VansonBourne

The Future of Network Security

Sophos 2012 Network Security Survey

Sophos and Vanson Bourne surveyed 571 IT decision makers globally to gain a deeper understanding of how IT teams are responding to technology changes in network security.

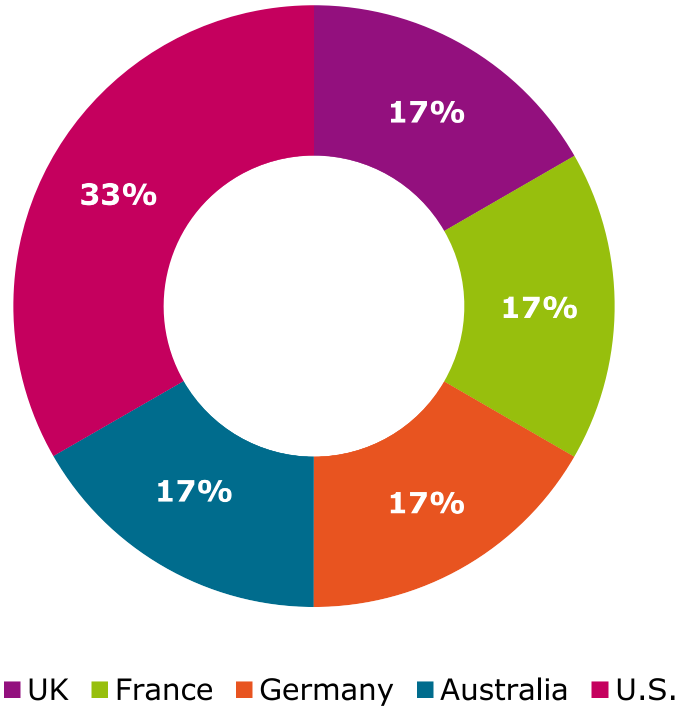
The survey focused on:

- Remote workers
- Wireless networks
- Network security challenges
- The future

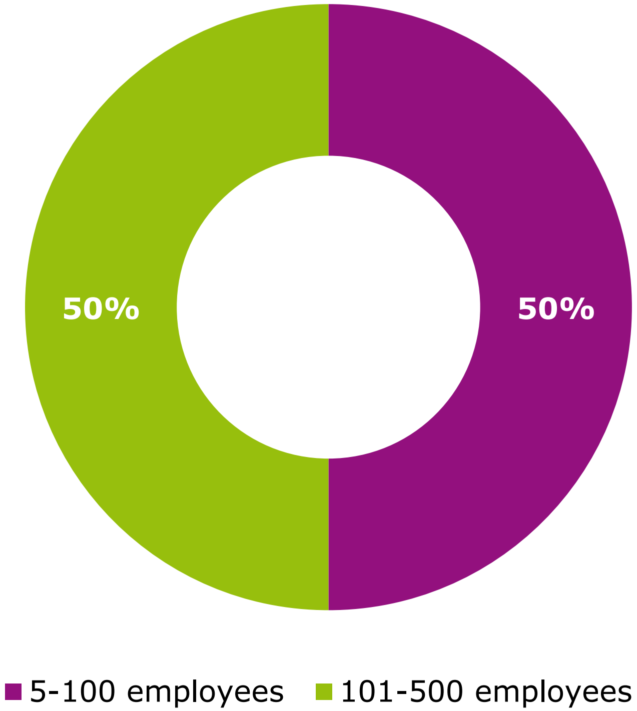
Demographics

We surveyed 571 IT decision makers from the U.S., UK, France, Germany and Australia.

Country



Company Size



Remote workers

What percentage of your employees work remotely?

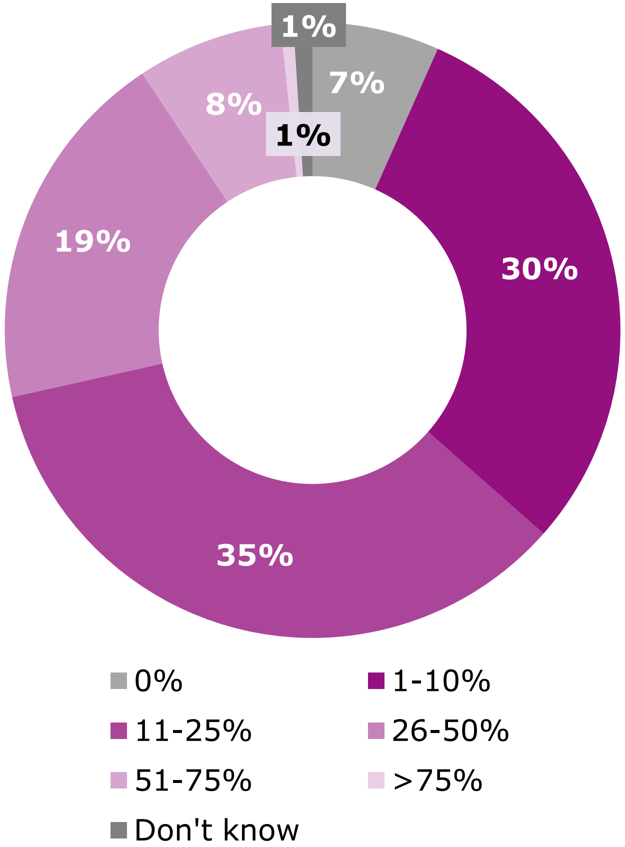


Figure 1a: Percentage of employees working outside central office(s) or at remote sites, i.e., branch offices, retail outlets, hotels

93% of SMBs have at least some remote workers. On average around 20% of all employees work remotely. Larger organizations (101-500 employees) are more likely to have remote employees (97%) compared to smaller ones with 5-100 employees (90%).

With such a high number of remote workers, it’s no surprise that IT departments have concerns around managing them.

On average almost a quarter of employees at U.S. SMBs work remotely, the highest among the countries surveyed.

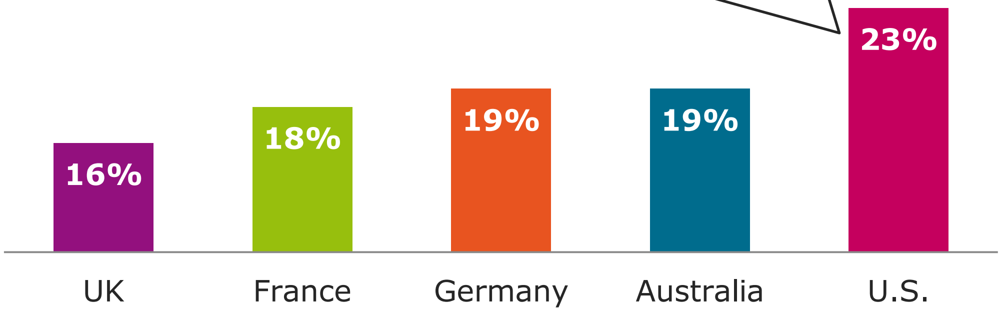
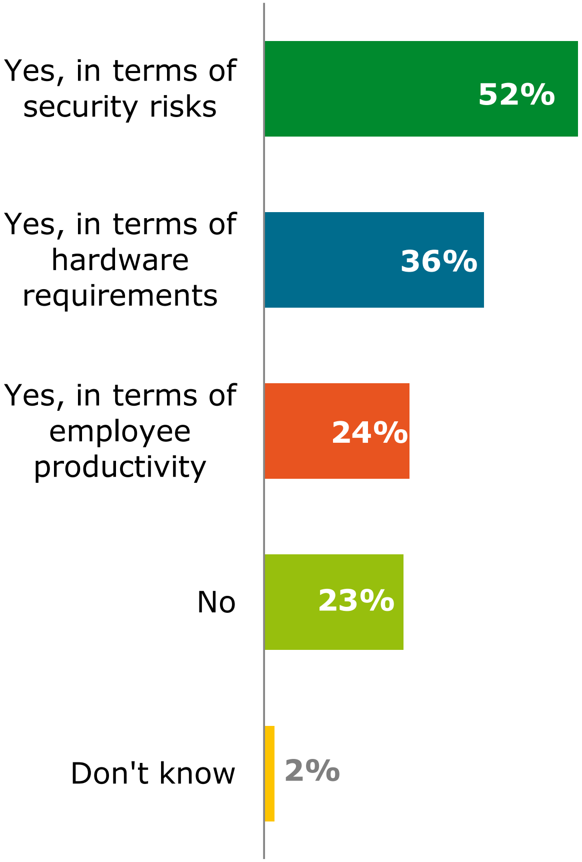


Figure 1b: Percentage of employees by country who work outside central office(s) or at remote sites

Are you concerned about supporting remote workers?



For 75% of SMBs, supporting remote working is an issue—most commonly in terms of security risks. More than half of SMBs are concerned about security risks from increased remote working.

Larger SMBs are more concerned than smaller ones about all three of these issues (security risks, hardware requirements and employee productivity).

While security risks are the most common issue in all countries surveyed, organizations in the U.S. and France are the most likely to be concerned.

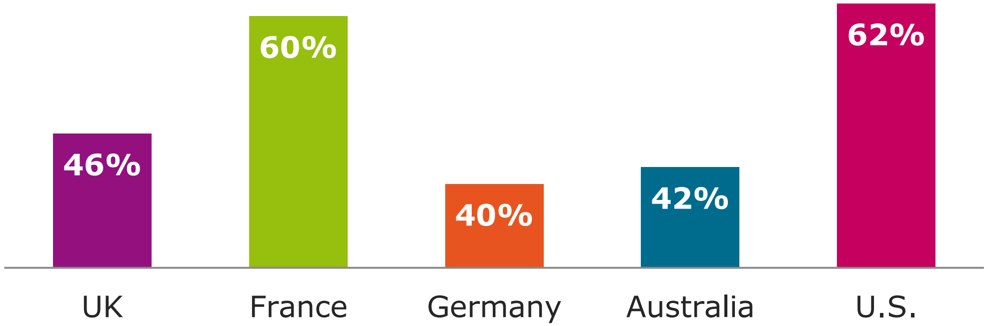


Figure 2a: Is supporting remote working, i.e., employees working from home/on the road, a growing issue for you?

Figure 2b: SMBs by country that believe supporting remote working is a growing issue in terms of security risks

What are the top challenges of securing remote sites?

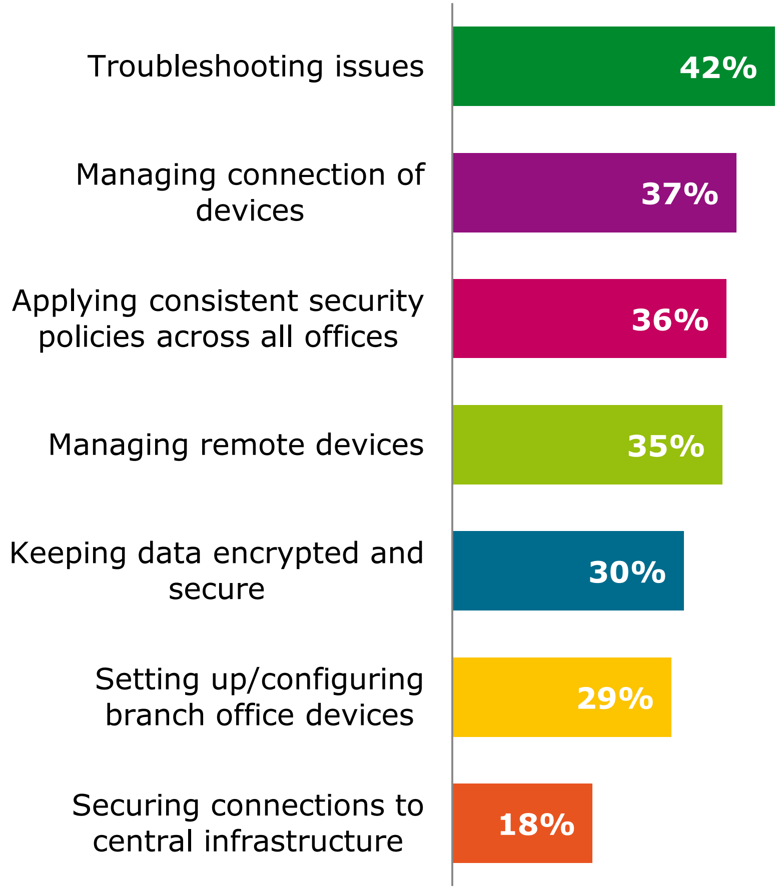


Figure 3a: Top IT challenges when securing and connecting remote sites

SMBs acknowledge a range of issues when it comes to securing and connecting remote sites. On average, respondents admitted that at least two of the issues listed in figure 3a affect them.

Their most common issue is troubleshooting, although opinion varies by country:

- Troubleshooting is the most common issue in the U.S. and UK (46% and 52% respectively)

- In France, the top answer is managing the connection of these devices (41%)

- In Germany, troubleshooting issues ties with applying consistent security policies across all offices (34%)

- In Australia, the top issue is "Managing remote devices" (45%)

Concerns about device management are a likely driver for IT security spending; 50% of those planning to increase their budgets also admit to concerns about managing remote devices.

Is securing and connecting remote sites a challenge?

Overall, 35% of IT decision makers at SMBs are concerned about managing remote devices. This varies by industry sector.

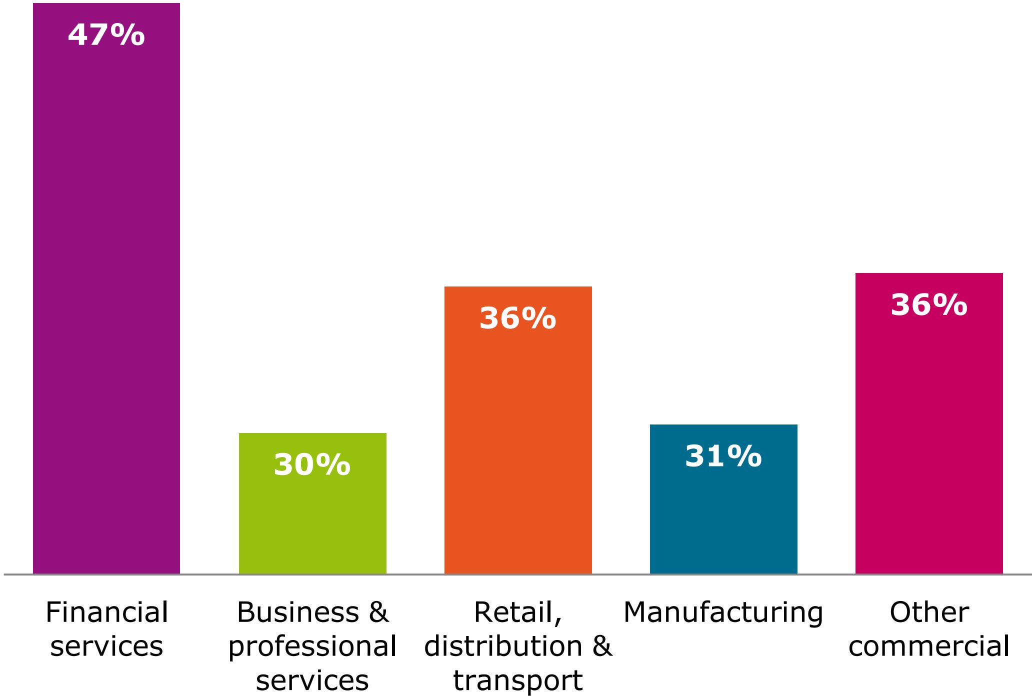


Figure 3b: SMBs by sector who say managing devices is a challenge when securing and connecting remote sites

The top two challenges are viewed almost equally by smaller SMBs, but larger ones view troubleshooting as a bigger issue.

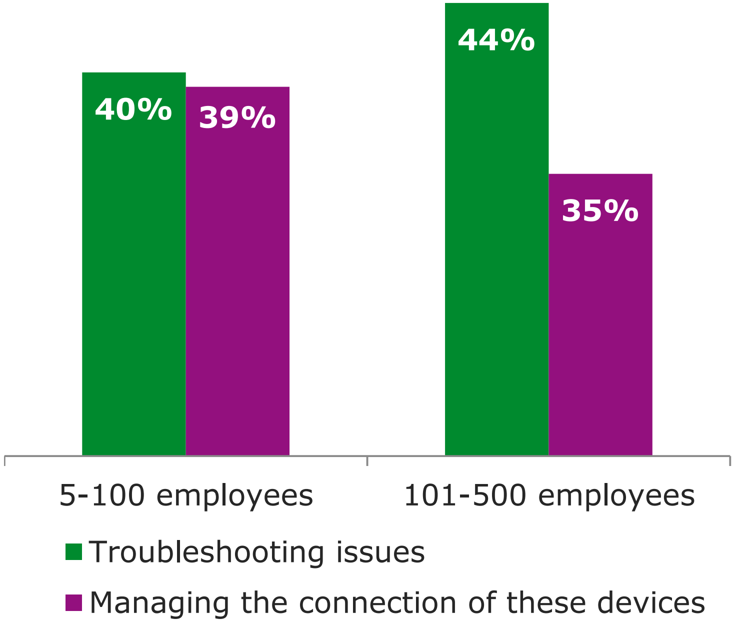


Figure 3c: SMBs by size: the top two challenges when securing and connecting remote sites

Wireless networks

How good is your Wi-Fi coverage?

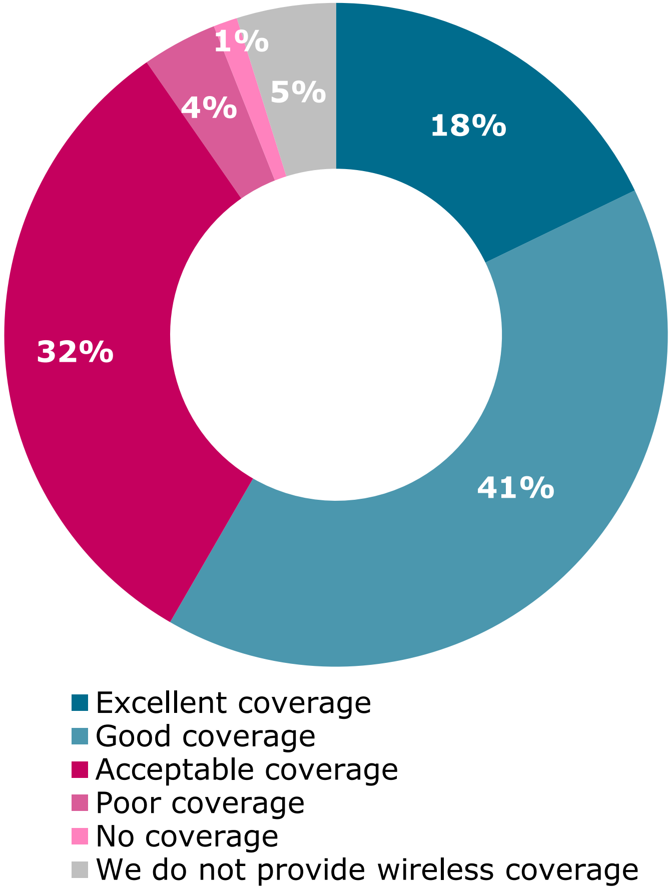


Figure 4a: How SMBs describe the wireless network coverage in their organization's offices

Fewer than one in five SMBs (18%) think that they have excellent wireless network coverage in their offices, while 37% feel their coverage is acceptable at best.

SMBs in the U.S. and UK are most likely to describe their Wi-Fi coverage as "excellent." And 74% of U.S. SMBs say their coverage is either "good" or "excellent."

And when looking at wireless coverage in relation to how easy managing multiple networks is, there's a clear connection.

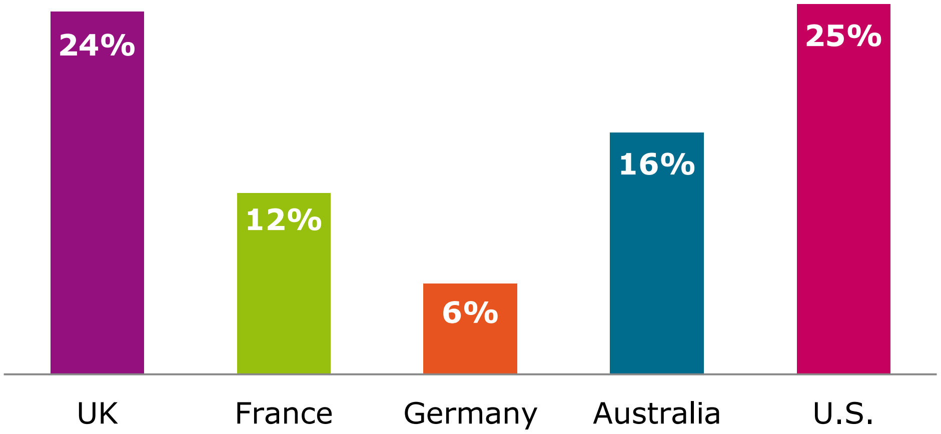


Figure 4b: SMBs by country that answered they have "excellent Wi-Fi coverage"

How easy do SMBs find managing multiple networks?

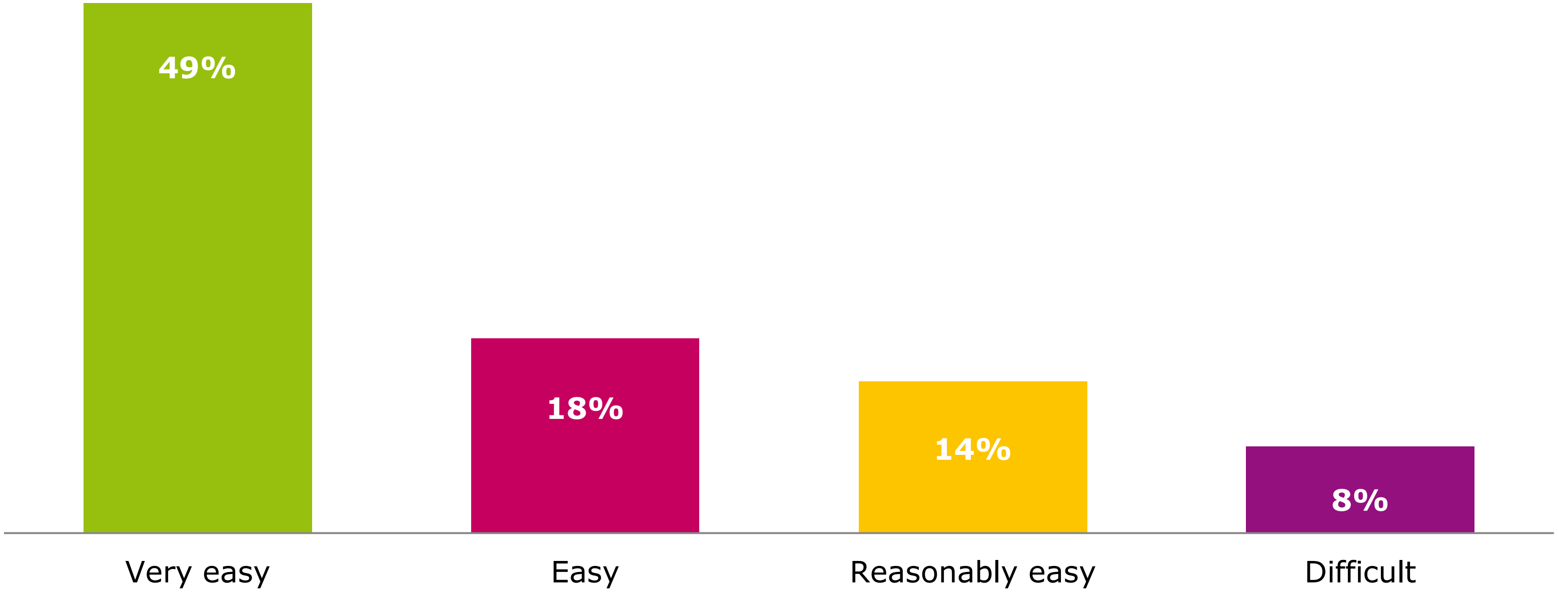
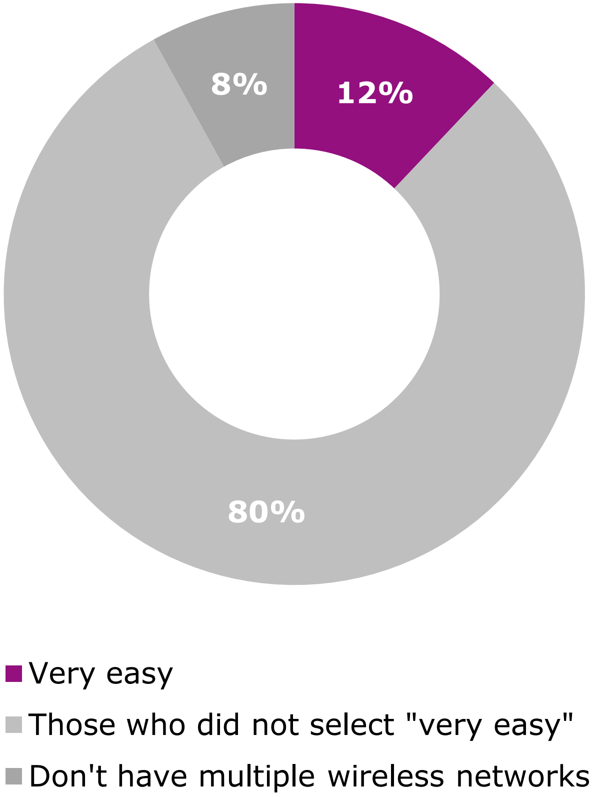


Figure 4c: SMBs that answered they have “excellent Wi-Fi coverage”

How difficult is managing multiple networks?



Just 12% of IT decision makers in SMBs find it very easy to manage multiple wireless networks; 80% experience some kind of difficulty.

Figure 5b shows that U.S. SMBs are most likely to find managing multiple wireless networks very easy.

But what about the security of the organization’s networks?

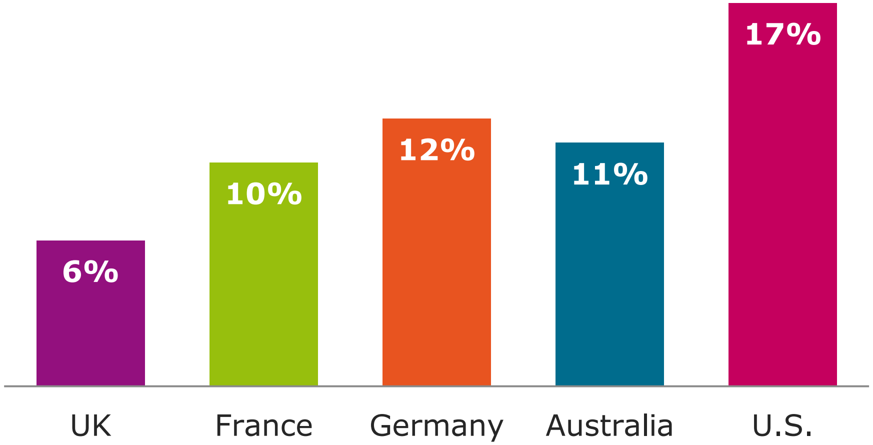


Figure 5a: Difficulty of managing multiple wireless networks, i.e., visitor and guest networks

Figure 5b: SMBs by country who find it very easy to manage multiple wireless networks

How confident are you that your wireless network is secure?

Only around one in five (21%) SMBs is “very confident” that their wireless network is secured; the vast majority have some degree of doubt.

Figure 6b shows that UK SMBs are slightly more confident than U.S. SMBs that their wireless networks are secure.

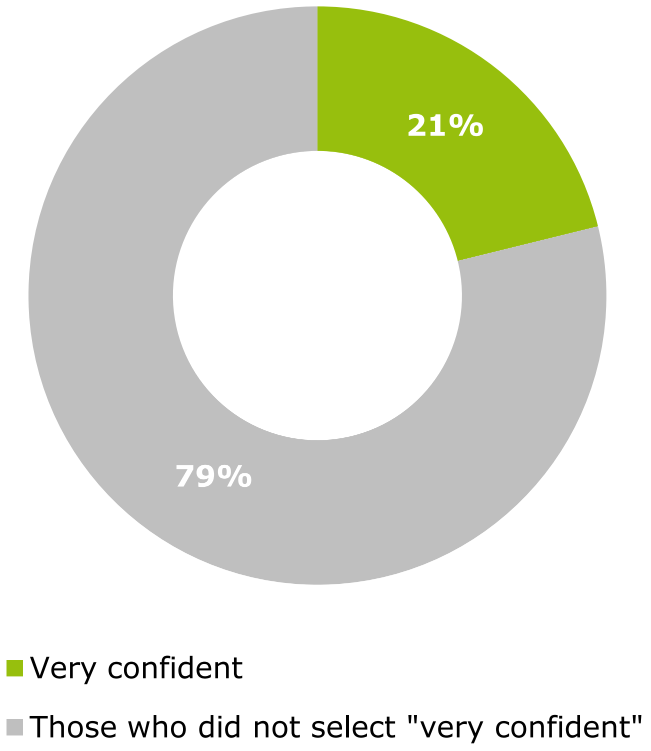


Figure 6a: Confidence of SMBs that their wireless network is secure

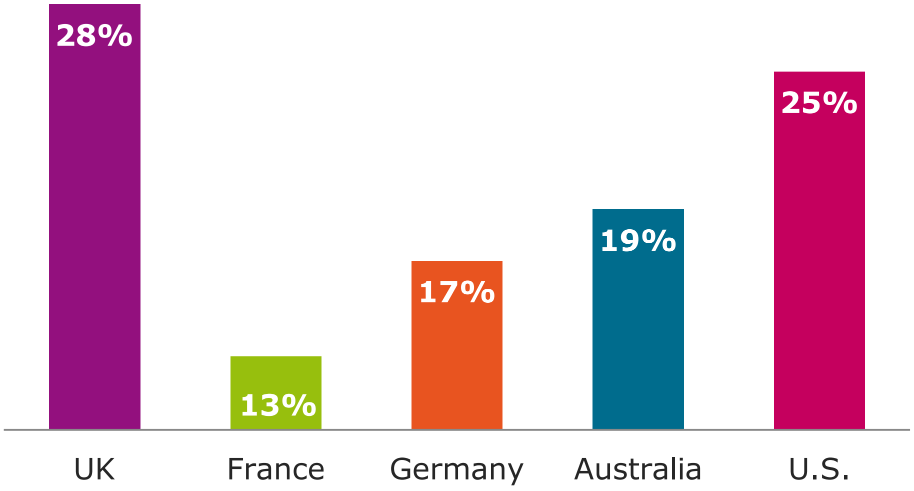


Figure 6b: SMBs by country that are very confident their wireless network is secured

Confidence in the security of wireless networks

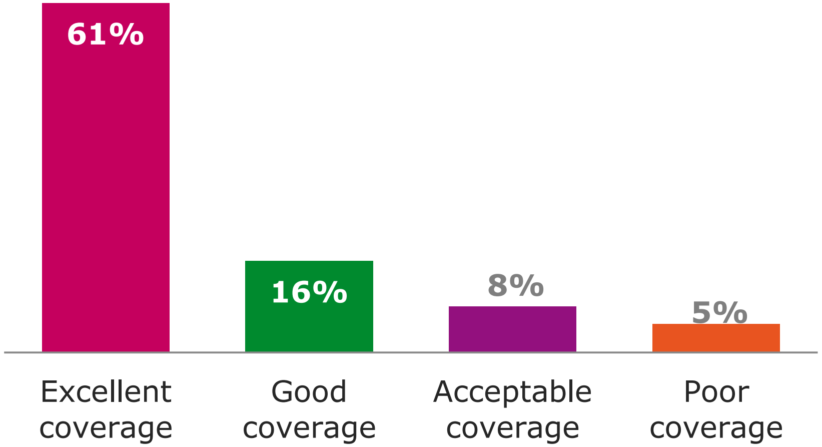


Figure 6c: SMBs by quality of coverage that answered "very confident"

Those with excellent coverage (figure 6c) and those that find managing multiple networks very easy (figure 6d) are the most likely to be confident in their network's security.

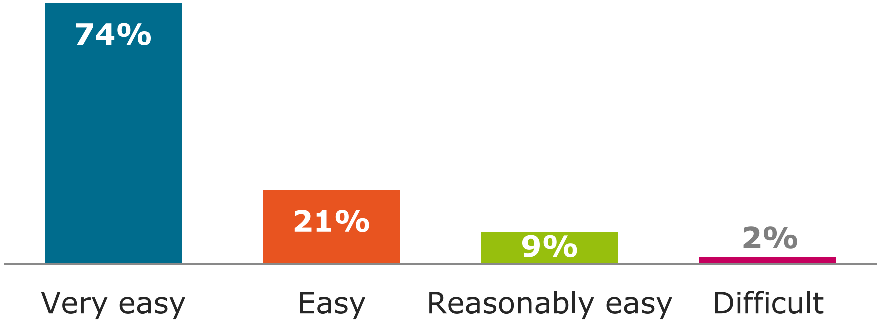


Figure 6d: SMBs by ease of wireless management that answered "very confident"

How long an SMB's firewall has been in place is also a factor. Those that have had their firewall for less than a year are the most confident about network security.

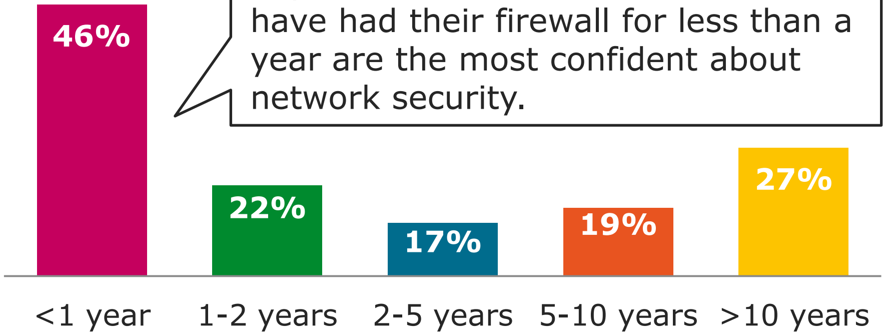


Figure 6e: SMBs that answered "very confident"

Network security challenges

VansonBourne

Challenges of network security

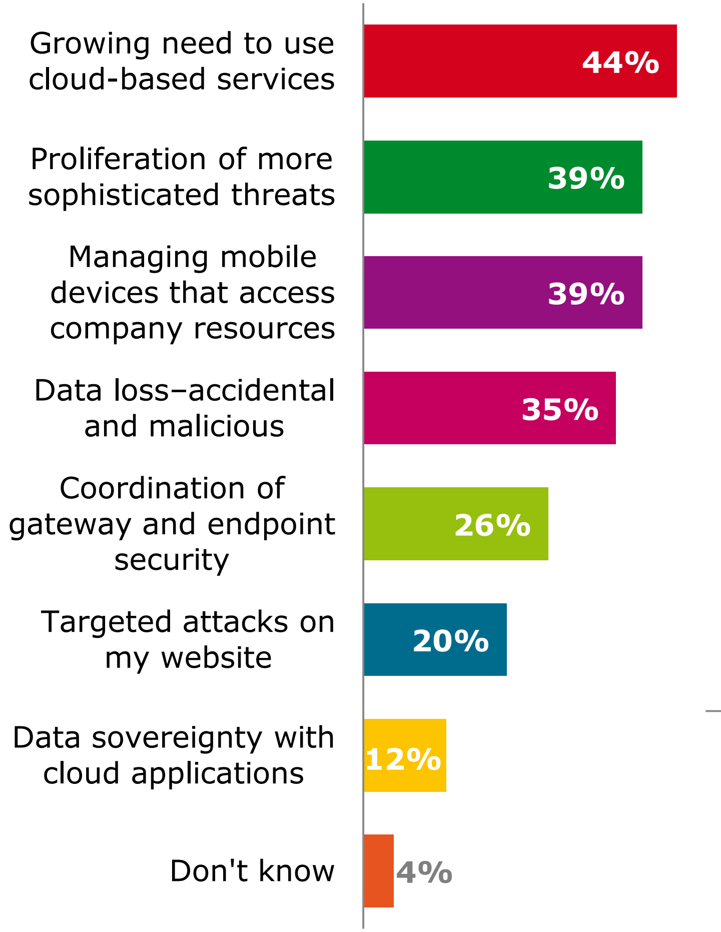


Figure 7a: What do you see as the challenges of network security going forward?

SMBs worry about network security. On average, respondents selected at least two of the challenging factors in figure 7a.

Each country has a different view. In the UK, 57% of IT decision makers are concerned about managing devices that access company resources, compared to just 39% overall. The growing need to use cloud-based services concerns 50% of U.S. SMBs, compared to just 44% overall.

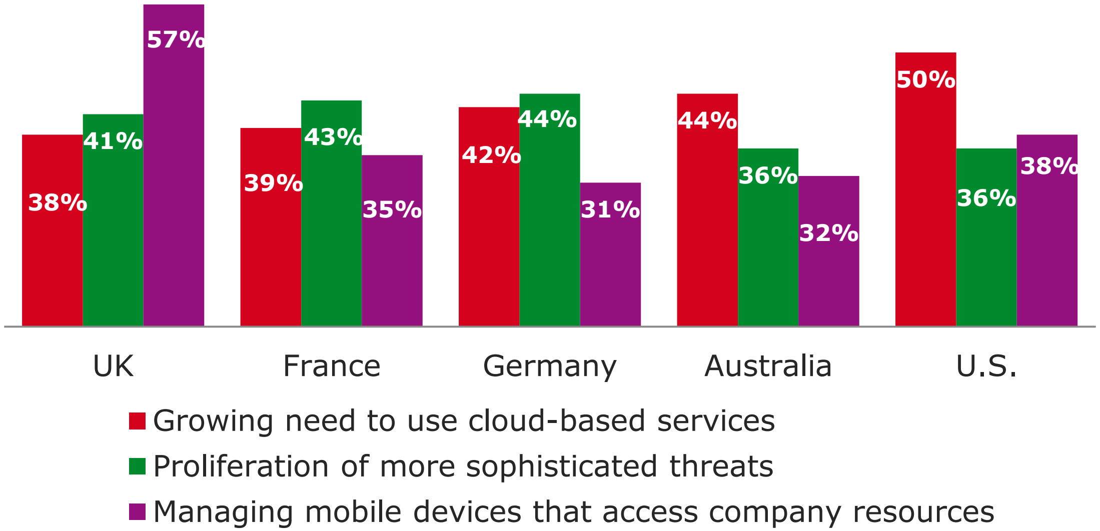


Figure 7b: SMBs that selected the top three answers by country

Network outages due to malware infections

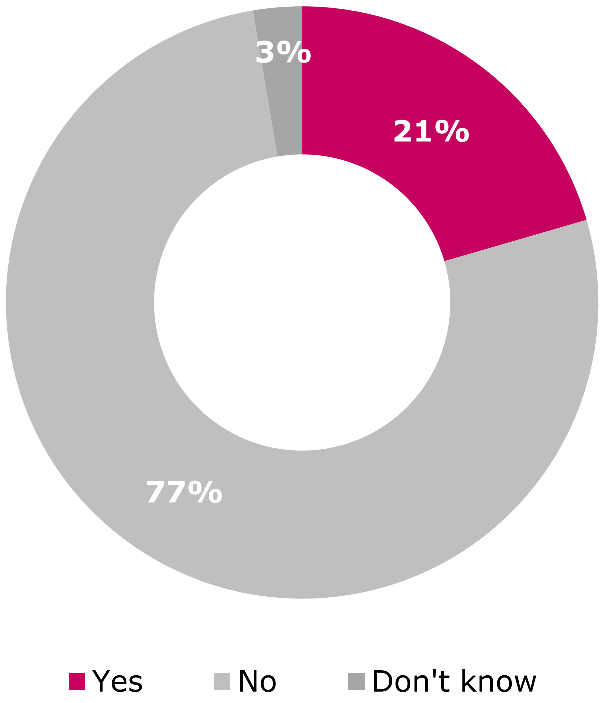


Figure 8a: Have you had a network outage caused by a malware infection in the last 12 months?

One in five SMBs experienced a network outage due to a malware infection in the last year. And 35% of those planning to increase their IT security budget to meet security requirements, e.g., increased threats from BYOD usage, had an outage due to malware in the last 12 months. This may indicate that an outage can prompt a budget increase, and/or that malware is a risk associated with BYOD.

Figure 6e illustrates that confidence in network security increased the more recently an SMB's firewall was deployed. Figure 8b shows that the newer the firewall, the more likely an SMB had a network outage in the last year. A possible conclusion is that they didn't previously have a firewall and experienced an outage; now that they have a firewall, they feel more confident in their network security.

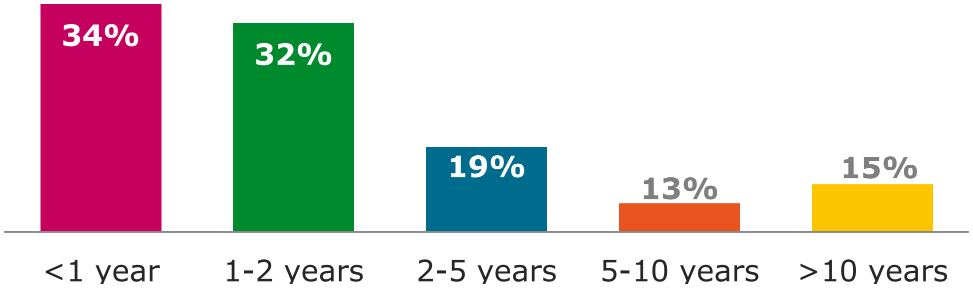


Figure 8b: SMBs that have had a network outage caused by a malware infection in the last 12 months, broken down by years they have had their firewall

Do IT decision makers understand UTM?

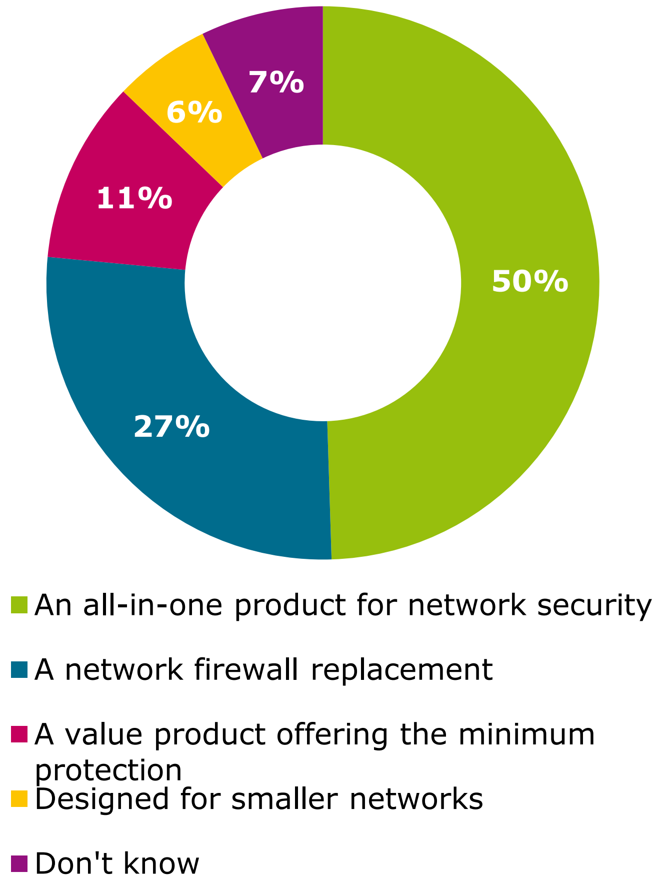


Figure 9a: Which of these statements best describes your view of unified threat management (UTM) solutions?

50% of IT decision makers consider UTM “an all-in-one product for network security.” However, 27% think a UTM is “a network firewall replacement”; 11% think it’s “a value product offering the minimum protection” and 7% don't know.

Figure 9b shows that U.S. and UK SMBs are more familiar with UTM solutions.

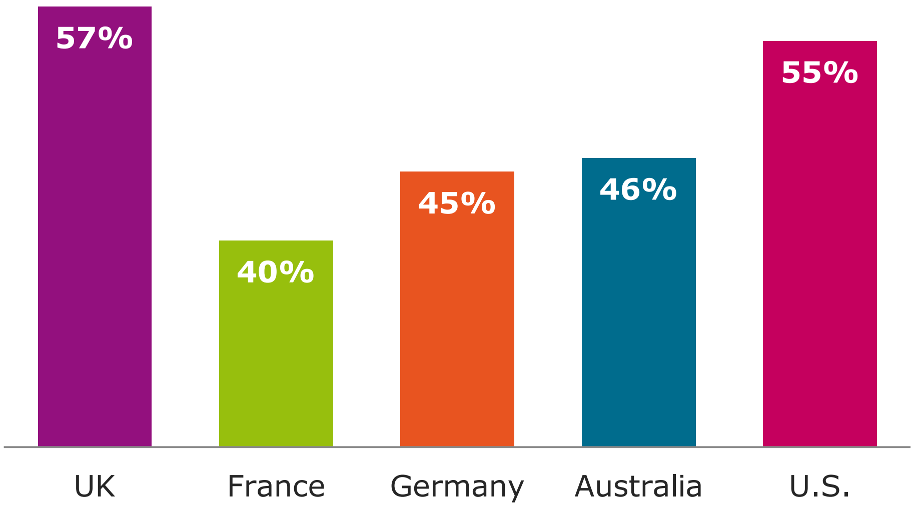
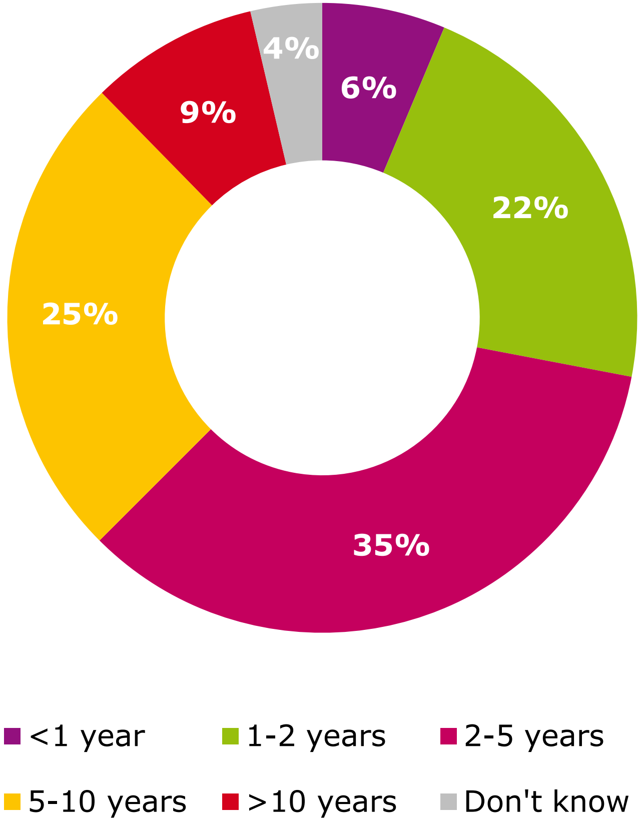


Figure 9b: SMBs by country that think a UTM is an all-in-one product for network security

How long have SMBs had their firewalls?



On average, SMBs have had their firewalls around five years, while 28% have had them for less than two years.

31% of the smallest SMBs (5-100 employees) have had their firewall for two years or less, compared to 25% of larger SMBs (101-500 employees).

Figure 10: How long have you had your network firewall?

What do you consider when choosing a network security solution?

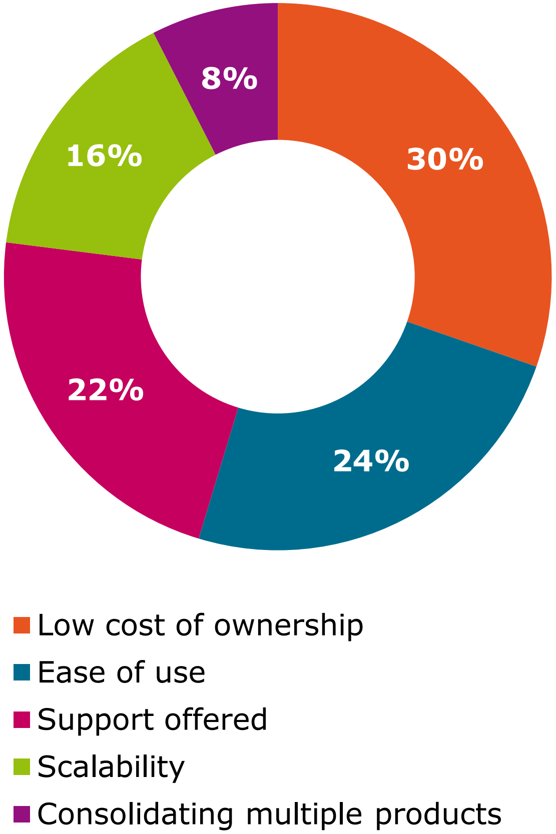


Figure 11a: The most important factors when choosing a network security solution

Low cost of ownership is the most important factor when choosing a network security solution (30%). Ease of use (24%) and the support offered (22%) are also important.

There's a difference of opinion by country. In Germany and Australia, low cost of ownership is more important than ease of use. However, in the UK, ease of use trumps low cost of ownership.

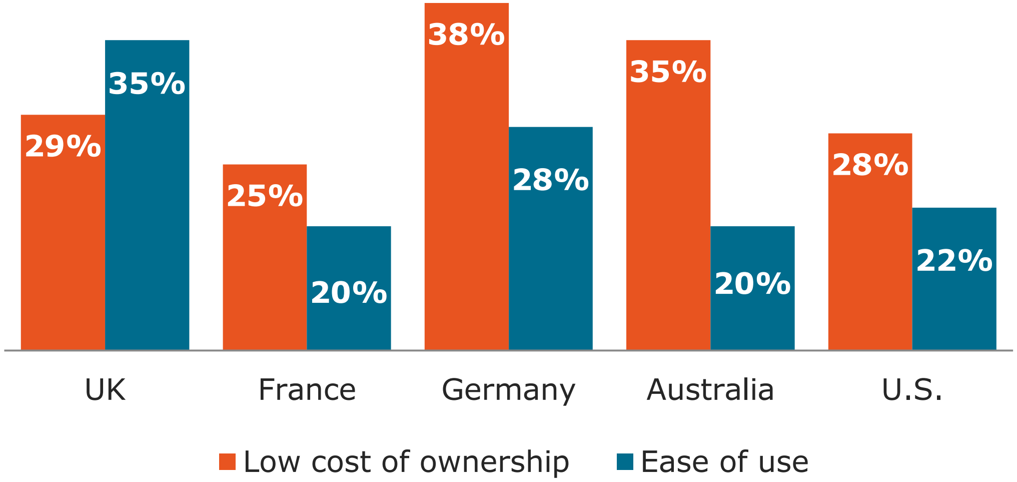


Figure 11b: SMBs by country that chose the top two answers

The future of network security

VansonBourne

How will your IT security budget change in the next year?

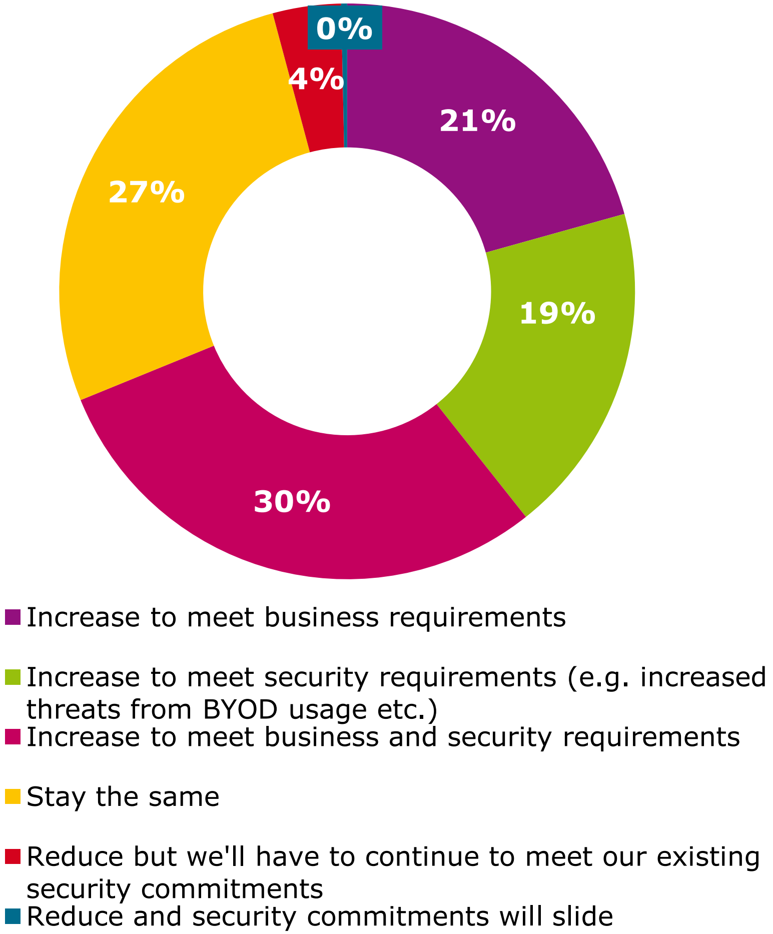


Figure 12a: How IT security budgets will change in the next 12 months.

Nearly half (49%) of organizations will increase their IT budgets to meet security requirements, 19% to address security requirements and 30% to meet both business and security requirements.

U.S. SMBs are the most likely to increase their IT security budgets. UK SMBs are the least; 10% of UK SMBs will be dealing with a reduced IT security budget and will have to do more with less.

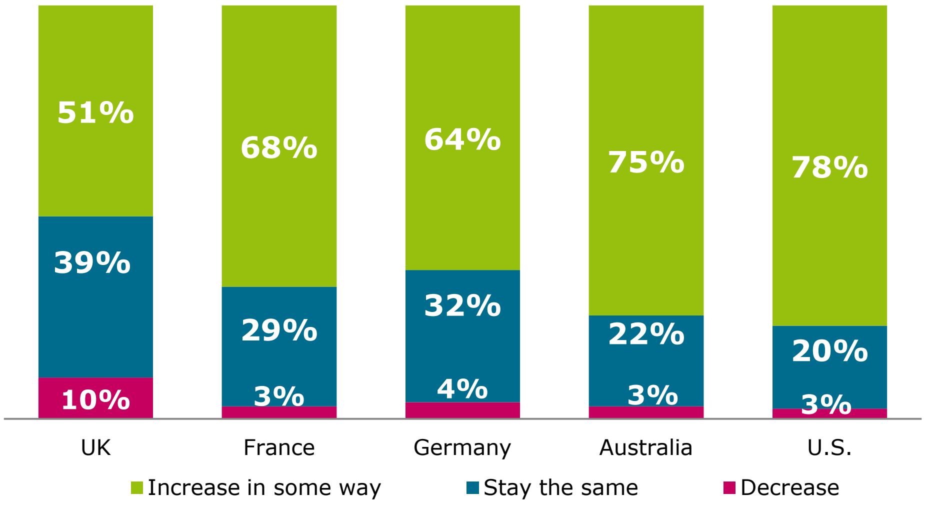


Figure 12b: SMBs by country: Differences in IT security budget over the next 12 months

What will you focus on in the next year?

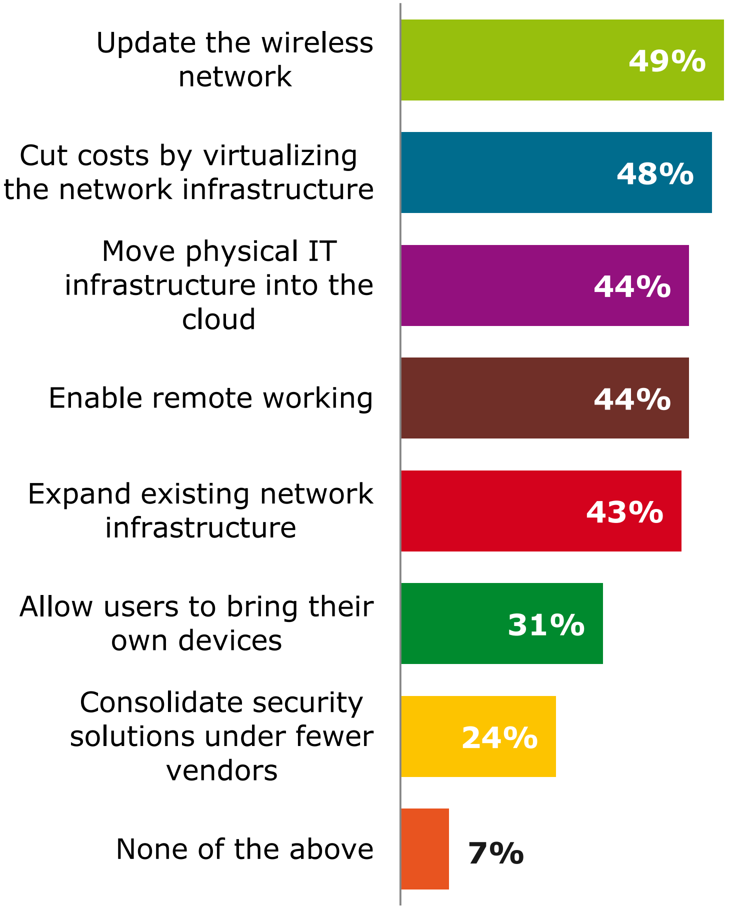


Figure 13a: Activities IT teams are planning in the next 12 months

Larger SMBs are more likely than smaller ones to carry out more tasks (an average of three compared to two in the smaller organizations). As a result, they are more likely to carry out each of the three most common tasks.

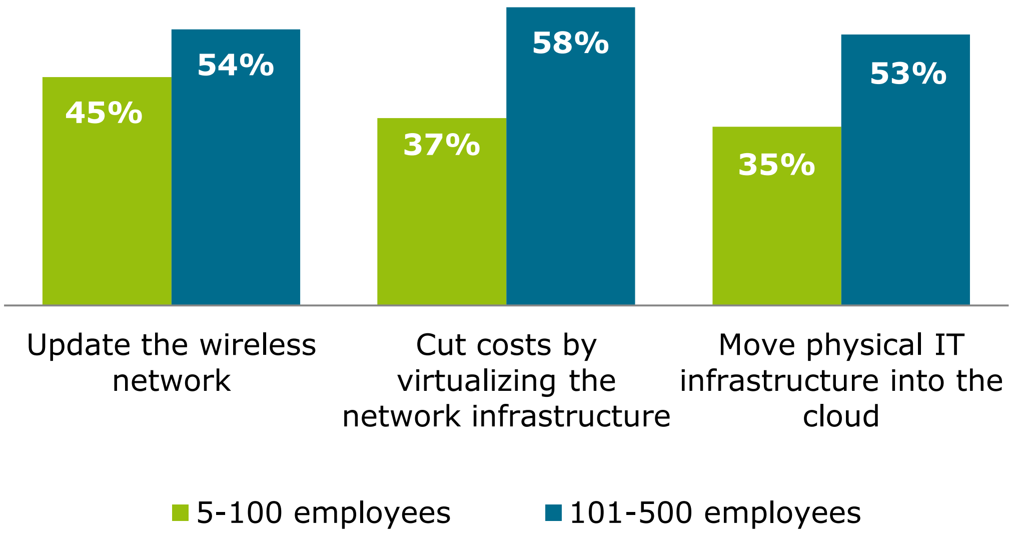


Figure 13b: SMBs by size: the three most popular activities IT teams are planning in the next 12 months