesses have experienced an increase in the number of data security attacks since the initial outbreak of COVID-19, and there has been a dramatic rise in the number of employees working from home. Many SMBs are reporting that at least some portion of their workforce will never return to a traditional office setting. This will make it challenging for IT departments to control who is using company PCs while they are in employees' homes, and what they are being used for. Analysys Mason recently conducted a survey of over 1800 SMBs regarding the impact that the COVID-19 pandemic has had on their business. Respondents expect that there will be a 54% increase in the proportion of staff that work from home post-crisis compared to the share that worked from home prior to the pandemic.[1]

Growth in security spending by small businesses will outpace that from other segments during 2020–2025

SMBs accounted for 52% of the USD110 billion spent on cyber-security solutions by businesses worldwide in 2020, and their share is expected to increase to 55% by 2025 (Figure 1). Analysys Mason estimates that the total spend on security-related solutions worldwide will reach USD165 billion by 2025, rising at a CAGR of 8.4% per year over the forecast period.

Security spending by small businesses (SBs; 0–99 employees) is projected to grow more quickly than that of any other business segment, at a rate of 10% annually throughout the forecast period. Spending by medium-sized business (MBs; 100–999 employees) is expected to increase by 9.1% year-on-year during the same timeframe. Large enterprises (1000+ employees) currently account for almost half of the total security spending worldwide, but the growth of this spending will be the slowest (6.9% per year throughout the forecast period). SMBs' spending on cyber-security is growing more rapidly than that of large enterprises because many of them are adopting a range of security products for the first time, partly in response to the need to support increased levels of remote working. Large enterprises already have more established infrastructure and security solutions to support remote working.

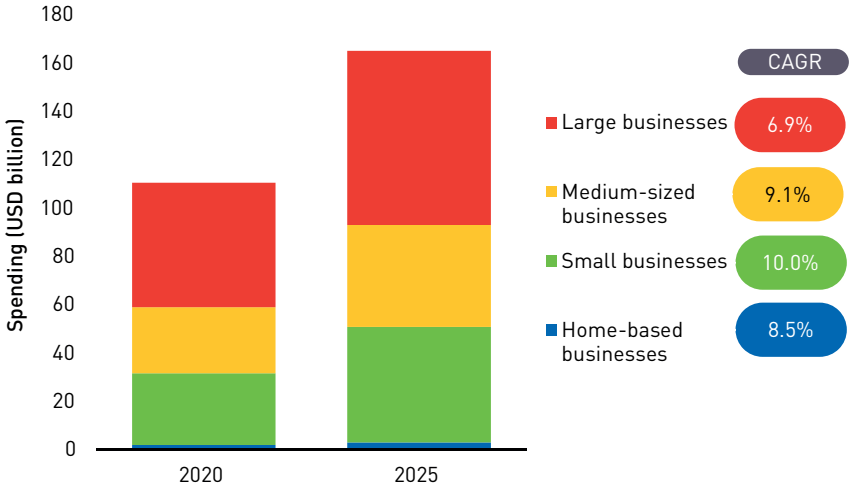


FIGURE 1: SECURITY SPENDING BY BUSINESS SEGMENT, WORLDWIDE, 2020–2025 [SOURCE: ANALYSYS MASON, 2021]

SMBs' cyber-security investments are being heavily influenced by ever-increasing concerns about security breaches, particularly as firms contend with WFH issues and changing operational conditions due to extended COVID-19-related restrictions. About 46% of SMBs reported that they have either started using cyber-security solutions for the first time, or have increased their usage since the initial outbreak of COVID-19.1 Over three quarters of SMBs surveyed plan to increase or maintain their current level of cyber-security usage. The majority (almost 8 out of 10) of SMBs we spoke to reported that they anticipate spending similar or greater amounts on cyber-security solutions in 2021 as they did in 2020.

SMBs' security spending with MSPs, SIs and telecoms operators will grow rapidly, but resellers and VARs will still remain important

Where SMBs buy cyber-security solutions from is heavily influenced by how much support they need to secure an increasingly remote workforce. We expect that an increasing number of businesses will look to outsource security due to their rising security needs and lack of in-house cyber-security resources. Indeed, 75% of SMBs surveyed reported that it would be helpful or very helpful if their IT/telecoms suppliers would upgrade their security solutions to cover new problems in the coming year (such as working from home, collaboration and BYOD policies). SMBs' security spending with MSPs and systems integrators (SIs) is expected to grow by 13% per year over the forecast period, from USD20 billion in 2020 to USD37 billion in 2025 (Figure 2).

Telecoms operators' direct sales represented just 5% of SMBs' spending on security in 2020, but this figure under-represents operators' role. A much larger share of security sales will come from telecoms operators' reseller partners (captured in our reseller and VARs category). The share of operators' direct sales will increase rapidly throughout the forecast period as they look to bundle security more closely with connectivity products. SMBs tend to rely on their telecoms providers as longstanding and trusted partners. Indeed, 44% of SMBs providing mobile connectivity for their employees reported that bundled mobile security is a very important aspect of their mobile service.[1]

Vendors should focus on the SMB segment and should support telecoms operators

Vendors should look to increase their focus on the SMB market relative to that on the large enterprise market. Spending in all segments will grow, but that in the SMB market will increase more quickly than that in the large enterprise segment. The move to working from home, accelerated by the pandemic, should encourage vendors to consider how well-suited their products are to this working environment. Security vendors need to offer remote installation for SMBs' employees that are currently working from home, as well as ongoing security training and support for these remote workers.

Security vendors should consider how they can best support the telecoms operator channel. It is the fastest growing channel in terms of spending, but, as we have discussed before, telecoms operators are not always well-served by security vendors.

[1] Analysys Mason's business survey on the impact of COVID-19 on SMBs worldwide in 1Q 2021, n = 1870.

[2] Note that the chart represents the channel that sells the service to the business. If a vendor sells a product through an MSP, the sale is captured under 'MSPs and SIs'. If a security product is supplied by a telecoms operator, but sold by a reseller, this sale is captured in the 'resellers and VARs' category.

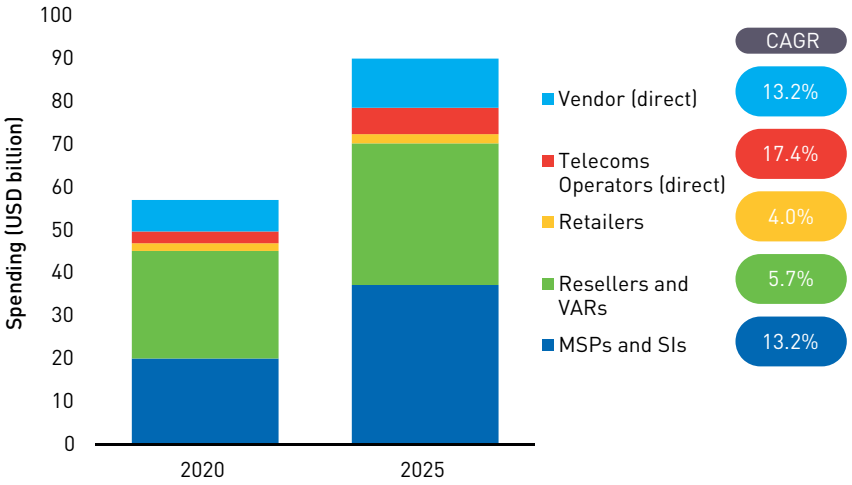
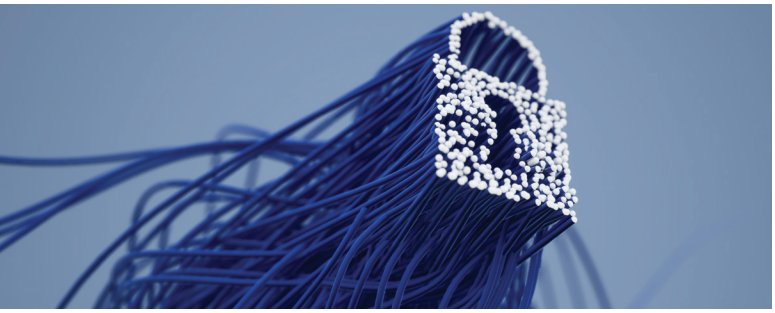


FIGURE 2: SMB SECURITY SPENDING BY ROUTE TO MARKET, WORLDWIDE, 2020–2025[2] [SOURCE: ANALYSYS MASON, 2021]

Questions?
Please feel free to contact Eileen Zimbler, Senior Analyst, Research at eileen.zimbler@analysysmason.com

Vendors of cyber-security solutions need to change their approach to benefit from the operator channel

Tom Rebbeck, Partner, Research



Operators provide an attractive route to market for vendors of cyber-security solutions: they have a large customer base, and bundling security products with connectivity is a logical move. Operators also have ambitious plans to expand their security propositions. However, vendors need to do more to benefit from this channel – operators require different types of support from other partners, a point that few vendors seem to recognise.

Operators are expanding their portfolios

We surveyed 34 telecoms operators in 3Q 2020 about their plans and activities in the small and medium-sized business (SMB) security market.[1] Figure 1 shows the products and services that operators offer and plan to offer. The plans should be treated with caution because they may mix aspirations with more solid plans. However, the direction of the results is evident; telecoms operators are expanding their portfolios. Existing propositions are dominated by network security products, such as firewalls and DDoS protection. Fewer operators offer endpoint or mobile security solutions, but many are planning to add these in the future.

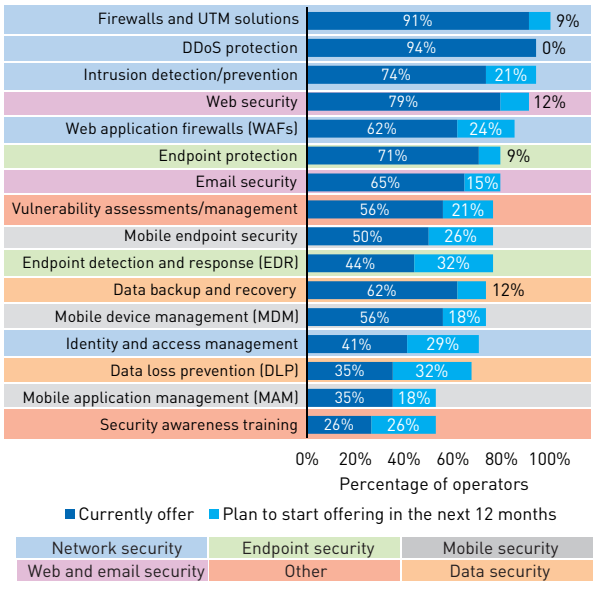
These findings have implications for vendors. Operators are already well set for firewall solutions. Each operator on our panel works with 2.4 network security vendors on average. Vendors that focus on this space will struggle to add themselves to the list.

Operators will be looking for partners to provide other solutions, such as endpoint detection and response, which 32% of our panel want to add, and mobile endpoint security (26%). The prospects of partnering with operators are brighter for security vendors with these products in their catalogue.

More operators are entering the security market

Security vendors should not just concentrate on operators that are already involved in the security market. More operators are launching security services. Figure 2 provides details of operators that announced significant expansions of their security propositions in 2020. Other operators also have plans, as yet unannounced, to enter or significantly expand their presence in the security market.

It is obvious why these operators have these plans. The market for security services is growing strongly – we expect SMBs' spending on security services to grow at around 10% annually for the period 2020–2025. Operators already have a customer base to sell services to and a close relationship exists between connectivity and security products.



Question: Which of the following security solutions (or services) do you currently offer to SMBs (and plan to start offering to SMBs in the next 12 months)?; n = 34.

FIGURE 1: OVERVIEW OF OPERATORS' CURRENT AND PLANNED SECURITY PORTFOLIOS FOR SMBS [SOURCE: ANALYSYS MASON, 2021]

SMBs are also open to purchasing security solutions from telecoms service providers, especially if they are satisfied with the core connectivity products. Well over half of SMBs would consider their telecoms operator as a supplier of security services if they were satisfied with the core connectivity offering, according to another of our surveys.

Operators are an attractive route to market for security vendors

Telecoms operators provide an attractive route to market for security vendors, but vendors need to change to better serve it. In our survey of operators, we asked how security vendors could improve their offerings. Ease of use of solutions was the most important issue for operators. Nearly two-thirds of respondents identified this as a top-3 priority. A vendor that can make its solutions easier to use, and can demonstrate this to operators, would have a clear advantage. Profitability inevitably was identified as another important area for improvement – a top-3 priority for 62% of operators.

In contrast, ease of doing business and marketing support were ranked the least important by respondents. Operators already have sufficient marketing resources of their own and are well-equipped to work with external vendors (for example, they have large procurement teams). It is likely that telecoms operators differ from security vendors' other channel partners (such as resellers and managed service providers (MSPs)) in these respects.

We also asked the operators for a single suggestion for what security vendors could do to help them. The most common suggestions related to support. Operators feel that vendors do not consider them to be a distinct type of channel with unique requirements. Vendors need to do more to understand how operators sell to SMBs, and how operators' requirements are different to those of their other channel partners.

Operators are also not impressed by the pricing models offered by many of the security vendors. They would like to see vendors offer more flexible pricing models, such as a pay-as-you-grow, rather than insisting on high minimum value or volume commitments.

Fortinet is an example of a vendor that does well in these respects. It was extremely well regarded by operators. It is also notably a key partner for both Vodafone Idea and Etisalat, two of the operators in Figure 2.

Operators are well placed to help security vendors to reach new customers but they have different requirements from other channel partners. Vendors need to respect and understand this, if they are to win share through the operator channel.

For more results from our survey, see our reports *Cyber security in the SMB market: survey of telecoms operators* and *Analysis of vendors of cyber-security solutions for SMBs: telecoms operator survey.*

[1] We define SMBs as companies with up to 1000 employees.

Operator	Plans announced in 2020	Details
Etisalat	Acquired the security firm Help AG	Etisalat completed its acquisition of the UAE-based security service provider Help AG in February 2020.
Fastweb	Using an acquisition to expand the set of security services that it will offer to customers	Fastweb took a 70% stake in security firm 7Layers in October 2020. In particular, Fastweb will expand its threat management and intelligence services.
Liquid Telecom	Launched a new Cyber Security unit	It is developing end-to-end managed security solutions in partnership with Cyber Risk Aware, Logicalis, Microsoft and Netskope.
Vodafone Idea (Vi)	Expanded its managed services offering with Fortinet	Vi Business, the business unit of Vodafone Idea, is building a set of managed network security services in partnership with Fortinet.

FIGURE 2: TELECOMS OPERATORS THAT ANNOUNCED SIGNIFICANT PLANS FOR SECURITY IN 2020 [SOURCE: ANALYSYS MASON, 2021]

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

Telecoms operators rated Fortinet as the best security vendor for the SMB market

Igor Babić, Senior Analyst, Research

Telecoms operators rated Fortinet as the best security supplier for the small and medium-sized business (SMB) market (organisations with up to 1000 employees) in Analysys Mason's survey. Other large vendors with a strong heritage in network security (Palo Alto Networks, Cisco and Check Point) also scored highly, as did F-Secure, Sophos and Microsoft.

Telecoms operators are looking to increase their presence in the security market. The 'big four' network security players look best-placed to help them given their popularity. F-Secure, Sophos and Microsoft are also well-positioned. Other vendors will need to increase operators' awareness of their brands and products if they are to compete more effectively for operators' business and for access to their existing large SMB customer bases.

We asked 34 operators for their opinions about security suppliers

We surveyed 34 telecoms operators during July–October 2020 to find out more about their security strategies for the SMB market. Respondents ranged from some of the world's largest telecoms operators to small specialists that focus on the business market. The survey was carried out worldwide: we received input from operators in the Americas, the Middle East, Asia–Pacific and across Europe.

We asked respondents for their views of security solution providers and for suggestions on how these providers could improve. We also asked about the operators' own security products and plans. The results are captured in our report *Cyber security in the SMB market: survey of telecoms operators.*

Telecoms operators' overall impressions of security vendors were clear: the largest four vendors with a background in network security (Fortinet, Palo Alto Networks, Cisco and Check Point) received the highest scores (Figure 1). The high scores earned by these players are based on direct experience; many of the operators surveyed already work with them. For example, Fortinet provides SMB security products to 26 operators in our panel, and Cisco works with 24. The vendors' focus on network security is also likely to have played a role in their strong performance. Indeed, products such as firewalls have been offered by telecoms operators for a long time and often form the base of operators' security portfolios.

Fortinet scored highly in all areas of assessment

Figure 2 shows the scores for overall impression, ease of doing business, pricing and portfolio and product quality for the seven leading security suppliers in Figure 1. The portfolios of these seven, though often overlapping, are different and so the scores will reflect a range of factors. For example, we did not ask operators to compare individual product lines from vendors. Some caution is therefore needed when reviewing the results.

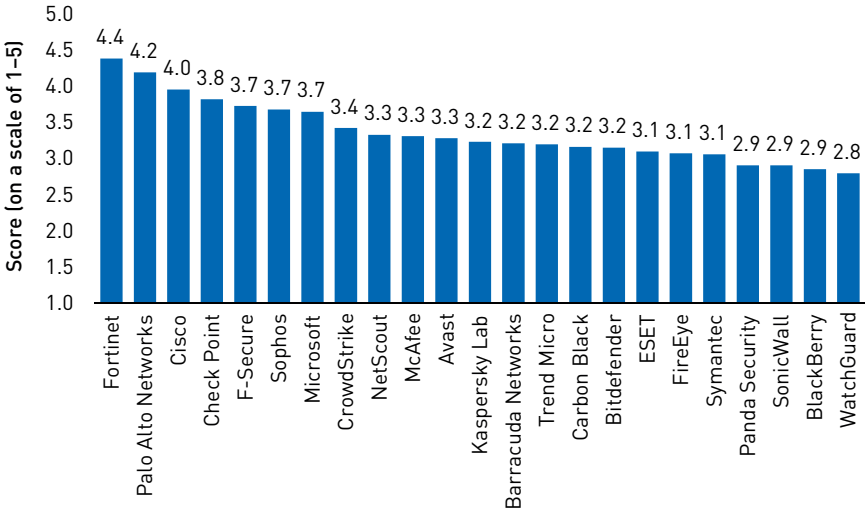


FIGURE 1: TELECOMS OPERATORS' RATINGS OF SECURITY VENDORS IN TERMS OF OVERALL IMPRESSION, 2020[1]
[SOURCE: ANALYSYS MASON, 2021]

- **Fortinet** received higher scores than any other vendor in all areas of assessment. The consistency of Fortinet's results stands out: out of over 100 ratings, it received a single score of 2 (for pricing) and nothing lower. More than 80% of its scores were a 4 or a 5.
- **Palo Alto Networks**'s overall score was almost as good as Fortinet's, but it received a number of lower ratings in other areas, particularly for pricing (though the correlation between pricing and overall impression is weak at best). The perception of being expensive may be costing it business; only 5 operators named it as their primary SMB network security provider, compared to 13 for Fortinet.
- **Cisco**'s results mimic those for Palo Alto Networks, though it is seen as slightly harder to do business with, and it received a slightly lower score for pricing.
- In contrast, **Check Point** did better on pricing than Cisco and Palo Alto Networks, and is slightly easier to do business with, but these factors were not enough to lift its overall score.
- **F-Secure** is a relatively small company. It is easily the smallest of the top-seven providers; its 2019 revenue was USD244 million, only around half of which came from business customers. However, it has several operator customers (seven of the panel sell F-Secure's solutions to SMBs) and is well-regarded by them. More than a third of its ratings were a 4 or 5; it only received a 2 twice, and never received a 1.
- **Sophos**, like Fortinet, received a very consistent set of results. It received a single rating of 2 (for pricing), and nothing lower. Just over half of its ratings were a 4 or a 5.
- **Microsoft** only outscored Sophos in one area: product portfolio and quality. However, even here there is potential for improvement because it only received a single score of 5 in this category. Overall, Microsoft is liked but not loved by operators; it received more than five times more scores of 4 than of 5.

The leading seven vendors are well-placed to do business with operators; others have work to do

Operators have ambitious plans for security. Major operators such as AT&T, Orange and Telefónica have established separate security divisions, often supported by large acquisitions. Orange is targeting EUR1 billion in annual security revenue by 2022 (from around EUR700 million today) and it is not alone in having ambitious revenue growth targets.

The leading seven vendors look well-placed to support operators in realising their SMB security plans. Other suppliers have work to do. Many endpoint security providers struggle to differentiate themselves or their offers. They failed to generate strong feelings (either positive or negative) from our operator panel. Smaller vendors also often failed to create a profound impression on the operator community, though it is possible for them to break into the operator market, as the example of F-Secure shows.

1 Question: "Thinking only about security solutions for SMBs, please score vendors on the following: overall impression"; n = 34. Scores were given on a scale of 1–5, where 1 was the worst/among the worst and 5 was market leading/among the leaders. Vendors with fewer than 9 responses are excluded.

2 Question: "Please score vendors on the following: overall impression, ease of doing business, pricing, product portfolio and quality"; n = 34. Note that each vendor has under 34 responses; respondents did not enter a score if they did not have an impression of the vendor. Scores were given on a scale of 1–5, where 1 was the worst/among the worst and 5 was market leading/among the leaders. F-Secure only received 8 responses for 'ease of doing businesses'.

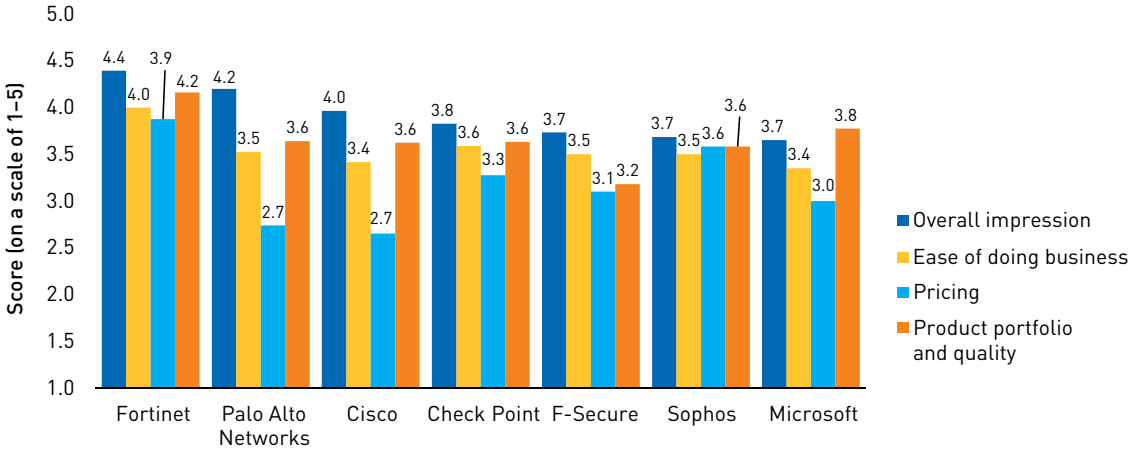


FIGURE 2: TELECOMS OPERATORS' RATINGS OF THE BEST-PERFORMING SECURITY VENDORS, 2020[2]
[SOURCE: ANALYSYS MASON, 2021]

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

Palo Alto Networks is emerging as the lead vendor in the competitive network security market

Igor Babić, Senior Analyst, Research

The revenue of nearly all major, publicly traded cyber-security vendors increased year-on-year in 1Q 2020.[1] This article explores the trends in the financial and operational metrics of the market-leading network security vendors (Check Point, Cisco, Fortinet and Palo Alto Networks). The data presented here draws upon Analysys Mason's Cyber-security vendors' revenue tracker.

Palo Alto Networks has overtaken Cisco as the largest network security vendor, in terms of revenue, thanks to sustained investment

Palo Alto Networks's quarterly revenue in 1Q 2015 was USD234.2 million; this approached USD900 million in 1Q 2020 (Figure 1). The vendor's sustained strong revenue growth has been supported by significant investment in sales and marketing activities,[2] as well as 11 acquisitions (on which the vendor spent nearly USD2.5 billion). Cisco's accelerated revenue growth in 2H 2018 and 2019 was also propelled by M&A activity, most importantly its acquisition of Duo Security in October 2018. Fortinet, too, has performed well; its revenue growth in 2H 2019 and 1Q 2020 was faster than Palo Alto Networks's, largely thanks to the popularity of its combined firewall and SD-WAN offering among businesses. Check Point's revenue also grew consistently between 2015 and 2020, but at a much slower pace than that of its main competitors. Its lack of SD-WAN capability and no major M&A activity explains this slower growth. Check Point is the only one of the vendors in Figure 1 that does not have its own SD-WAN offering.

Check Point remains more profitable than Fortinet and Palo Alto Networks

Check Point consistently turns a profit. Its operating margin was 44% in 2019, and was between 44% and 53% in every quarter in 2017, 2018 and 2019. Fortinet also turned a profit in 2019, and its operating margin continued to grow (from 7% in 2017 to 20% in 1Q 2020). Conversely, Palo Alto Networks generated an operating loss of USD133.3 million in 2019 (equal to 15.1% of its revenue during the year, and nearly 2.5 times higher than the loss it generated during 2018). Its accumulated loss surpassed USD1 billion in 2019 and its free cash flow in 1Q 2020 was weaker than Check Point's and Fortinet's (Cisco does not report information on the profitability of its security business). Palo Alto Networks could find itself in a weaker position than its smaller rivals if there is a major downturn in the US economy as a result of the COVID-19 pandemic, largely because of its lack of profitability and its high level of exposure to the US market (nearly two thirds of its revenue comes from the USA).

However, Palo Alto Networks spent the most out of the three vendors on both research and development (R&D) and sales

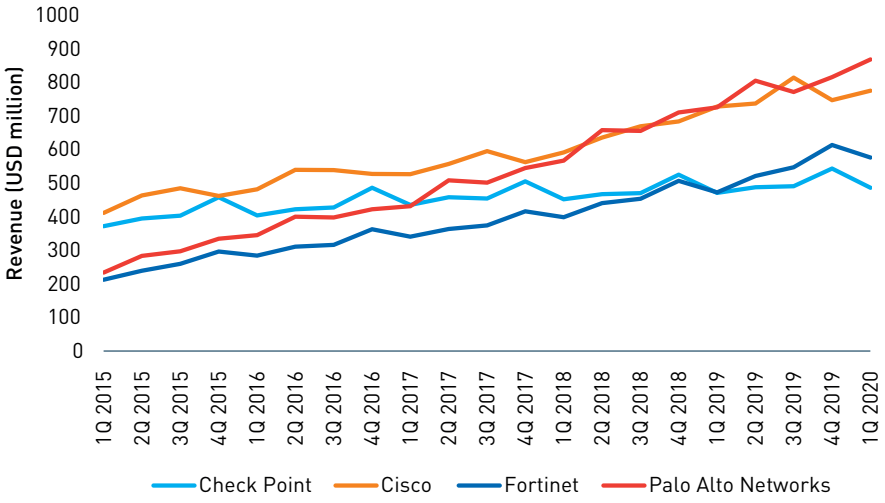


FIGURE 1: REVENUE OF THE FOUR MARKET-LEADING NETWORK SECURITY VENDORS ('SECURITY REVENUE' IN THE CASE OF CISCO), 1Q 2015–1Q 2020[3] [SOURCE: ANALYSYS MASON, 2021]

and marketing (S&M) in 2019 and 1Q 2020 (Figure 2). Its spending on R&D was not only higher as a proportion of revenue than Check Point's and Fortinet's in 2019, but it was also 33% higher than the other two vendors' combined expenditure in absolute terms. Palo Alto Networks's headcount also grew faster than its competitors': Check Point added around 130 people to its workforce between the beginning of 2019 and the end of March 2020, Fortinet added around 1600 and Palo Alto Networks added nearly 2200 employees during the same period (supported by the six acquisitions that it made in 2019 and 2020).

Other network security vendors are far behind the market-leading four in terms of scale, which is inhibiting their growth

The quarterly revenue of Barracuda Networks, Juniper Networks, SonicWall and WatchGuard, for example, is significantly lower than that of the four market-leading network security vendors.[6] Similarly to their larger counterparts, these vendors are also increasingly expanding their portfolios beyond network security in order to differentiate (for example, WatchGuard acquired Panda Security in June 2020).

However, they do not have the same means as their larger counterparts to provide financial support for channel partners and end customers during the COVID-19 pandemic. For example, Cisco is offering its customers an option to defer 95% of payments until 2021, and Palo Alto Networks has created a financial services arm to offer financing for multi-year engagements. The disparity between the market-leading vendors' financial might and that of certain private-equity-backed (particularly early-stage) vendors may enable Check Point, Cisco, Fortinet and Palo Alto Networks to acquire technology and market access (and therefore accelerate their growth) at discounted prices.

Palo Alto Networks has outgrown its main competitors by taking greater acquisition risks and accepting the negative impact of this on profitability. Check Point has lost ground, but its more-cautious approach to revenue growth may provide it with stability in the coming challenging economic climate.

[1] NortonLifeLock's revenue decreased by 48% year-on-year due to Symantec's sale of its Enterprise Security business to Broadcom. Other vendors that experienced a year-on-year decline in revenue are NetScout (–2%), Forcepoint (–6%) and Forescout (–24%).

[2] Palo Alto Networks's sales and marketing spending as a percentage of revenue were as follows: 51% (FY2017), 47% (FY2018) and 46% (FY2019). For comparison, Check Point's figures were 22% (FY2017), 25% (FY2018) and 26% (FY2019), and Fortinet's figures were 47% (FY2017), 43% (FY2018) and 43% (FY2019).

[3] The chart is based on calendar years rather than financial years. Check Point's and Fortinet's financial years coincide with the calendar year, while Cisco's and Palo Alto Networks's do not. February is taken to be the starting month of their calendar years for this chart.

[4] Cisco is excluded from this table because it reports a more-limited set of metrics related to its cyber-security business.

[5] Estimate. Check Point reported that it had 5152 employees at the end of 2019; in June 2020 it had over 5200 employees.

[6] Security revenue in the case of Juniper Networks.

Metric	Check Point (quarter ending 31 March 2020)	Fortinet (quarter ending 31 March 2020)	Palo Alto Networks (quarter ending 30 April 2020)
Revenue	USD486.5 million (+3.1% year-on-year)	USD576.9 million (+22.1% year-on-year)	USD869.4 million (+19.7% year-on-year)
R&D spending (as a percentage of revenue)	USD56.6 million (12%)	USD80.3 million (14%)	USD196.3 million (23%)
S&M spending as a percentage of revenue	27%	45%	45%
Operating profit (loss)	USD200.6 million	USD115.9 million	(USD56.5 million)
Percentage of revenue from outside the Americas	54%	58%	32%
Deferred revenue (as a percentage of quarterly revenue)	USD1349 million (277%)	USD2227 million (386%)	USD3371 million (388%)
Number of employees	5200[5]	7448	8049

FIGURE 2: SELECTED FINANCIAL AND OPERATIONAL METRICS FOR CHECK POINT, FORTINET AND PALO ALTO NETWORKS, LATEST FINANCIAL REPORTING QUARTER (END OF MARCH/APRIL 2020[4])
[SOURCE: ANALYSYS MASON, 2021]

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

Business survey 2020: the COVID-19 pandemic will accelerate the cyber-security spend of SMBs in the USA

Igor Babić, Senior Analyst, Research

Analysys Mason surveyed over 400 small and medium-sized businesses (SMBs) in the USA in April and May 2020 to assess how the COVID-19 pandemic will affect (and is affecting) their demand for IT services.[1] This article uses the results from this survey to examine the pandemic's impact on SMBs' adoption of cyber-security solutions and related plans.

Our survey results suggest that the move to working from home (WFH) has accelerated (and will continue to accelerate) the demand for security services among those SMBs that are still in business, even though a sizeable portion of the SMBs surveyed have had to close branch offices or stores (28%) and permanently lay off staff (11%).[2] The data shows that the increased use of security solutions is unlikely to only be temporary. Over a quarter of the SMBs surveyed anticipate spending more on security this year than they had originally planned, while only 7% of them plan to spend less.

SMBs' increased use of cyber-security solutions should translate into higher long-term adoption

44% of SMBs in the USA increased their use of cyber-security solutions in April/May 2020 and/or are planning to do so once 'shelter-in-place' regulations have been relaxed (Figure 1). This figure is higher for MBs than SBs because a greater portion of MBs than SBs had plans to increase their security spending in 2020 and MBs in the USA have been less severely financially affected by the pandemic than SBs (another finding of our survey).

The percentage of SMBs that have increased/plan to increase their use of cyber-security solutions does not vary drastically by vertical. SMBs that provide professional services (such as legal, marketing, accounting/tax and management consulting services) are the most likely to have increased (or plan to increase) their use of security solutions, while those that provide 'other services' are the least likely. These results reflect the importance of IT security to SMBs in various verticals.

93% of the SMBs that increased their use of cyber-security solutions in April/May 2020 (40% of all SMBs surveyed) plan to maintain this new level of use or increase it further once COVID-19-related restrictions are relaxed. Security vendors and their channel partners that started offering certain solutions free of charge at the beginning of the COVID-19 breakout should examine which solutions have been used the most by SMBs (where this is possible) to more effectively capitalise on these plans for increased use in the long term.

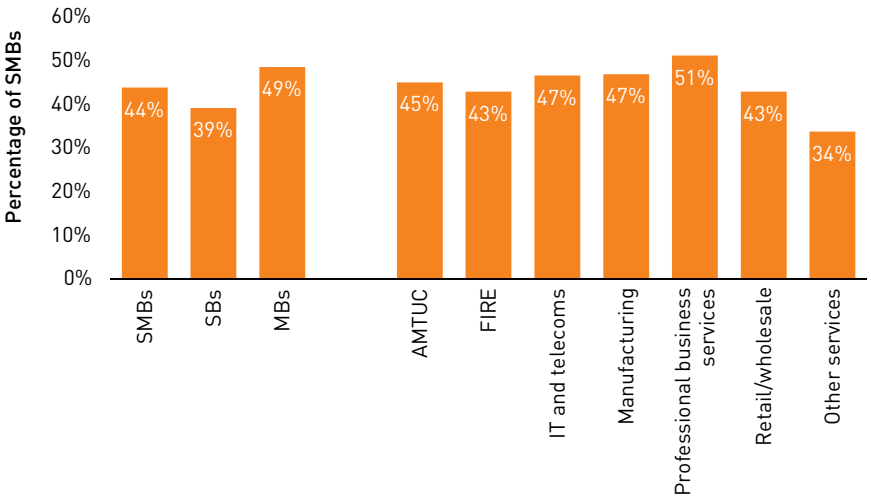


FIGURE 1: PERCENTAGE OF SMBS THAT INCREASED THEIR USE OF CYBER-SECURITY SOLUTIONS DURING THE COVID-19 PANDEMIC AND/OR ARE PLANNING TO DO SO ONCE 'SHELTER-IN-PLACE' REGULATIONS HAVE BEEN RELAXED, BY SMB SIZE AND VERTICAL, USA, APRIL/MAY 2020[3]
[SOURCE: ANALYSYS MASON, 2021]

Over a quarter of the SMBs surveyed anticipate spending more on cyber-security solutions this year than they had originally planned

Our survey results show that far more SMBs in the USA will increase their use of cyber-security solutions in 2020 than will decrease it. This is reflected in the changes to SMBs' security budget plans made in light of the COVID-19 pandemic (Figure 2) and represents an opportunity for vendors.

Figure 2 shows that 26% of SMBs in the USA plan to spend more on cyber-security solutions once COVID-19-related restrictions are relaxed compared to what they had planned to spend prior to the outbreak of the pandemic. This figure is higher for MBs than for SBs, and it varies notably by vertical. SMBs that deliver IT and telecoms and professional business services are the most likely to spend more than they had originally planned on security after restrictions are relaxed. The difference between the percentage of firms that plan to spend more and the percentage of firms that plan to spend less is the largest for these two verticals (33% and 25%, respectively), while it is only 3% for the AMTUC industry grouping. Security vendors and their channel partners should therefore prioritise targeting SMBs in the IT and telecoms and professional business services verticals in the USA in order to access SMBs' increased cyber-security budgets.

SMBs' changing attitude towards WFH will be one of the drivers of the increase in adoption of cyber-security solutions

71% of the SMBs surveyed intend to change their WFH policy once the COVID-19 crisis is over. This is especially true for larger SMBs; 50% of SMBs with 1–9 employees plan to make a change compared to 82% of SMBs with 250–499 employees. We expect that most businesses will support an increase in WFH in the long run if they can. This will create a sustainable demand for remote working solutions, many of which are provided primarily by security vendors.

Cyber security is more challenging to manage when employees work remotely and are widely distributed compared to when they are working in an office. We expect that this will drive a long-term, sustained increase in the demand for managed security services by SMBs. This is supported by data from the survey: 27% of SMBs in the USA anticipate spending more on managed IT services once the COVID-19-related restrictions are relaxed than they had originally planned, and only 9% of them plan to spend less. This, coupled with the increase in spending on cyber security that was discussed previously, should provide a sustainable revenue opportunity for security-focused managed service providers that are targeting SMBs in the USA.

[1] The sample of 404 firms was split equally between companies with 1–99 employees (small businesses (SBs)) and those with between 100 and 499 employees (medium-sized businesses (MBs)).

[2] The survey excluded firms that had gone out of business prior to April/May 2020, and those that had significantly cut back their operations were probably less likely to participate in it.

[3] AMTUC stands for agriculture, mining, transportation, utilities and construction; FIRE stands for finance, insurance and real estate; the 'other services' category includes admin/support services, repair and maintenance, waste management, healthcare, hospitality and other services not captured in the remaining six categories.

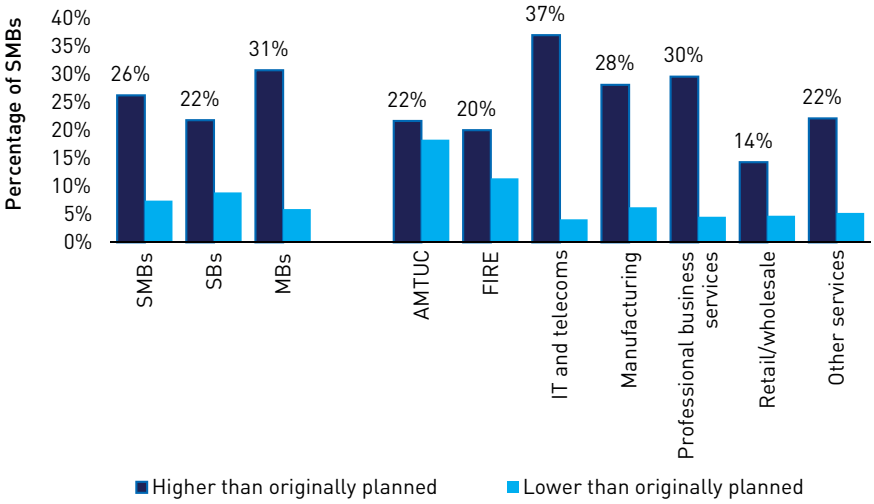


FIGURE 2: SMBS' PLANNED SPEND ON CYBER-SECURITY SOLUTIONS ONCE COVID-19-RELATED RESTRICTIONS ARE RELAXED RELATIVE TO THEIR PRE-COVID-19 PLANS, BY SMB SIZE AND VERTICAL, USA, APRIL/MAY 2020
[SOURCE: ANALYSYS MASON, 2021]

Questions?
Please feel free to contact Igor Babić, Senior Analyst, Research at igor.babic@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 and SMBs are at the core of this growth opportunity.

SMBs are often underserved by security vendors, many of which focus on large enterprises. However, while SMBs face many of the same risks as large enterprises, the impact of a security breach on them can be far more destructive.

Overview of the subscription

A subscription includes:

- **access to all of our of published research materials,** including forecasts, survey data and analysis, trackers, strategy reports and market commentary
- **access to our analysts** – an unlimited number of 30-minute enquiry calls with our analysts.

Why our research is different

The key differentiators of our research are our focus on:

- the SMB market segment (firms with up to 1000 employees)
- go-to-market strategies and issues – we also cover technology, but are most interested in how vendors sell to SMB and the support they provide for their solutions
- providing strategy support – our research can help with marketing, but we are a strategy consulting firm and our main aim is to help our customers make decisions that will improve their performance.

Who our research is aimed at

Our Cyber Security research programme is designed to help all parties that are interested in selling cyber security solutions to the SMB market, including:

- security vendors
- other vendors of technology services 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, web and email, mobile, data and network 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 "The impact of COVID-19 on SMBs in the USA".
Strategy reports	Differentiators, route-to-market approaches, opportunities for security vendors and operators.	"Approaches to providing security services to the mid-market: 12 telecoms operator case studies".
Vendor profiles	Overviews of vendors' strategies and our assessment of their strengths and weaknesses.	Vendor profiles of CrowdStrike, Sophos, Bitdefender, Avast, Acronis, Proofpoint, Barracuda Networks...
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 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 and YouTube.

linkedin.com/company/analysys-mason

@AnalysysMason

youtube.com/AnalysysMason

analysysmason.podbean.com