

Understanding the Security and Data Backup Market for Managed Service Providers (MSPs)

Survey of MSPs in UK and US serving SMB customers and understanding the security and data backup market opportunity

Sponsored By

Acronis

April 2020

Roy Illsley
Distinguished Analyst
roy.illsley@omdia.com

© 2020 Omdia

Brought to you by Informa Tech

OMDIA

Content

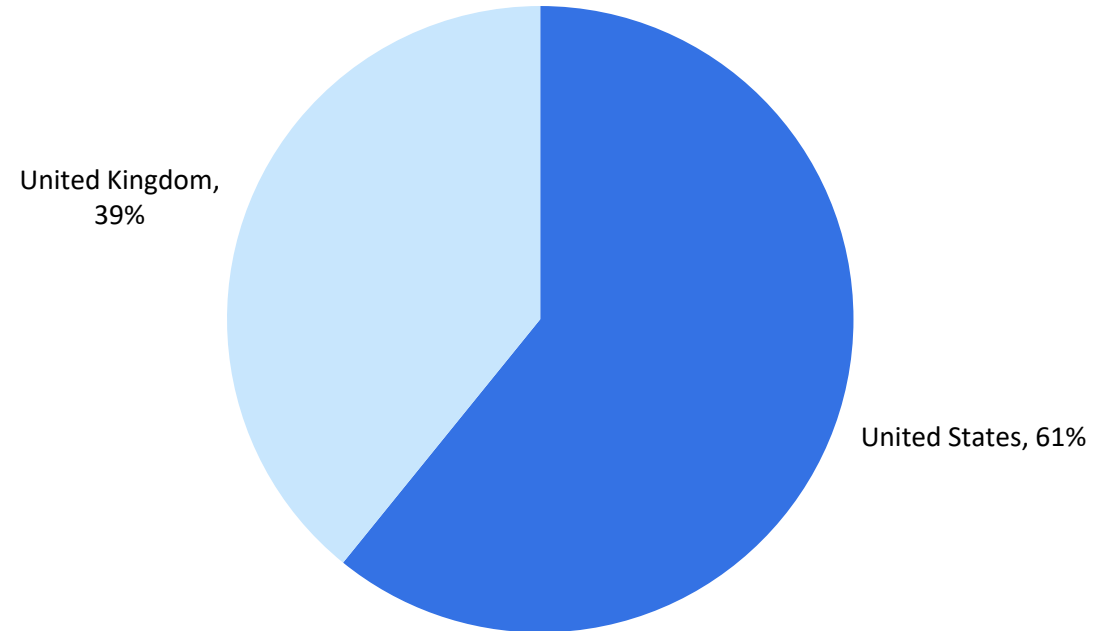
- What we did
- Findings
 - Current and future capabilities
 - Business challenges with achieving future capabilities
 - MSP challenges with delivering security as a service
 - Key considerations for MSPs when selecting a supplier
 - MSPs views on the vendors
- Summary
- Appendix
 - Survey demographics

What we did

Omdia MSP survey

- Conduct a survey of 263 MSPs in UK and US that serve SMB customers (Figure 1)
- Focused on MSPs that do not use open source technologies.
- Focused on MSPs that either deliver or are planning to deliver security and backup capabilities.

Figure 1: Respondent company location



Current and future capabilities

Top security capability today: minimizing data loss

- **Minimizing data loss** is #1 most important security capability with nearly 30% of all respondents (Figure 2).
- **Minimizing data loss** is 10% more important in US than in UK (Figure 2).
- **Rapid mitigation** is #2 most important security capability with nearly 23% of responses.
- **Forensic investigation** is lowest rated security capability with only 13% putting it as most important.
- The results show that MSPs consider the ability to protect customers data and deal with known threats quickly as core capabilities. Other capabilities are currently seen as secondary considerations.

Figure 2: Current most important security capabilities

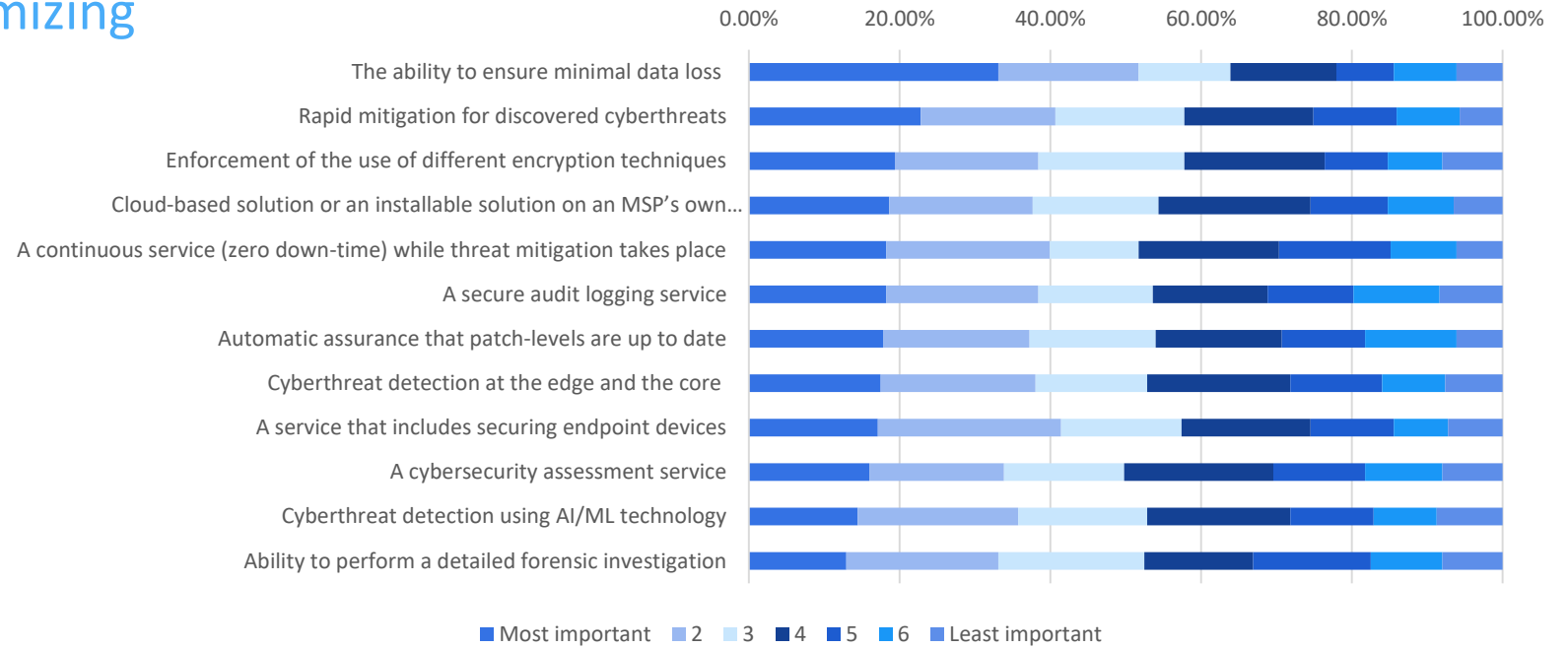
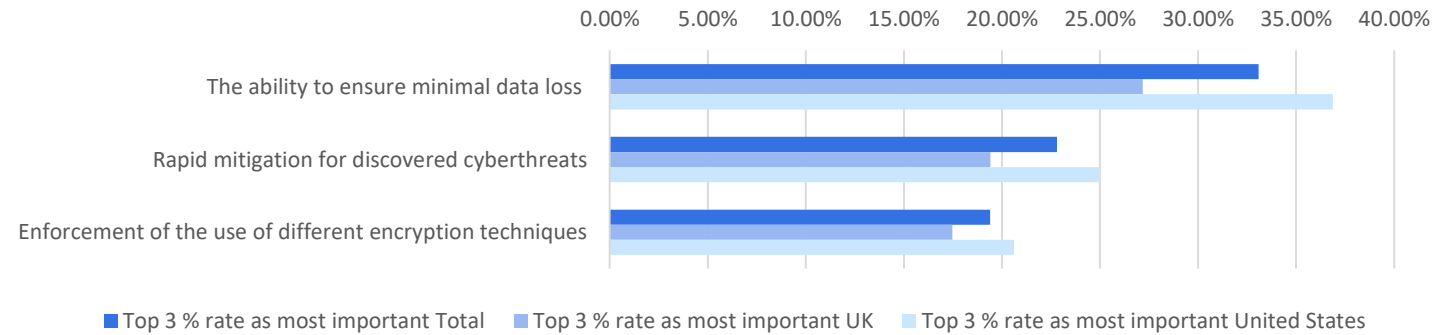


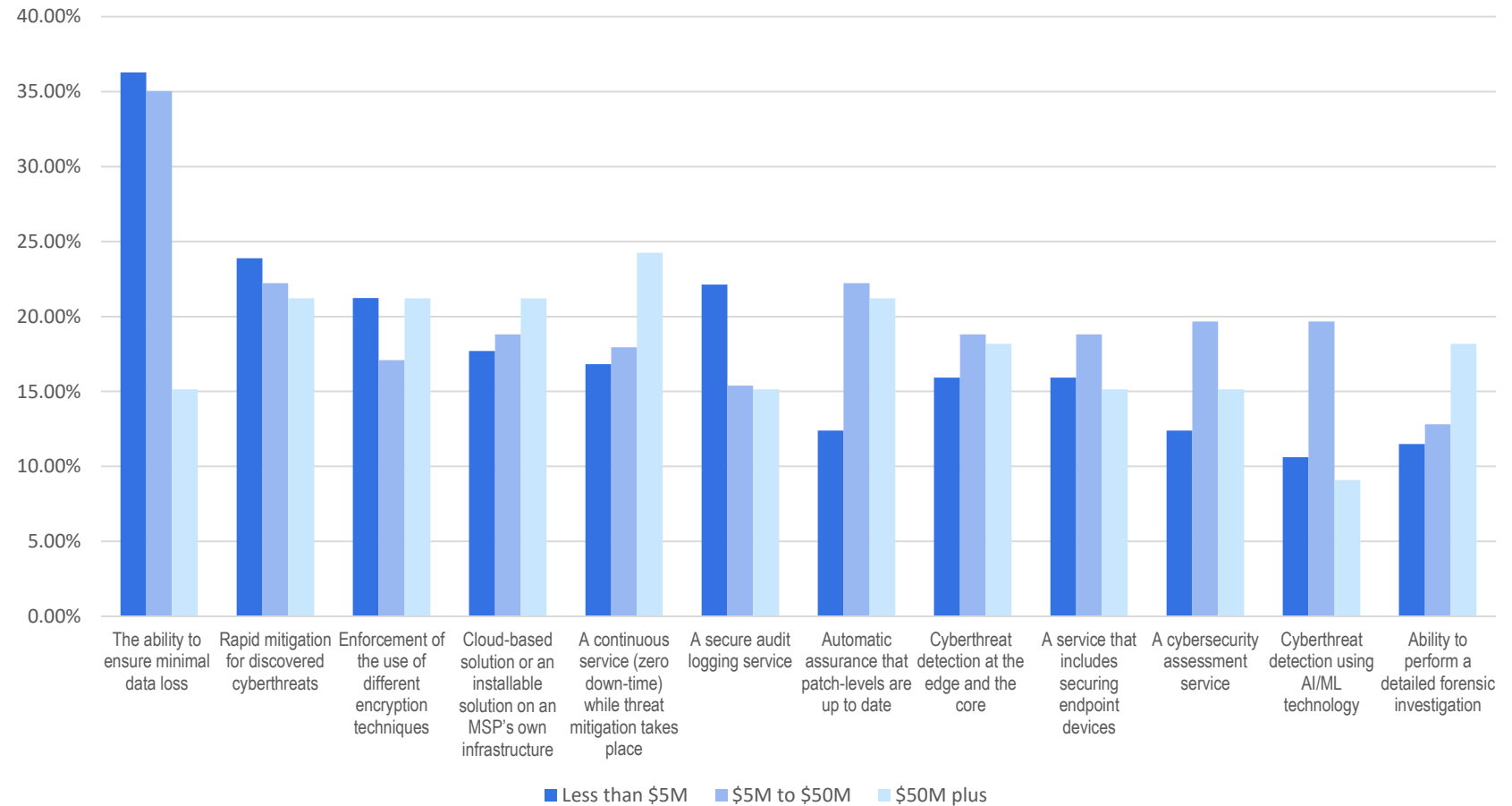
Figure 3: Top 3 current security capabilities by country



MSP differ on top security capability depending on size

- **Minimizing data loss** is #1 for MSPs with revenues of less than \$50M (Figure 4).
- **Rapid mitigation** is #2 for all MSPs, but slightly more important for MSPs with revenues of less than \$5M.
- **Zero downtime** is #1 for MSPs with revenues greater than \$50M.
- **AI/ML** is least important to MSPs with greater than \$50M revenue and less than \$5M. For MSPs revenue of \$5-\$50M it was joint third most important.
- Rapid mitigation is a common capability considered important.

Figure 4: MSP by revenue band most important current security capability



Minimizing data loss remains #1 future security capability

- Minimizing data loss** remains the #1 security capability (Figure 5). UK has seen an increase in importance but remains 7% behind North America (Figure 6).
- Zero downtime** is second most important as MSPs recognize the need to minimize data loss includes data availability.
- Rapid mitigation** and **securing endpoints** are joint third. Endpoints are now recognized as one of the most common ways security is compromised.
- The US is consistently more interested in the top 3 security future capabilities than UK (Figure 6).

Figure 5: Future most important security capabilities

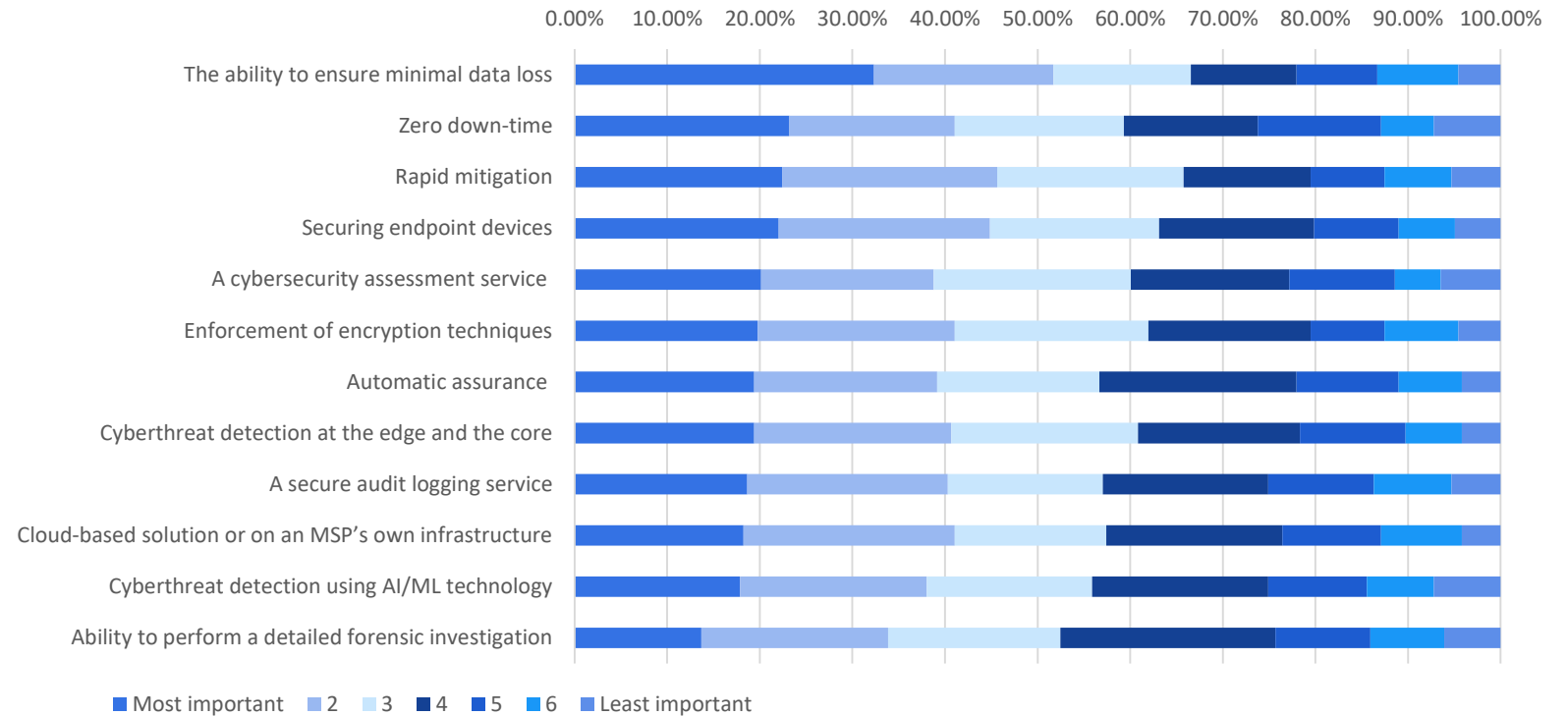
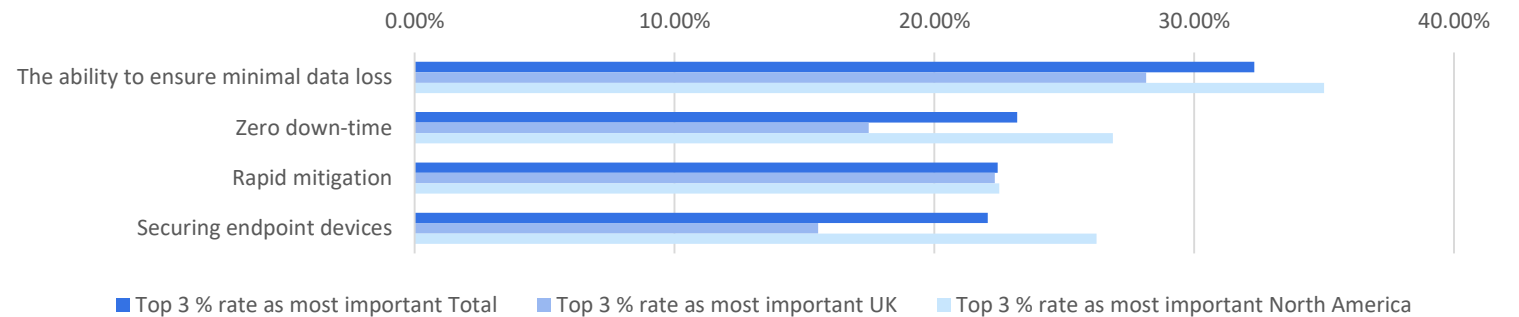


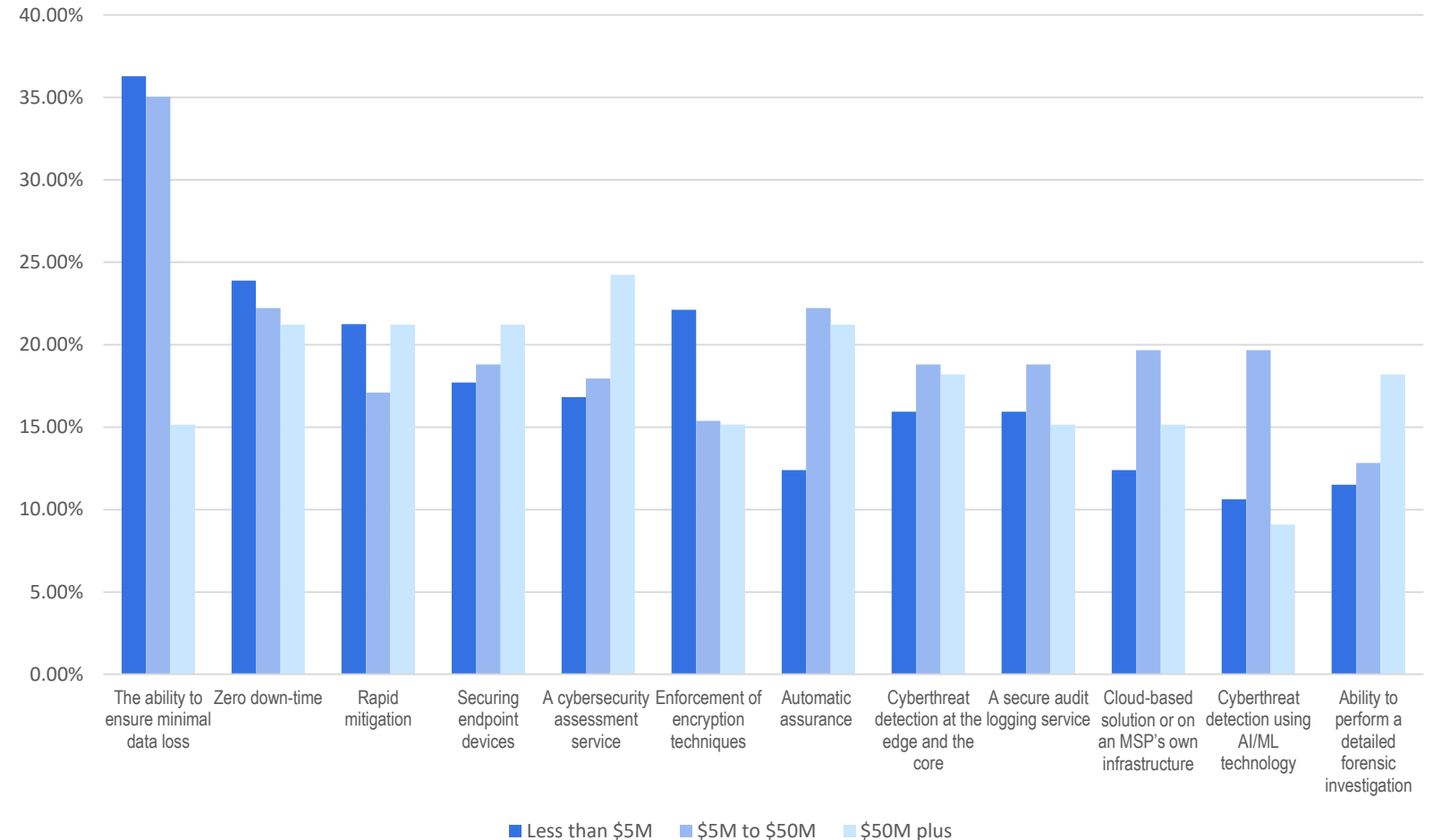
Figure 6: Top 3 future security capabilities by country



Differences exist in MSPs by revenue size as to future most important security capability

- **Minimizing data loss** remains the top capability for MSPs with revenues below \$50M.
- **Cyber assessment service** is the top future security capability for MSPs with greater than \$50M, showing that they believe their capabilities must now extend beyond basic security offerings.
- **AI/ML** remains least important to MSPs with greater than \$50M and less than \$5M. This suggests an education issue with understanding the value of AI/ML.
- **Zero downtime** is second as MSPs recognize that data availability is part of what customers consider data loss.

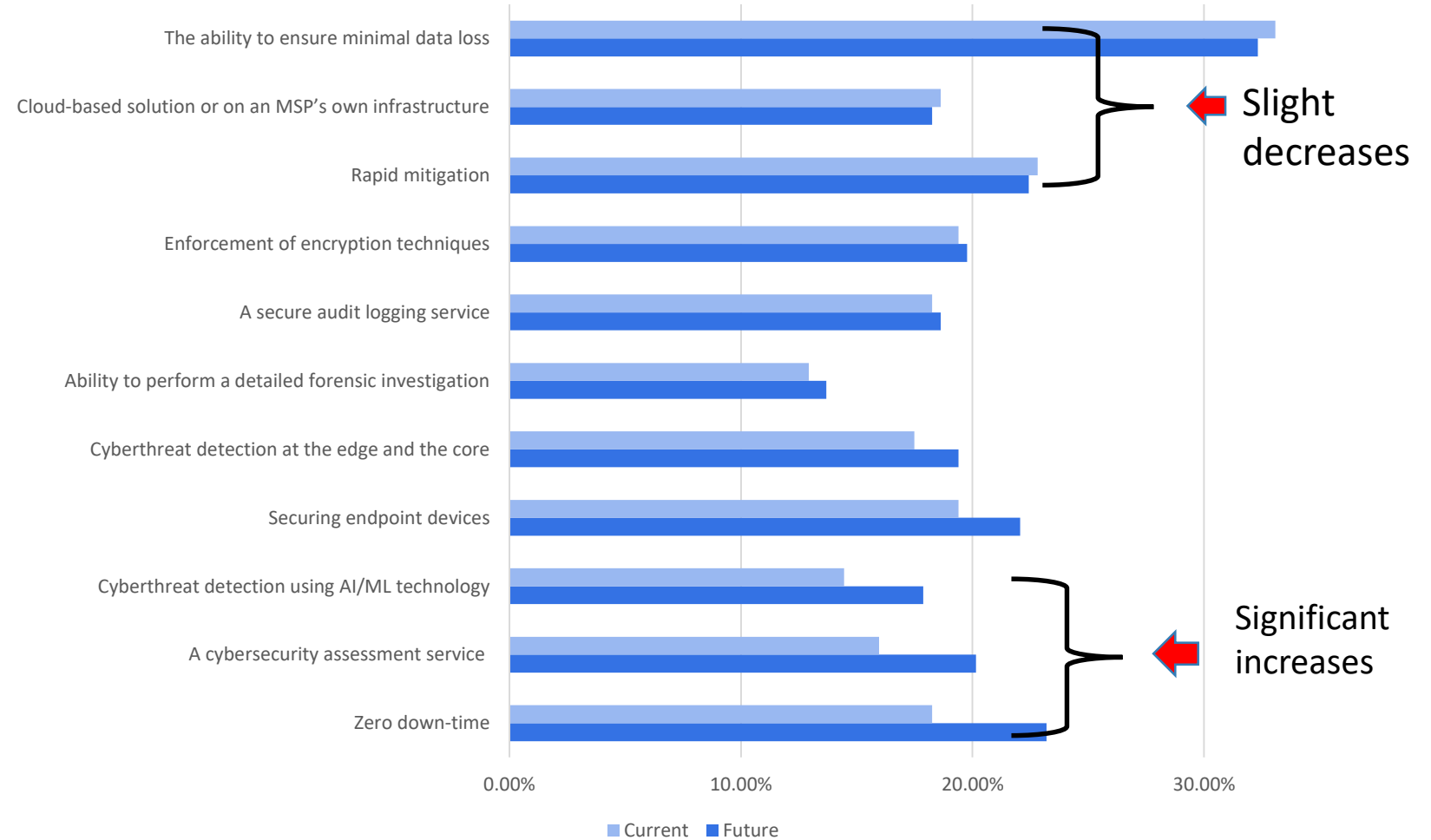
Figure 7: MSP by revenue band most important future security capability



Differences between current and future security capabilities

- **Zero downtime** shows the biggest increase in interest from current to future security capabilities (Figure 8).
- **Cyber security assessment** shows second biggest increase in interest, with **AI cyber detection** with third biggest increase.
- **Minimizing data loss** remains top capability but shows slight decline in interest – probably not much to read into this as it is such a clear top topic of interest.
- **Rapid mitigation** was the second capability to show a decline of interest from current to future, but again unlikely enough to be of significance.

Figure 8: Most important capability comparing current and future responses



Automation is the #1 current backup capability

- **Automate the backup process** is the top most important capability with over 25% putting it most important and nearly 50% as important or higher (Figure 9).
- **Ransomware protection** was second most important capability.
- **Copy test data** and **RTO/RPO** are the least important capabilities with only 13% of respondents.
- US ranked **automation** much more important than UK, in fact US ranked top 3 consistently more important than UK (Figure 10).

Figure 9: Most important current backup capabilities

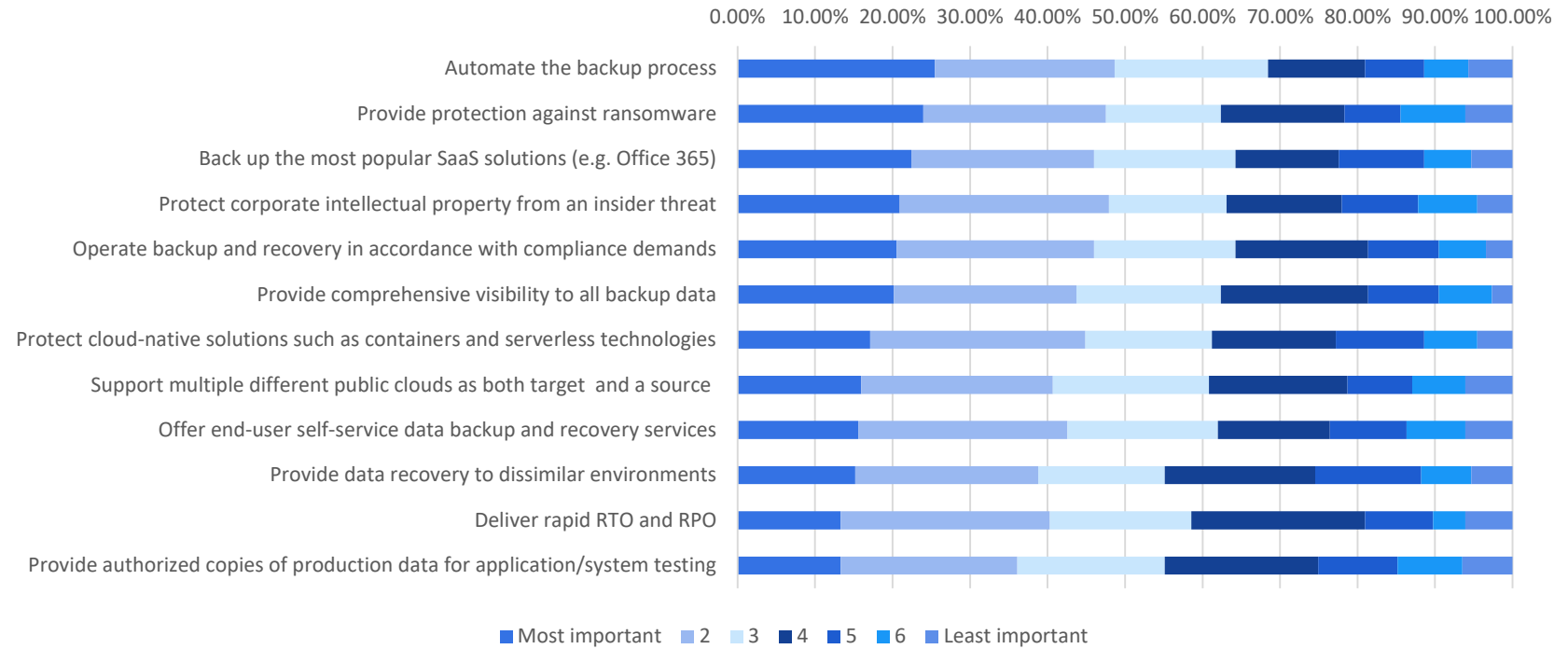
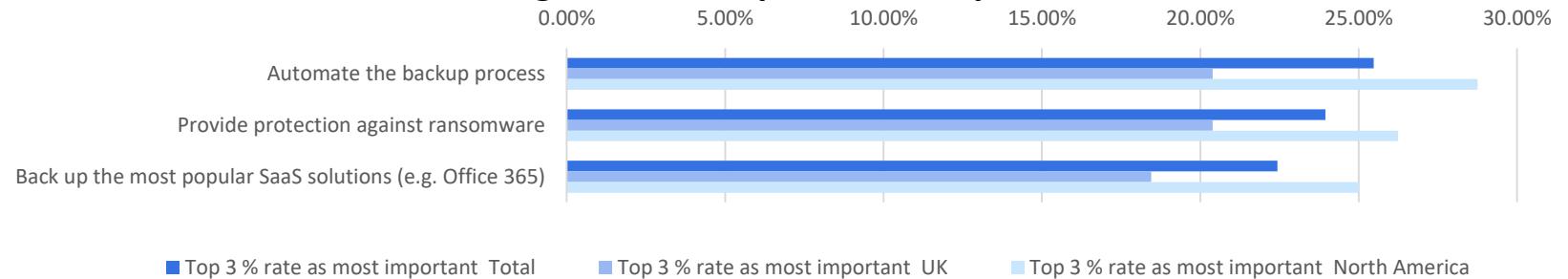


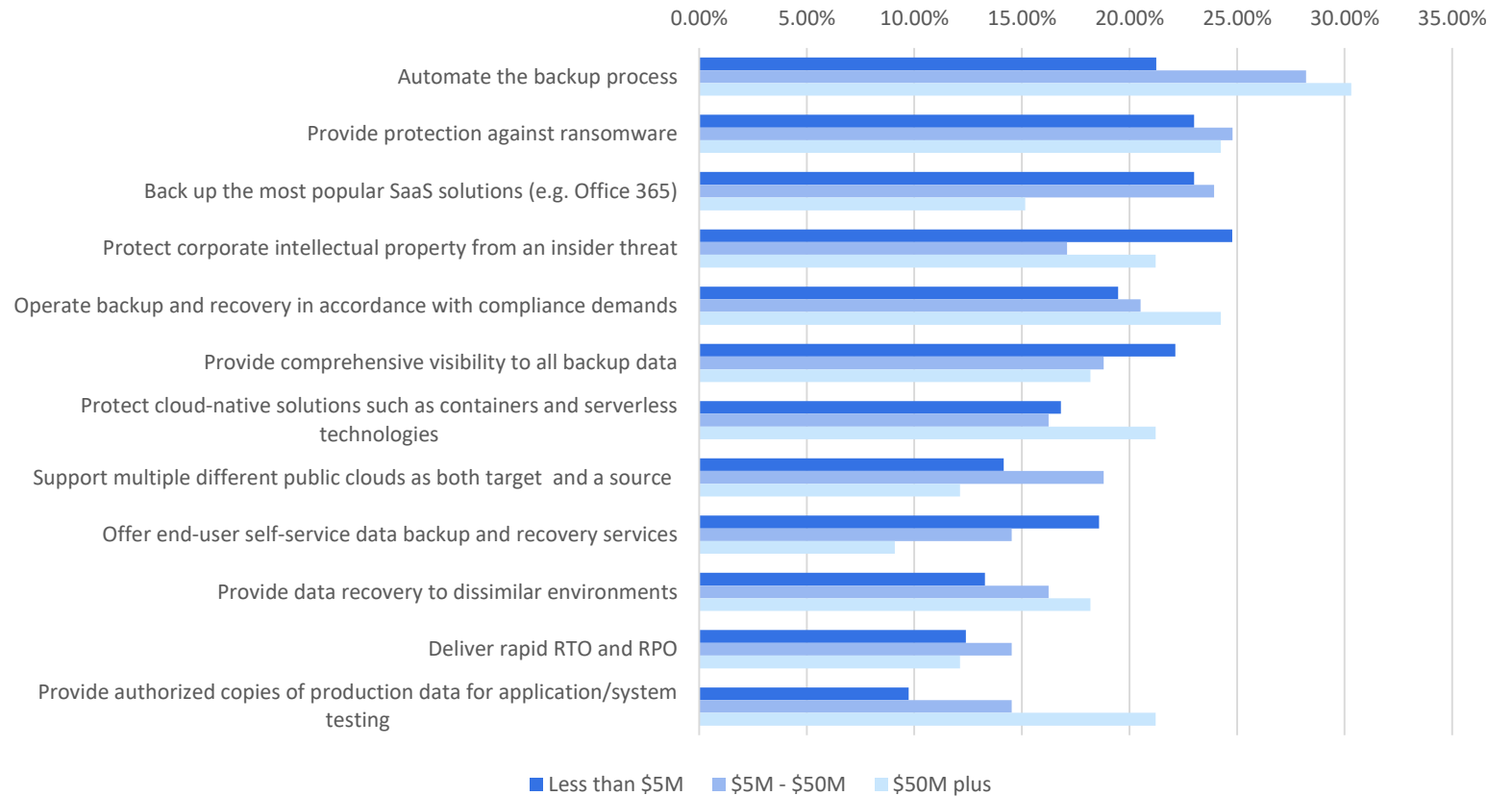
Figure 10: Comparison of top 3 UK to US



Larger MSPs place automation as more important than smaller MSPs

- **Automating backup** was put as most important by over 30% of MSPs with revenues greater than \$50M and 28% of those in \$5M-\$50M revenue bracket, compared to 21% of MSPs with revenues less than \$5M (Figure 11).
- **Protecting IP** was the most important capabilities for MSPs with revenues of less than \$5M.
- **User self service** was of least interest to MSPs with over \$50M in revenue, with just 9% respondents putting as most important.

Figure 11: Most important current backup capabilities by size of MSP based on revenue



Automation remain #1 most important future capability

- **Automate the backup process** remains the top-most important capability (Figure 12).
- The need to protect against **ransomware** – second most important – is driven by increased awareness of this threat and the number of out-of-support Microsoft Windows servers expected to be active in 2020/21 (Figure 12).
- **User self-service** and **test copy data** are the two least important future capabilities. This is a reflection of the customers served by the MSPs where internal app dev is not a common capability, and user self-service is not considered important due to lack of understanding of the benefits (Figure 12).
- US more concerned by **ransomware** than UK (Figure 13).

Figure 12: Most important future backup capabilities

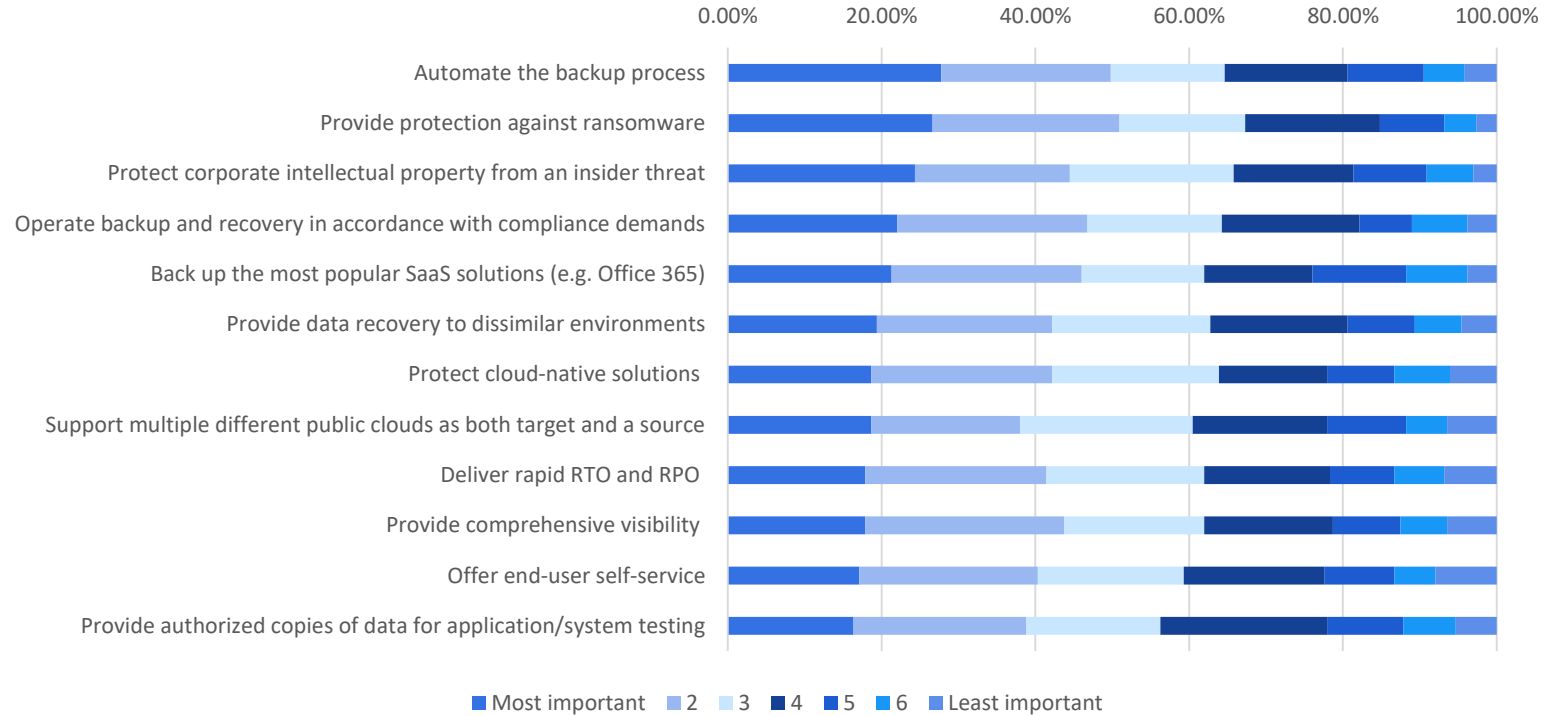
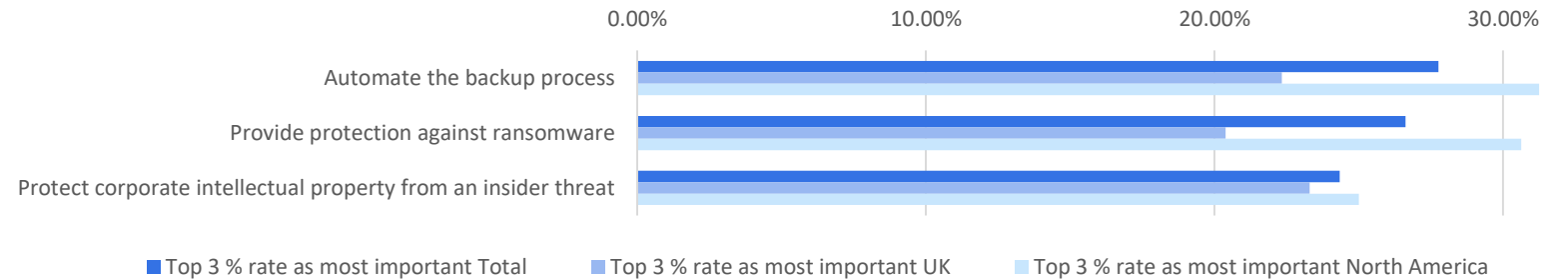


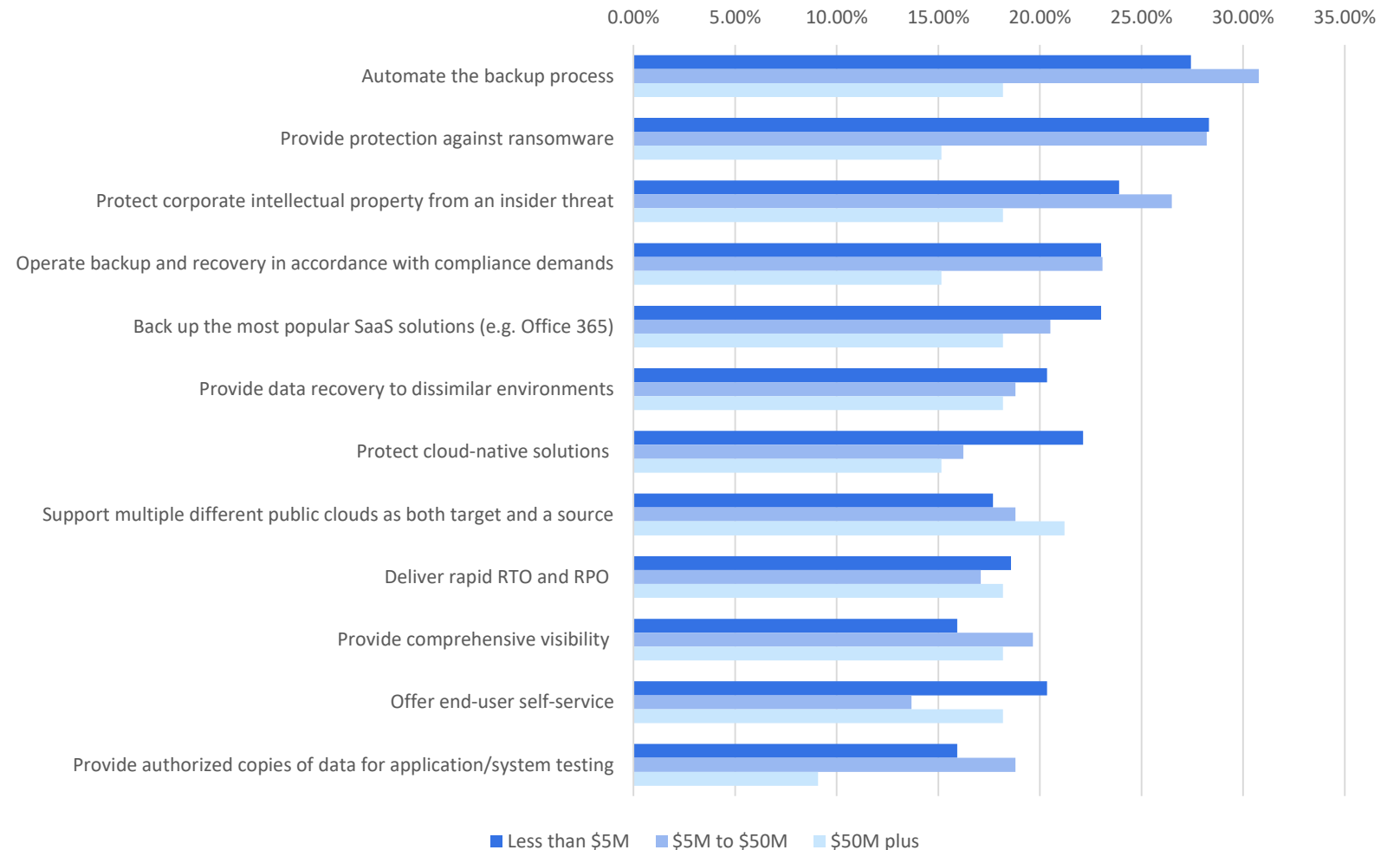
Figure 13: UK compared to US future most important backup capabilities



Future backup capabilities

- **Automation** is the singular most important future backup capability (Figure 14).
- **Automation** is more popular with those MSPs with revenues of between \$5M and \$50M, 31% put it as most important compared with 18% of MSPs with \$50M+ revenue.
- **Copy test data** is the least important future capabilities
 - **Copy test data** least significant for MSPs with greater than \$50M revenue – 9% put as most important compared to 16% average.
- Most important future capability for MSPs with revenues greater than \$50M was support for **multiple cloud** as source and target for backup data.

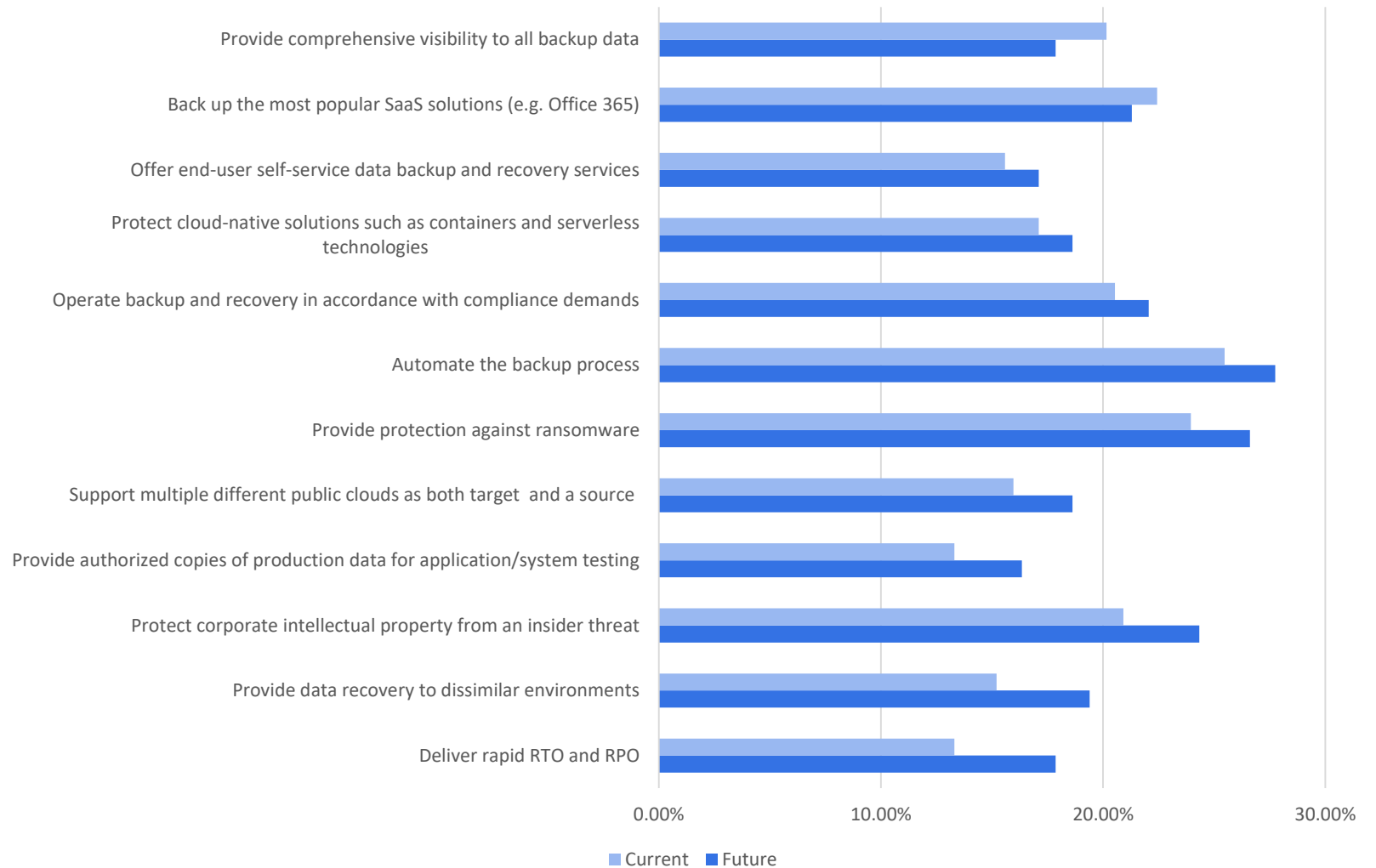
Figure 14: Most important future capabilities by MSP size in terms of revenue




Differences between current and future backup capabilities

- Only 2 capabilities show a decline in interest; **visibility** and **backup of SaaS applications** (Figure 15).
- Biggest growing capability of interest is **rapid RTO and RPO**, which shows a 5% increase in MSPs putting it as most important – organizations are recognizing that speed and completeness of protection is important.
- Second biggest growing capability of interest is **recover to dissimilar hardware environments**, which shows a 4% increase in MSPs putting it as most important.

Figure 15: Most important capabilities comparison current to future



Customer requested services from MSPs

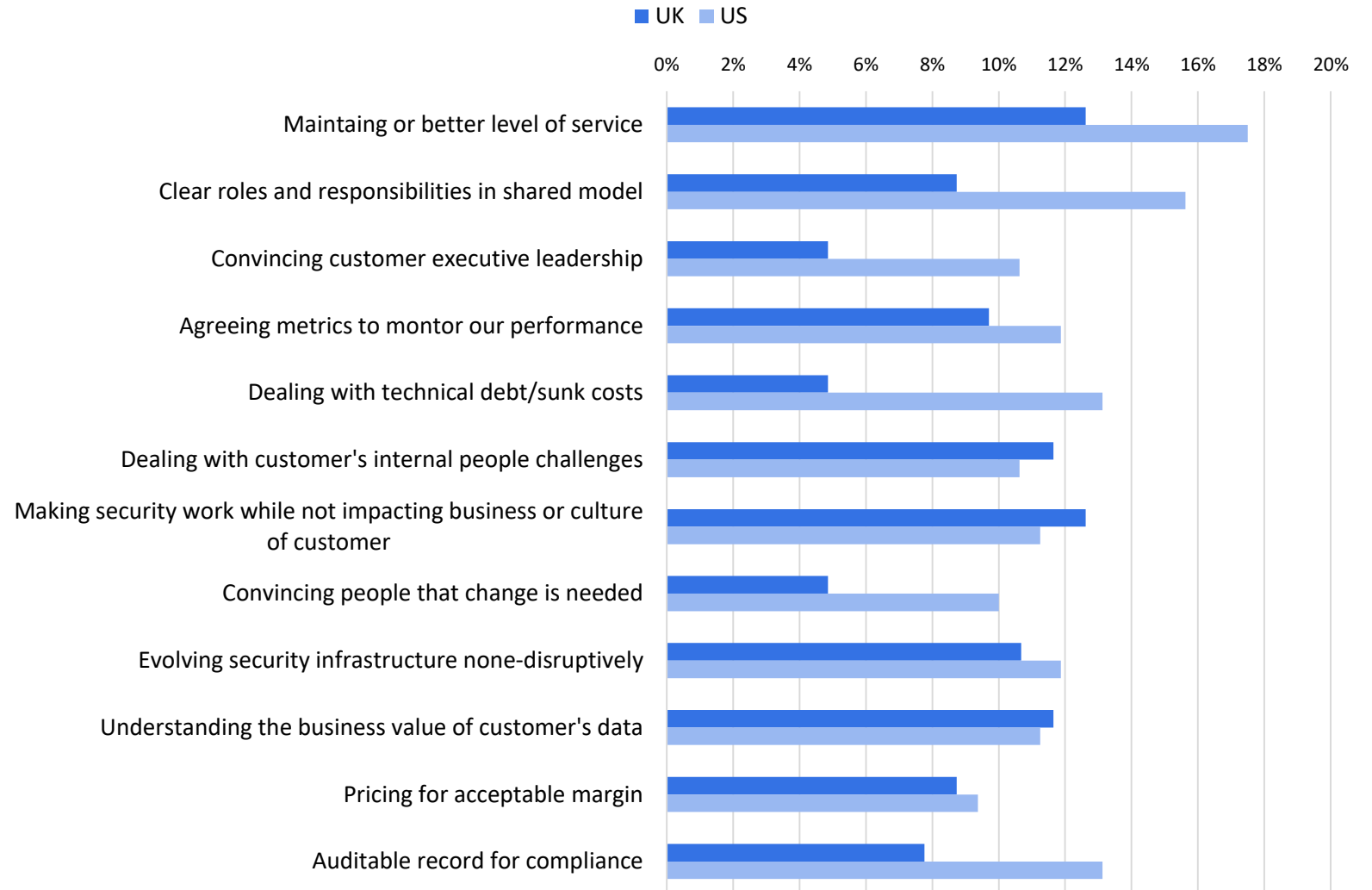
	Most requested	Second and third most requested	UK compared to US
 <p>Customer requested services</p>	<p>20% put security, or security related, as most requested new service, 19% put second, and 11% as third most requested new service</p> <p>In total 50% put security, or security related, as a top 3 most requested new service.</p>	<p>10% put keeping up with technology and 18% cost as biggest challenges in delivering the most requested new services</p>	<p>UK was higher with 23% compared to US 11% with security as most requested new service</p>

Business Challenges to achieving future capabilities

Key considerations in building a business case for customers

- **Maintaining or delivering better levels of service** has the highest impact in US (Figure 16).
- **Making security work while not impacting the business** is the highest impact in UK.
- Biggest difference between US and UK is **convincing people that change is needed**.
 - In UK fewer than 5% report it has a high impact on building a business case, whereas in US it is more than double with 10%.

Figure 16: Highest impact considerations on building a business case by country



Lack of skills is the biggest business obstacle for MSPs in adopting new services

- **Lack of skills** shows the biggest variance between most and least important, demonstrating that the skills shortage is a real concern for MSPs (Figure 17).
- **Lack of skills** most common obstacle irrespective of MSP size; in fact it was the top response in all size groups.
- **We are a specialist MSP** is the obstacle with the biggest variance (Figure 18):
 - In the 20 – 99 employee MSPs it was second most important obstacle.
 - In both **fewer than 19** and **more than 100 employee** MSPs it was the lowest business obstacle.
 - This response to the business obstacles shows that MSPs face different pressures depending on their relative size – as such, no one size solution will meet all needs

Figure 17: Difference between important and unimportant

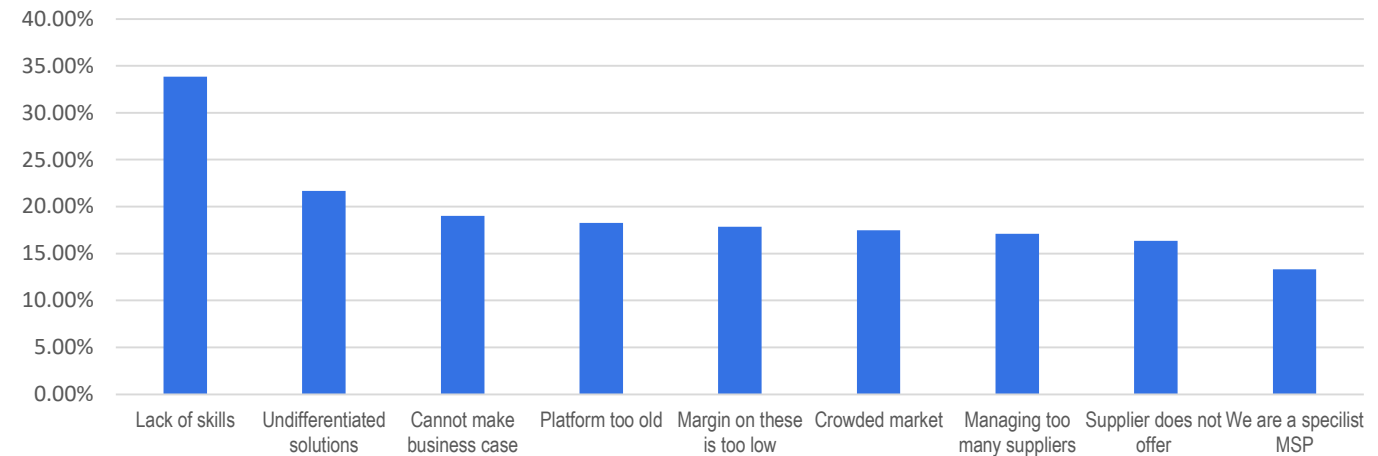
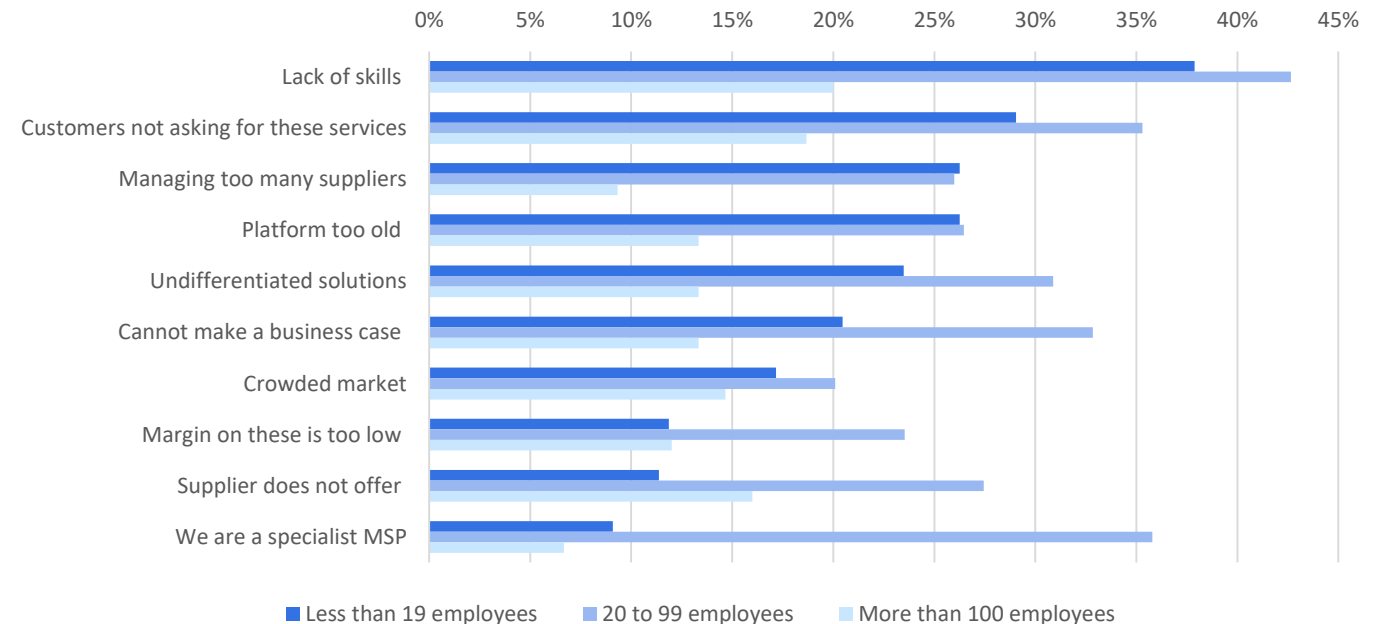


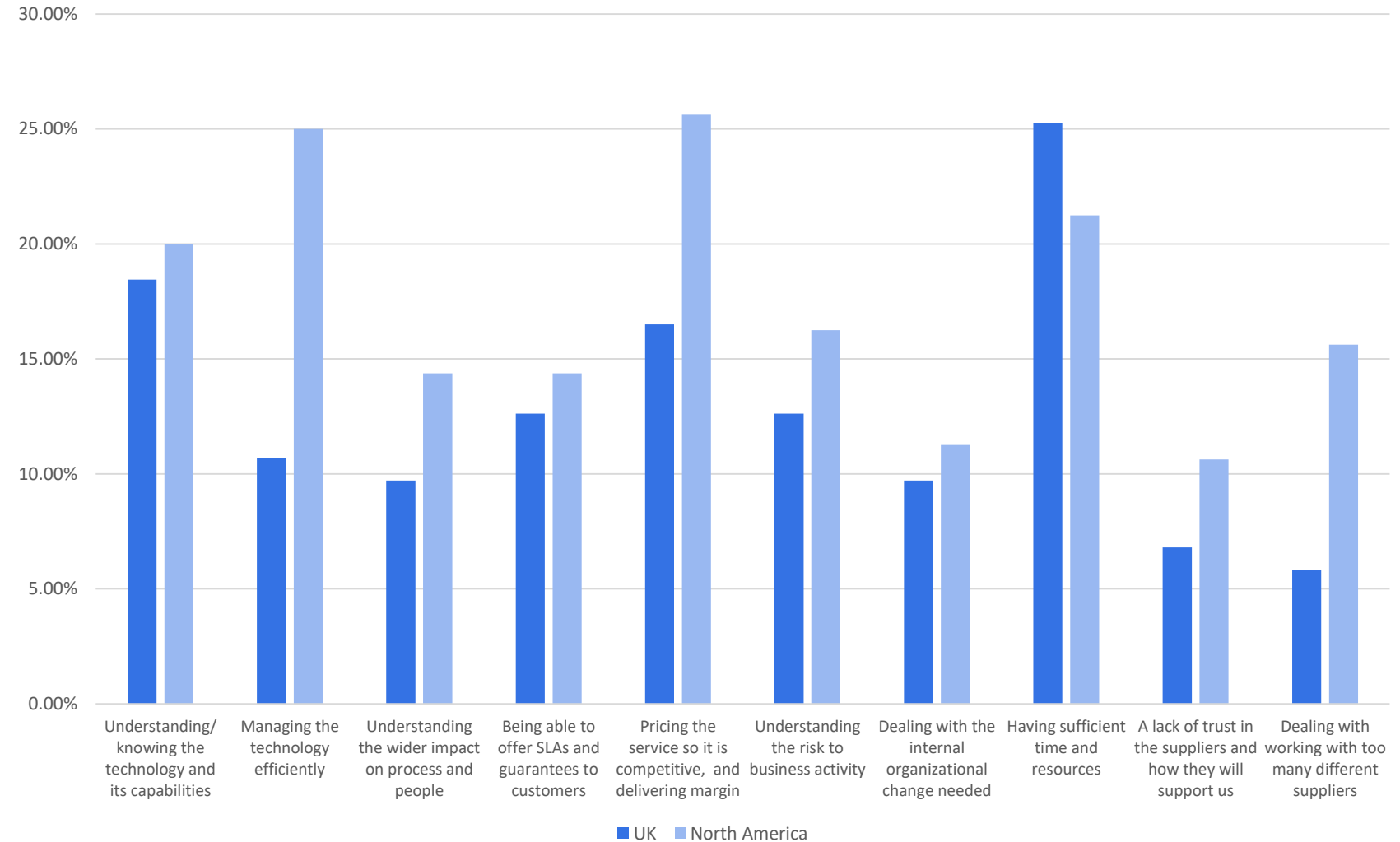
Figure 18: Most important business obstacle by MSP size number of employees



Organizational obstacles

- **Pricing the service** is the top obstacle in US, whereas in UK it is **having sufficient time** (Figure 19).
- US put **managing efficiently** second, compared to UK where **understanding the technology** was second.
- UK ranked dealing with **too many suppliers** as the least important business obstacle.
- US and UK both consider their suppliers as **trustworthy**, with only 10% and 6% respectively stating that it was an important business obstacle.

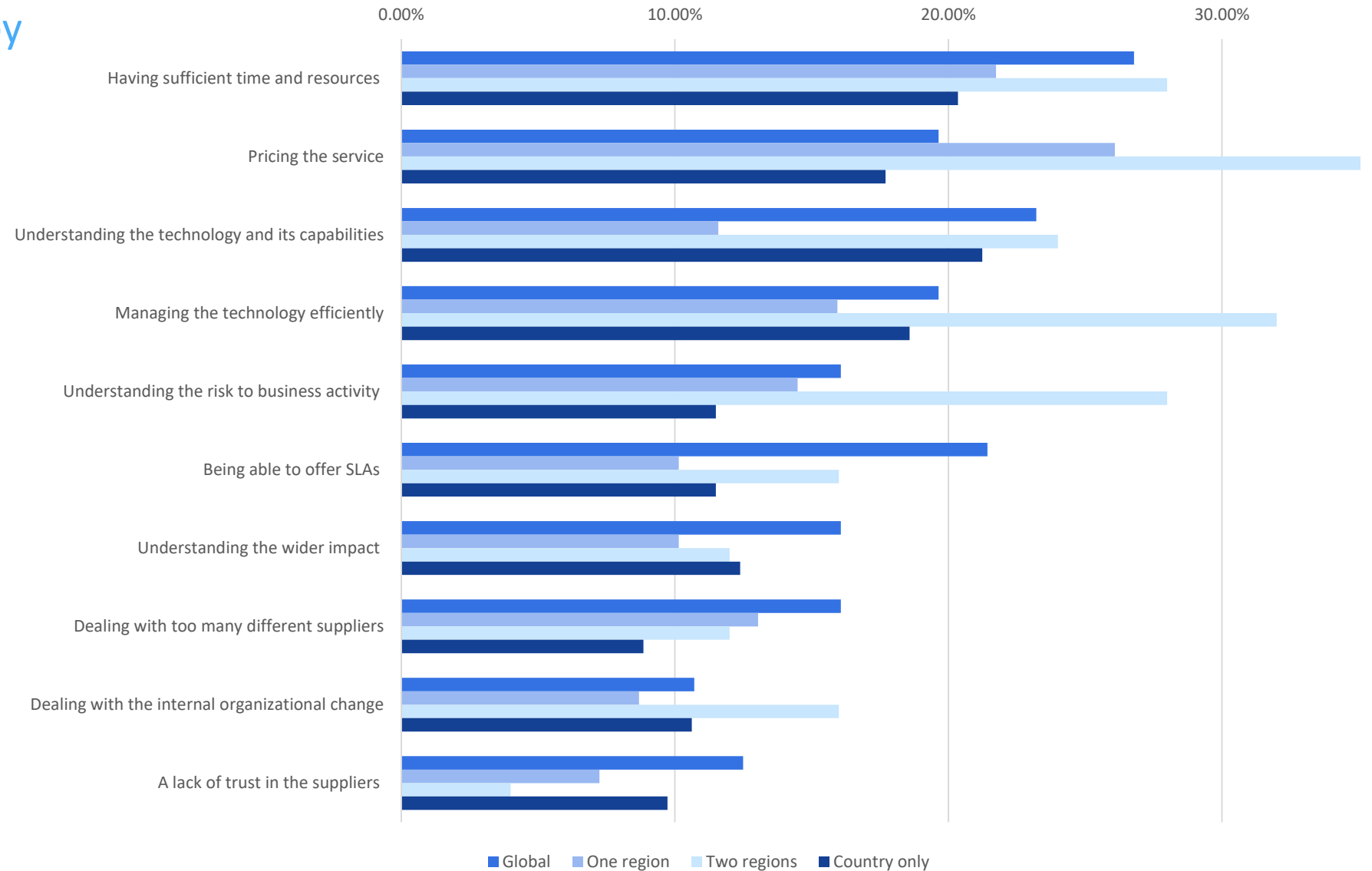
Figure 19: Business obstacles by country



Organizational obstacles by operating regions

- Those MSPs operating in two regions put **pricing the service** as most important – 36% of respondents – whereas only 18% of those MSPs operating in one country have **pricing the service** as most important – as such, pricing in more than one currency is a challenge (Figure 20).
- The biggest challenge for those MSPs operating in country is **having sufficient time** (Figure 20).

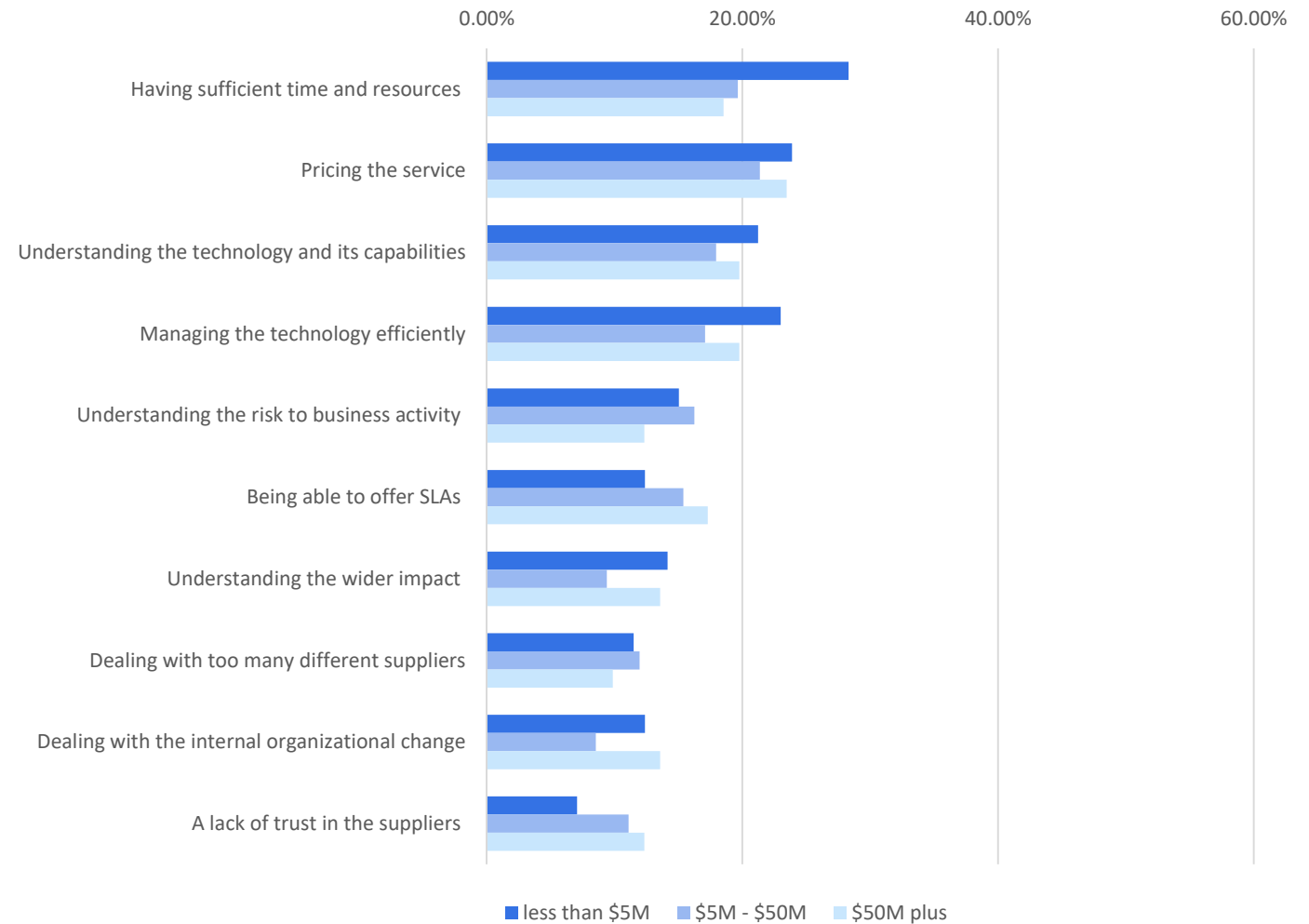
Figure 20: MSP most import organizational obstacles by operating region



Organizational obstacles by MSP size

- **Having sufficient time** was top for MSPs with less than \$5M in revenue, emphasising the pressure to release resources to learn new skills. This supports the finding in the previous slide and indicates smaller MSPs are in country only.
- **Pricing the service** was most important for MSPs with more than \$5M in revenue. This supports the previous slide where operating in more than one country creates problems with pricing.

Figure 21: MSP most import organizational obstacles by MSP size in terms of revenue

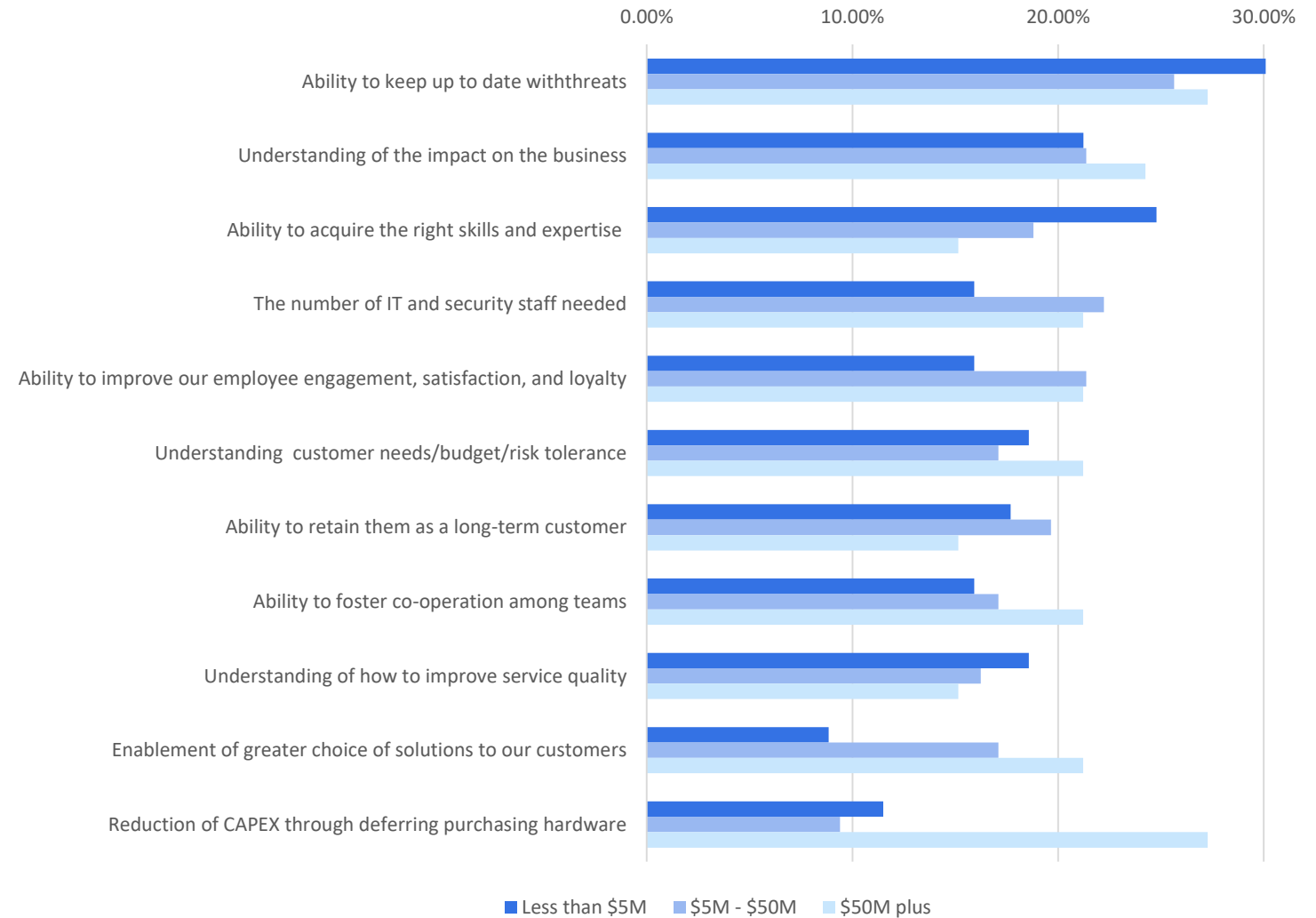


MSP challenges with delivering security as a service

People and process challenges with delivering security management as a service

- **Ability to keep up to date** is the top challenge for MSPs of all size. It was most important to those with revenues of less than \$5M (Figure 22).
- **Reduction in capex** was the least important challenge for MSPs with revenues below \$50M. But for those MSPs with more than \$50M in revenue it was joint top challenge.
- **Enabling greater choice for customers** was the least important for MSPs with revenues of less than \$5M. The customers of these MSPs are less concerned by choice and are more concerned by cost.

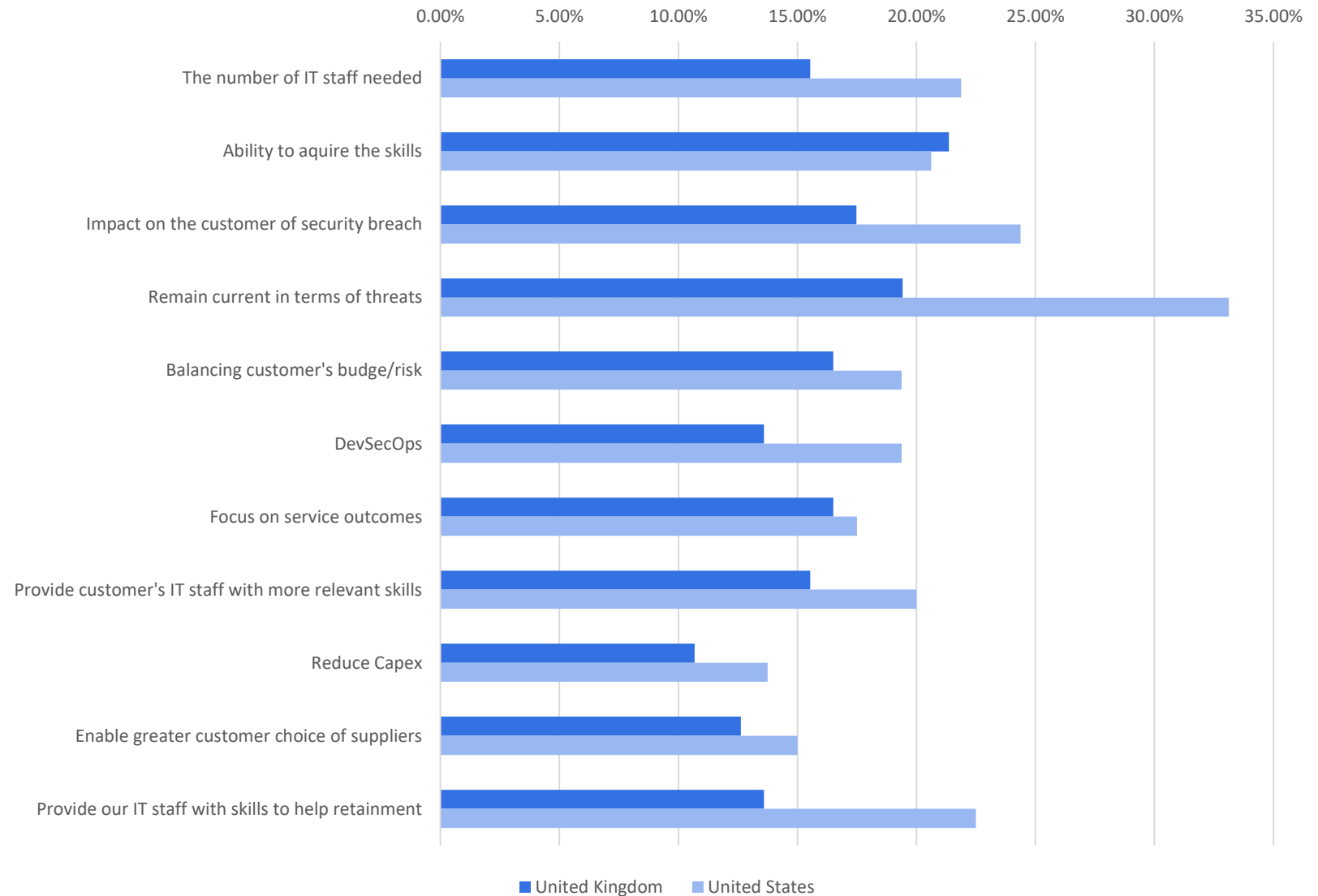
Figure 22: Most important challenge by MSP size in terms of revenue – delivering security as a service



People and process challenges with delivering security management as a service

- **Remaining current in terms of threats** was most important for US MSPs (Figure 23). This was also the challenge with the biggest difference between US and UK.
- **Skills** showed US and UK in agreement and this demonstrates **remaining current** is not directly skills related.
- This challenge can be linked to organizational obstacle **sufficient time and resources** – this was the only obstacle where 20% or more of both UK and US MSPs rated it most important (Figure 18).
- **Reducing Capex** through deferring purchases is lowest most important challenge for both UK and US MSPs.

Figure 23: Most important technical challenges with delivering security management by country



Technical challenges with delivering security management as a service

- **Early identification and isolation** is the top technical challenge for MSPs with less than \$5M in revenue (Figure 24).
- **Encryption as a default** for any service was the most important challenge for MSPs with revenues of between \$5M and \$50M (Figure 24).
- Integrating services, **integrated identity and access** as well as **integrating with other services** were joint most import for MSPs with more than \$50M in revenue (Figure 25).
- Top country only challenge is **encryption as default** compared to global where **early identification** is top challenge (Figure 25).

Figure 24: Top technical challenges by MSP size in terms of revenue

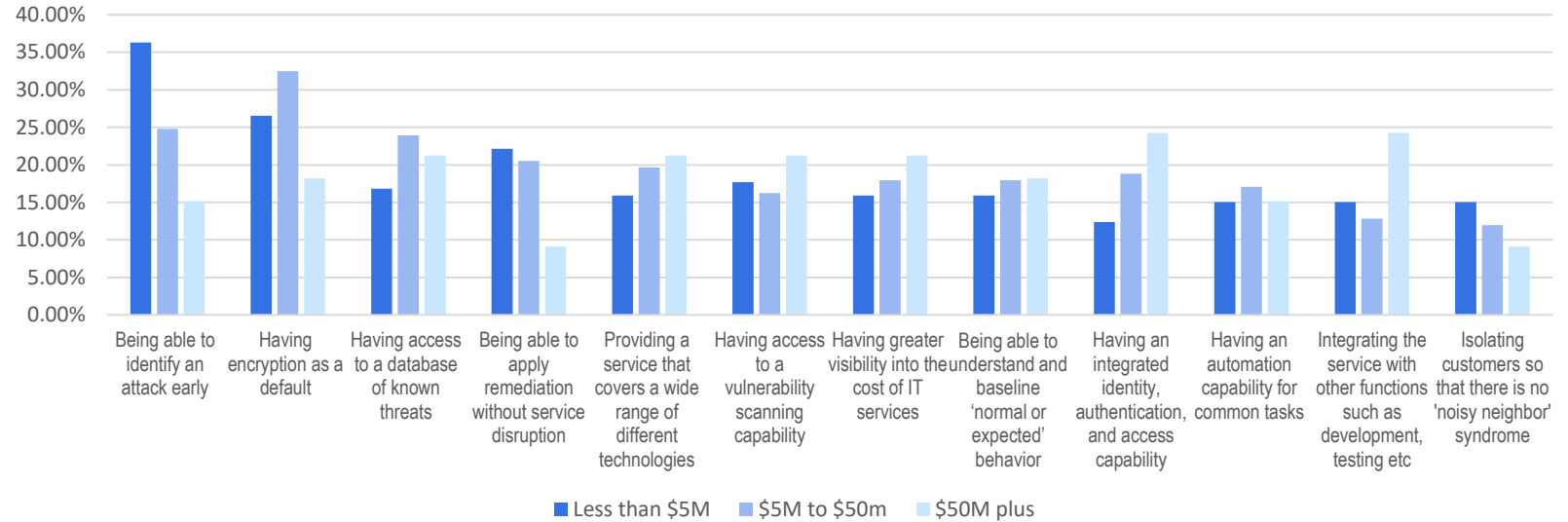


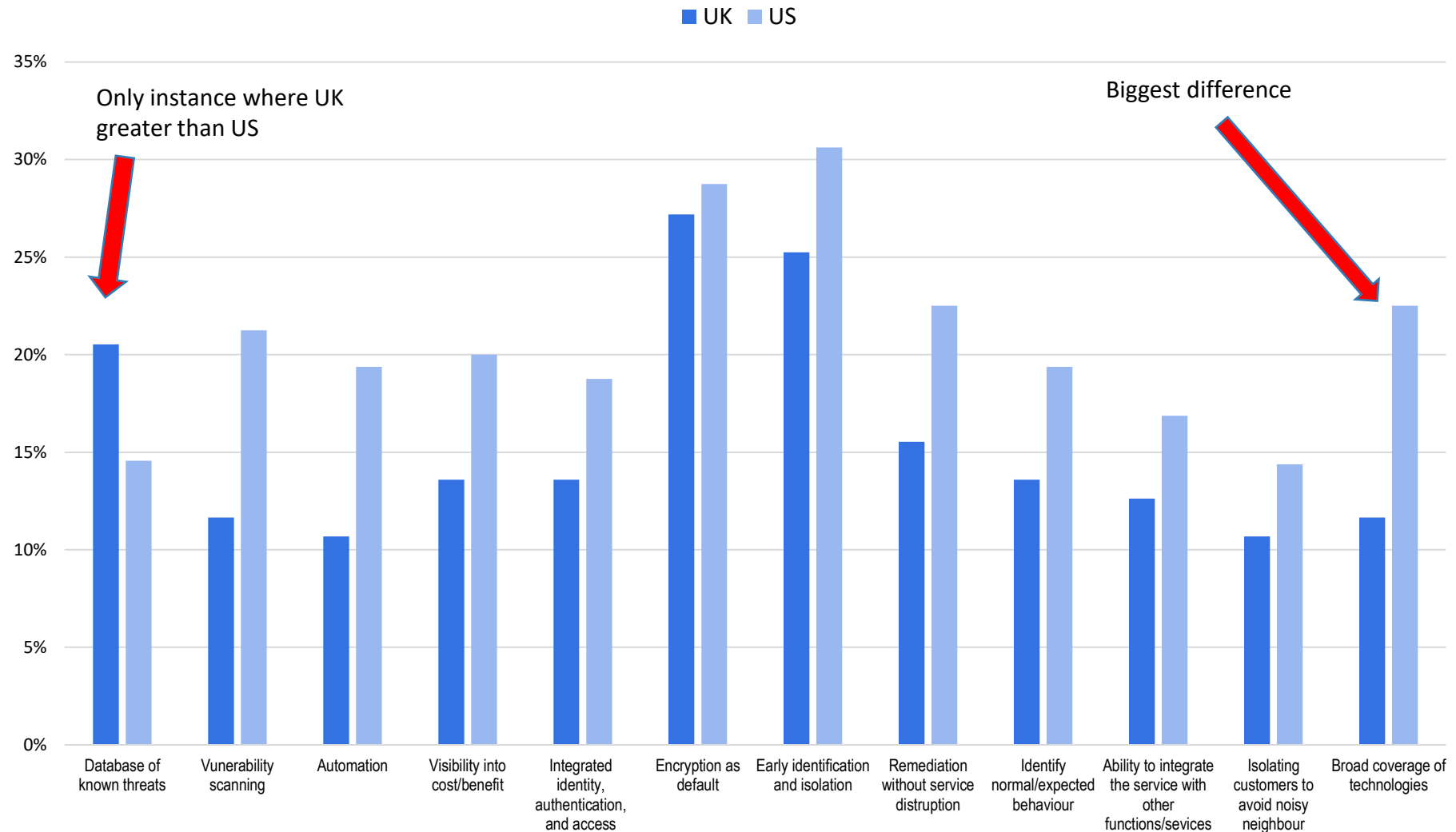
Figure 25: Top technical challenges by MSP coverage global v local



Technical challenges with delivering security management as a service

- UK MSPs place a **database of known threats** as the only technical challenge where it is more important than US MSPs (Figure 26).
- Top US technical challenge is **early identification** with over 30% putting it as most important.
- Top UK technical challenge is **encryption by default** with 27% putting as most important.
- Broad coverage of technologies** is the technical challenge with the biggest difference between UK and US responses.

Figure 26: Most important technical challenge by country



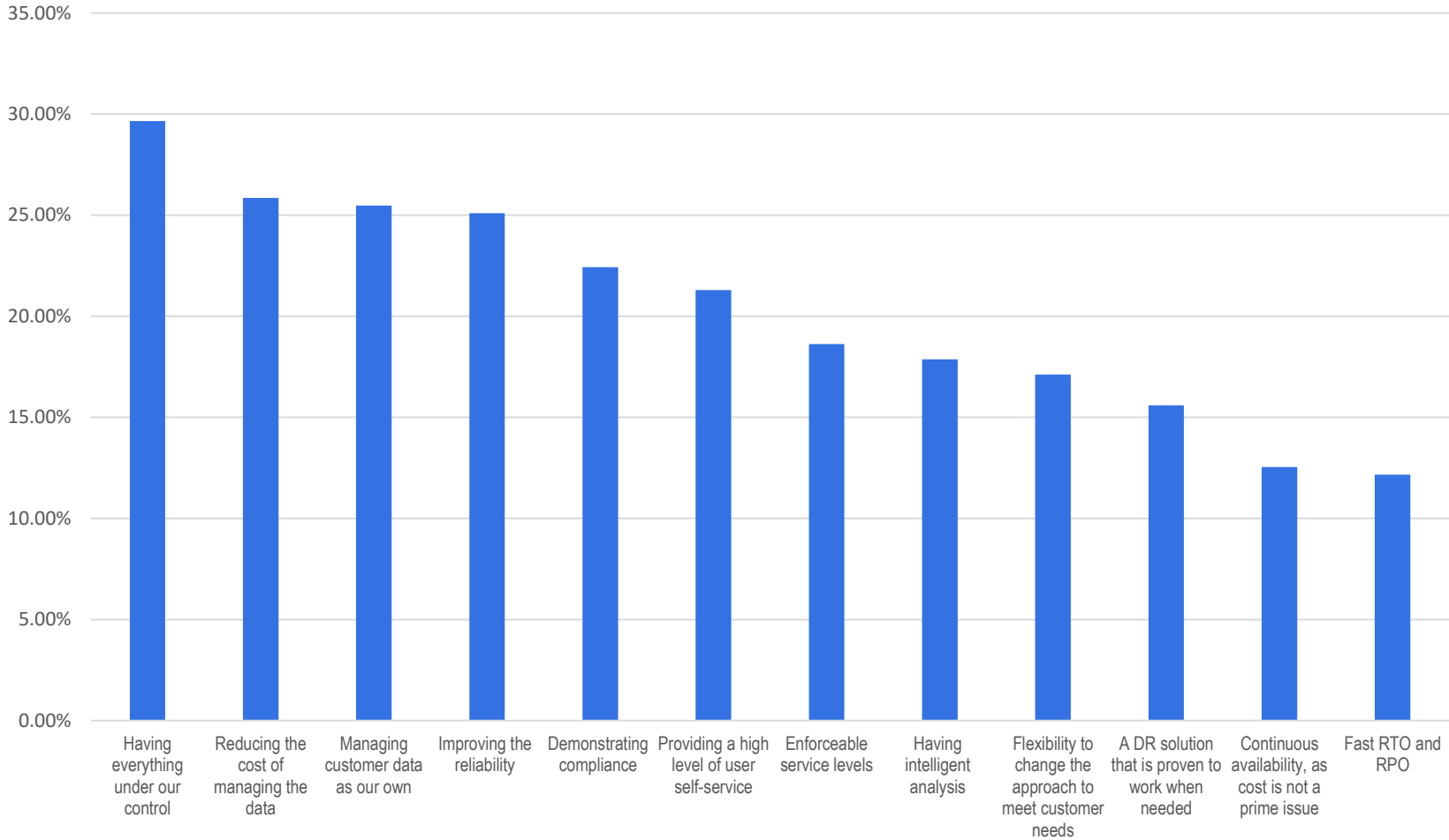
Key considerations for MSPs when selecting a supplier

Key MSP considerations and the
show stoppers preventing MSPs
using a supplier's technology

Supplier selection show MSPs want to control the delivery and manage the customer experience

- Most MSPs want to have **everything under their own control**, with nearly 30% selecting it as the most important consideration.
- **Reducing cost** was second most important, closely followed by **managing data as if was our own** and **improving reliability**. These three were all within 1% of each other and show a focus on customer experience.
- **Fast RTO and RPO** were the least important features when selecting a supplier.

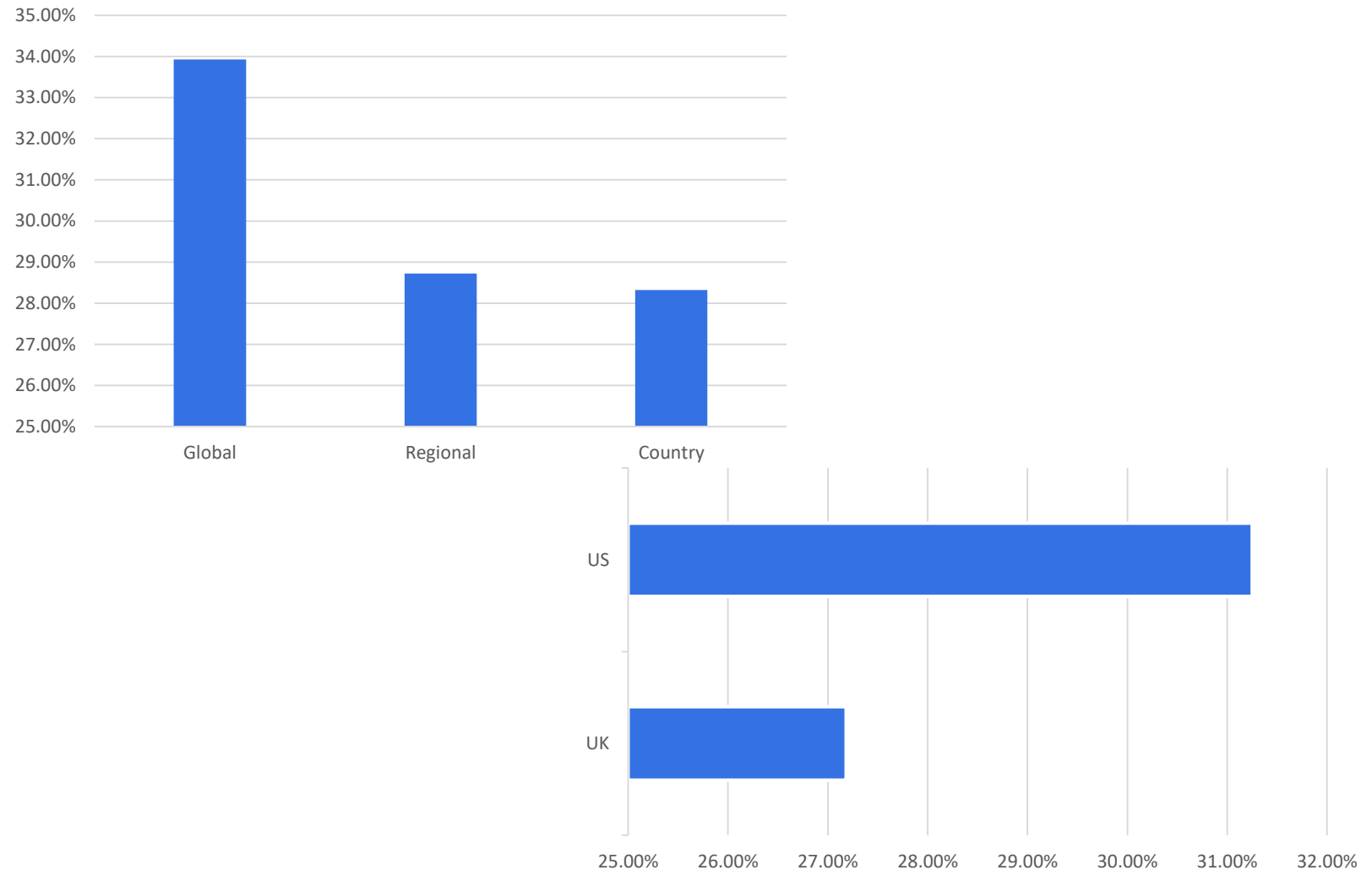
Figure 27: Most important considerations when MSPs are selecting a supplier



US MSPs place more importance on control than UK MSPs

- Global operating MSPs want to have everything under their own control (Figure 28).
- US MSPs are more likely to want to control all aspects of the service delivery than UK MSPs.
- Smaller (fewer than 19 employees) and mid-sized MSPs (20-99 employees) put **having everything under our control** as most important. Larger MSPs ranked it as the second most important consideration.

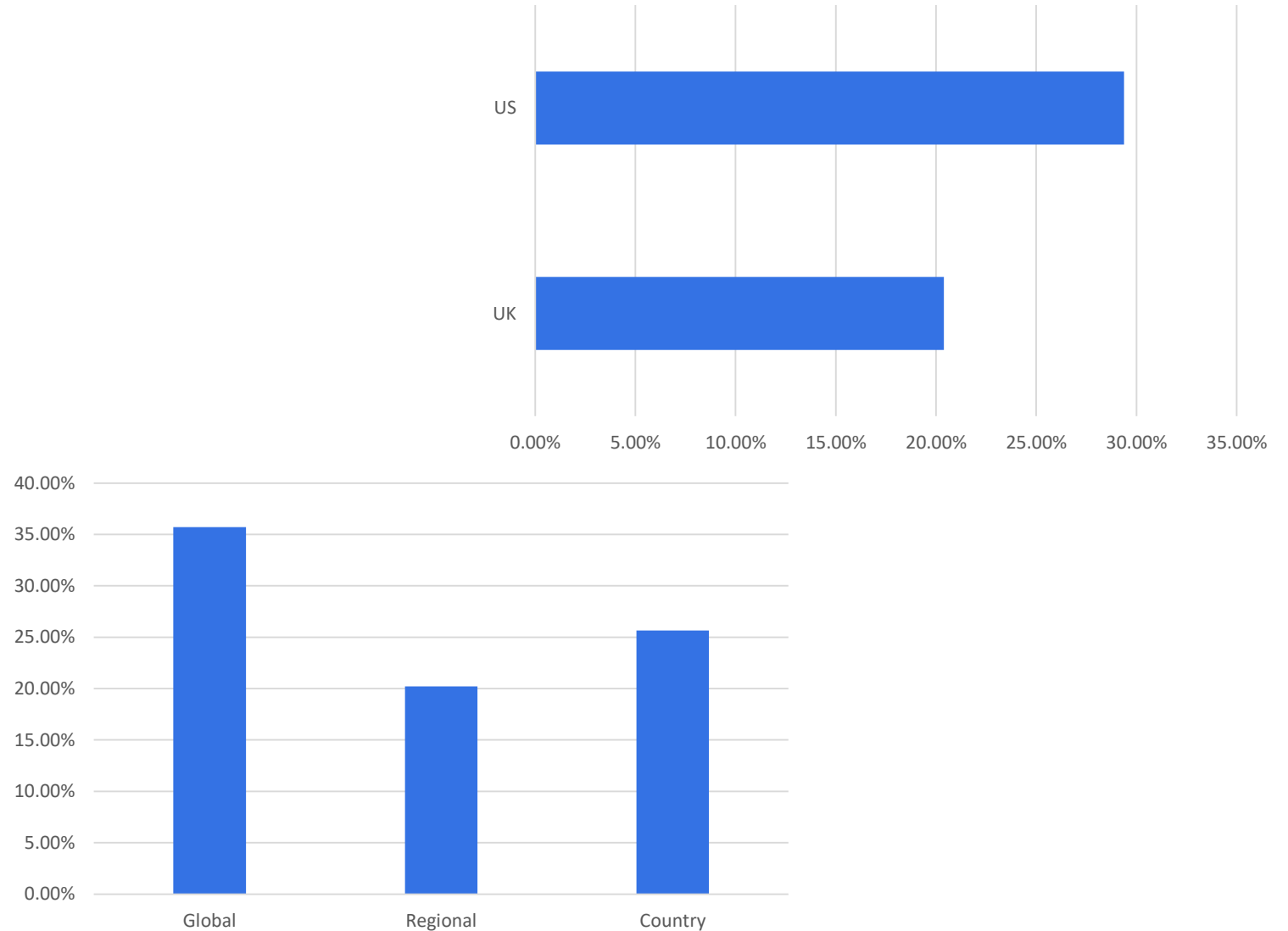
Figure 28: Having everything under our control deeper analysis



Global MSPs put cost reduction as top consideration

- In US **cost reduction** was second most important and is more important than in UK MSPs (Figure 29).
- In UK this was fifth most important with 20%.
- **Cost reduction** was of least interest to those MSPs operating regionally where it was fourth most important consideration.
- Global operators put **cost reduction** as the top consideration.
- **Reducing costs** was second lowest consideration for larger MSPs (greater than \$50M revenues) with 15%, compared to nearly double that from MSPs with revenues less than \$50M

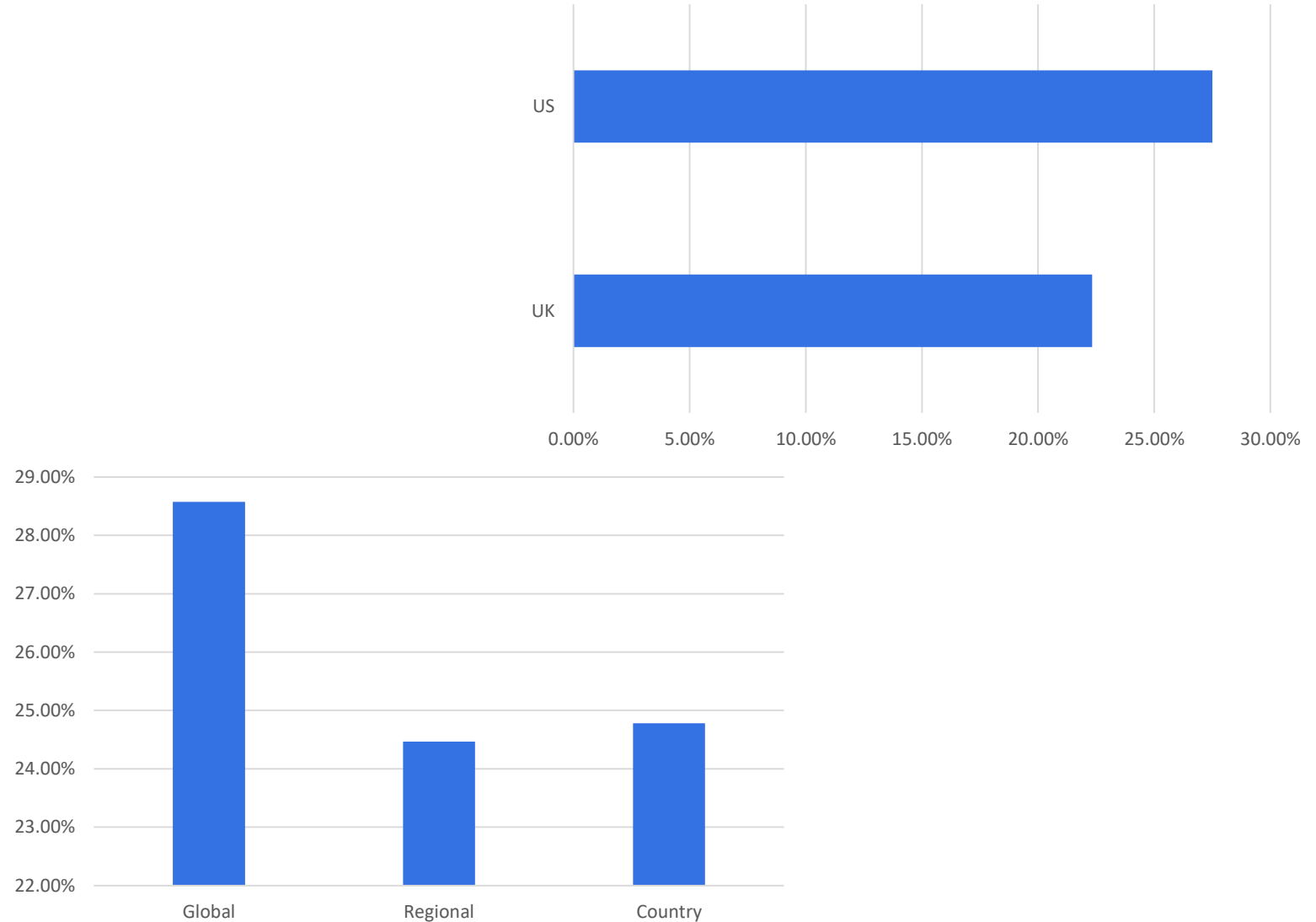
Figure 29: Reducing cost deeper analysis



Managing data was most important to MSPs with revenues of less than \$5M

- **Managing data like it is our own** is more significant to smaller MSPs
- MSPs with revenues less than \$5M rated it second most important with 30%, compared to \$6-\$50M where it was only 20% (joint-fifth most important)
- Geographic coverage was at odds though, with MSPs with a global presence scoring nearly 29% as most important compared to 24% for regional MSPs (Figure 30).
- US MSPs consider it more important than UK MSPs. UK # consideration was **improving reliability** with over 30% putting as a most important consideration.

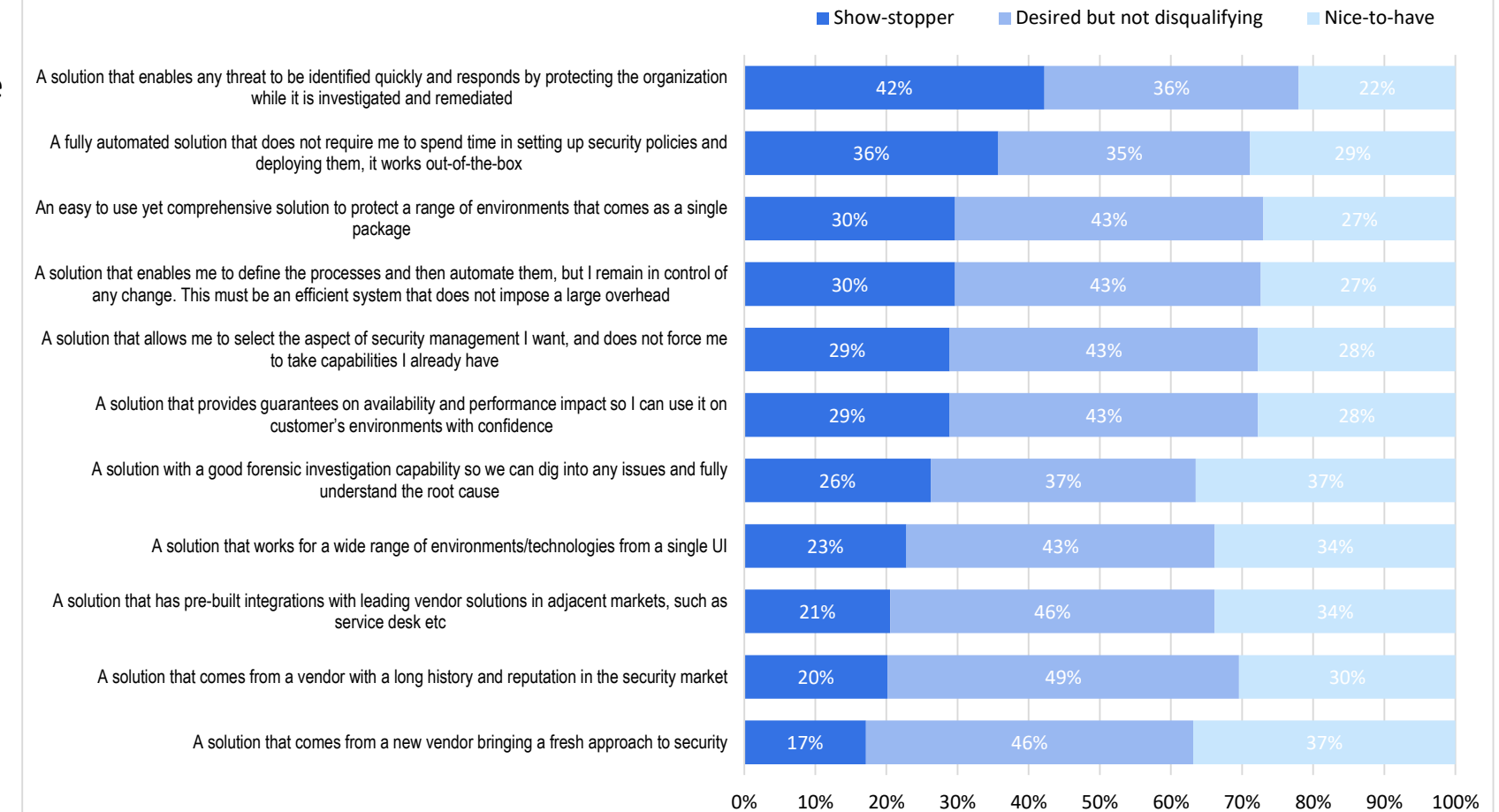
Figure 30: Managing data as our own – deeper analysis



What is stopping MSPs

- Lack of **fast identification** of incidents/threats and **automation** are the top 2 reasons given by MSPs that are show-stoppers when assessing security management solutions (Figure 31).
- UK top show stopper is **fast identification**, which is recorded 43% of respondents with a **solution that allows MSPs to select the aspect of security they want** was #2 with 33%.
- US top 2 (**fast identification and automation**) are broadly similar with 42% and 41% receptively.

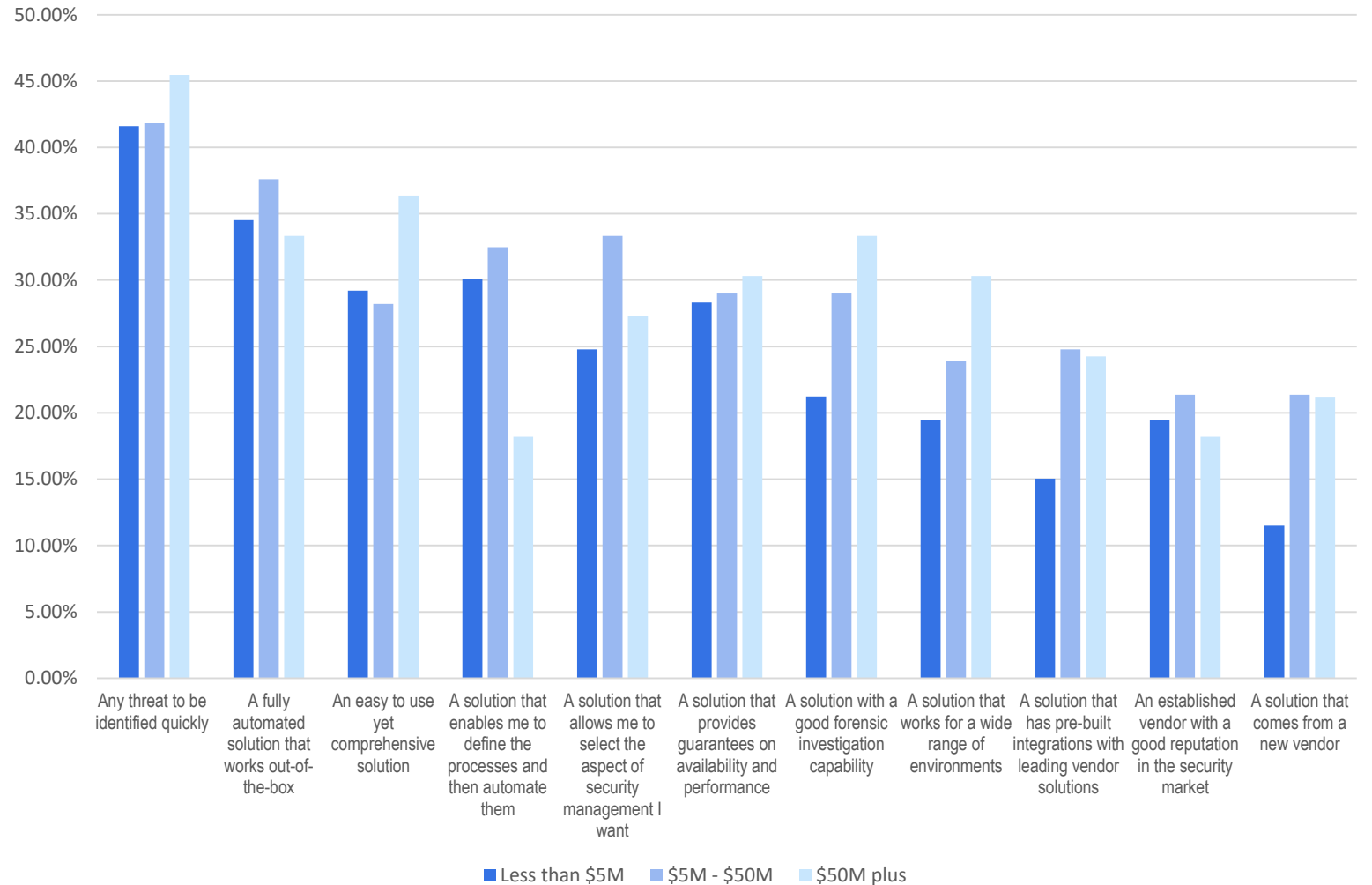
Figure 31: Attributes MSPs consider show stoppers for delivering security as a service



Show stoppers vary by MSP size

- Being able to **define processes and automate** them is of least importance to MSPs with more than \$50M in revenue (Figure 32).
- Smaller MSPs are less interested in **new security vendors**.
- A solution that provides **guarantees for availability and performance** is the attribute that shows most consistency across all MSP sizes.
- Regional MSPs put **rapid threat detection** most important with 50% saying it is a show stopper compared to 40% of country only MSPs, and 34% of global MSPs.

Figure 32: Top show-stoppers deeper analysis

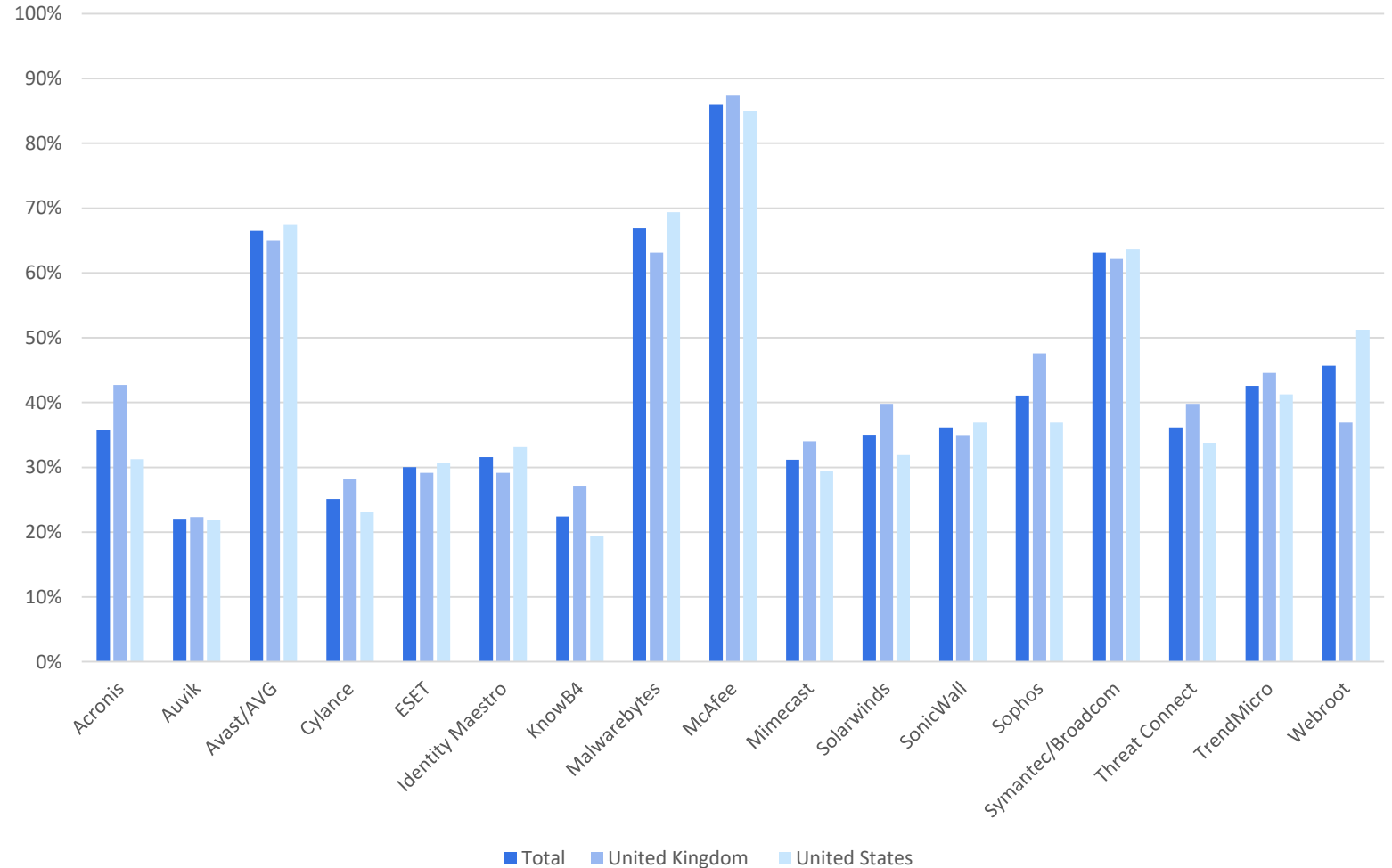


MSPs views on the vendors

Vendor perception

- **McAfee** is most well-known vendor – potentially because it has a strong name in both consumer and business environments
- Not much variation between US and UK MSPs in terms of known vendors
- **McAfee** with 52% is top current supplier
- **Symantec/Broadcom** #2 current supplier with 30%

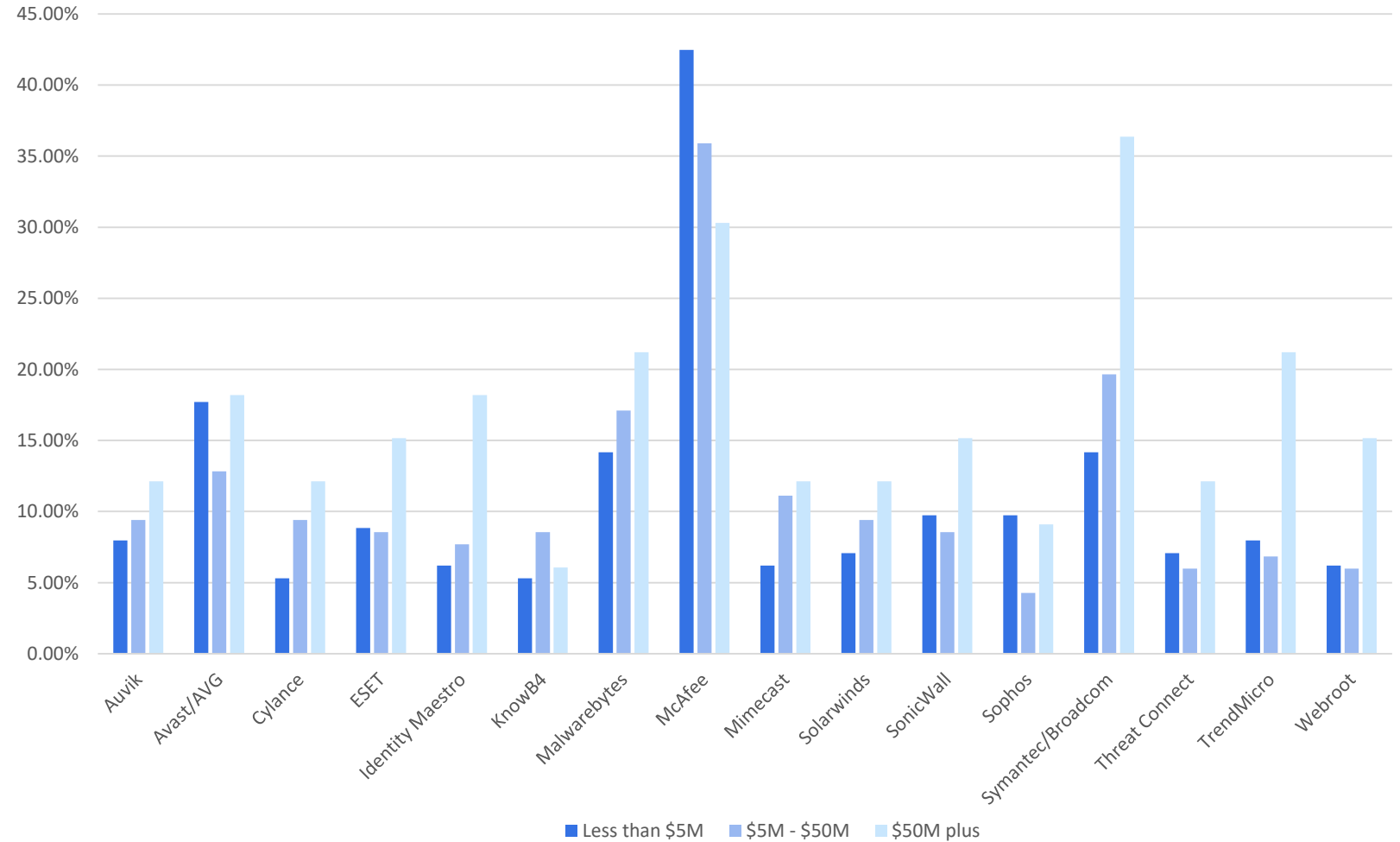
Figure 33: Known vendor



Market presence is dominated by McAfee

- **McAfee** has a much higher market presence than any other vendor (Figure 34).
- **McAfee** is top market presence in all MSPs with less than \$50M in revenue.
- **Symantec/Broadcom** have biggest market presence in MSPs with revenues of greater than \$50M.

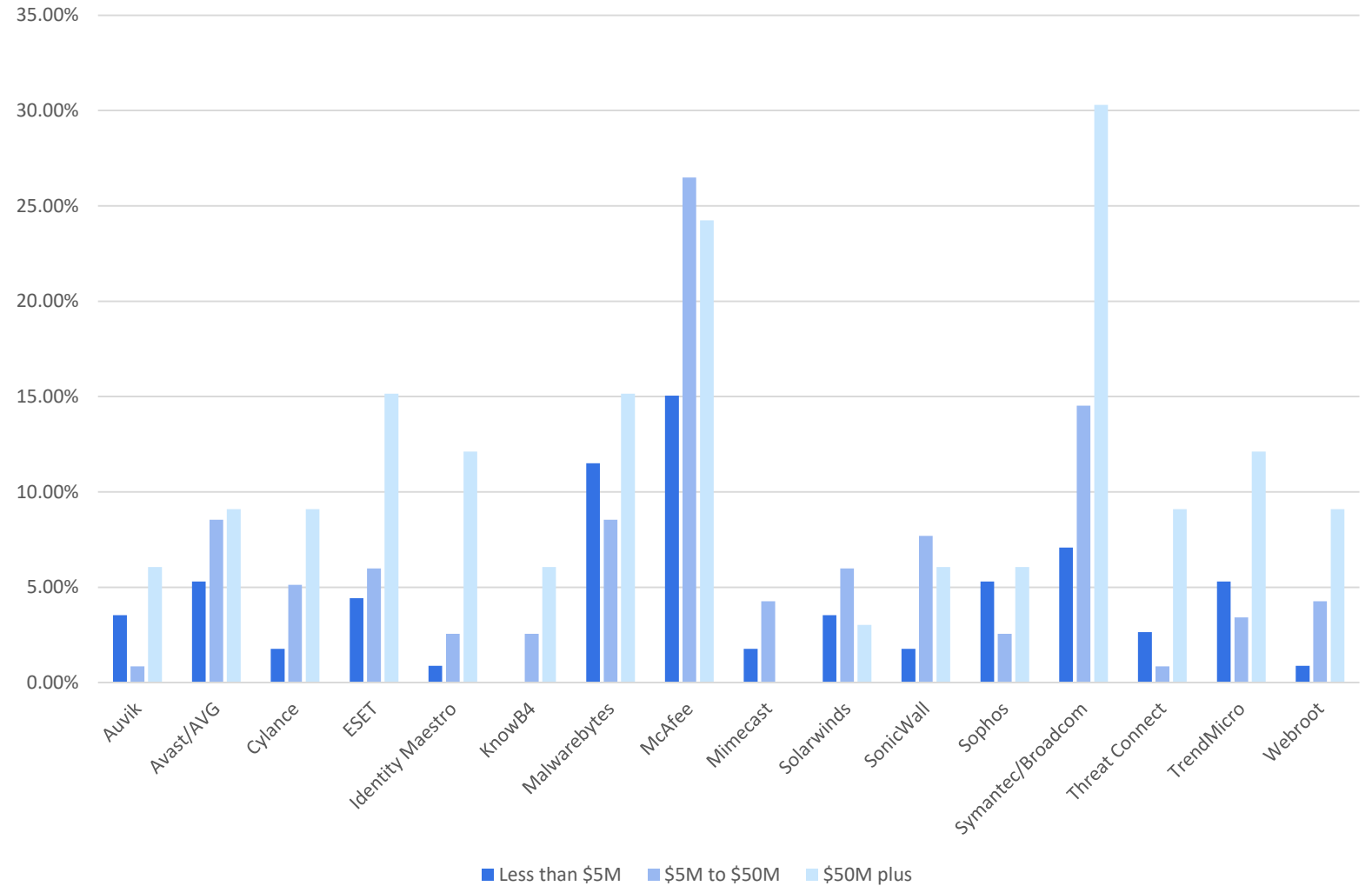
Figure 34: Market presence by vertical industry leading



Symantec/Broadcom recorded the largest industry leading score in value for money

- **McAfee** was strongest in value for money in MSPs with revenues less than \$50M (Figure 35).
- **Symantec/Broadcom** is #1 in MSPs with revenues over \$50M, and recorded the top score of nearly 30% in this group.
- **KnowB4**, **ThreatConnect**, and **Mimecast** all recorded entries where 0% considered them as industry leading.

Figure 35: Value for money industry leading by vendor



Summary

Summary

- The needs of MSPs vary by the size and scope of their operations, with pricing being particularly sensitive. Those working globally rate this more than twice as much of a problem as those with operations in country only.
- Minimizing data loss is the clear top security capability, but this varies significantly by MSP size. Zero downtime is the fastest growing security capability.
- Automation and ransomware protection are most important backup capabilities. These indicate customers are looking more broadly at where threats are coming from and how to mitigate them quickly.
- Security as a service is what customer want from MSPs, MSPs want to have everything under their own control, so any supplier to MSPs must be able to deliver:
 - Rapid identification of incidents.
 - Automation to overcome the lack of skills.
- The biggest vendor in the target market is McAfee – in terms of both perception and actual presence, followed by Symantec/Broadcom.

Thank You

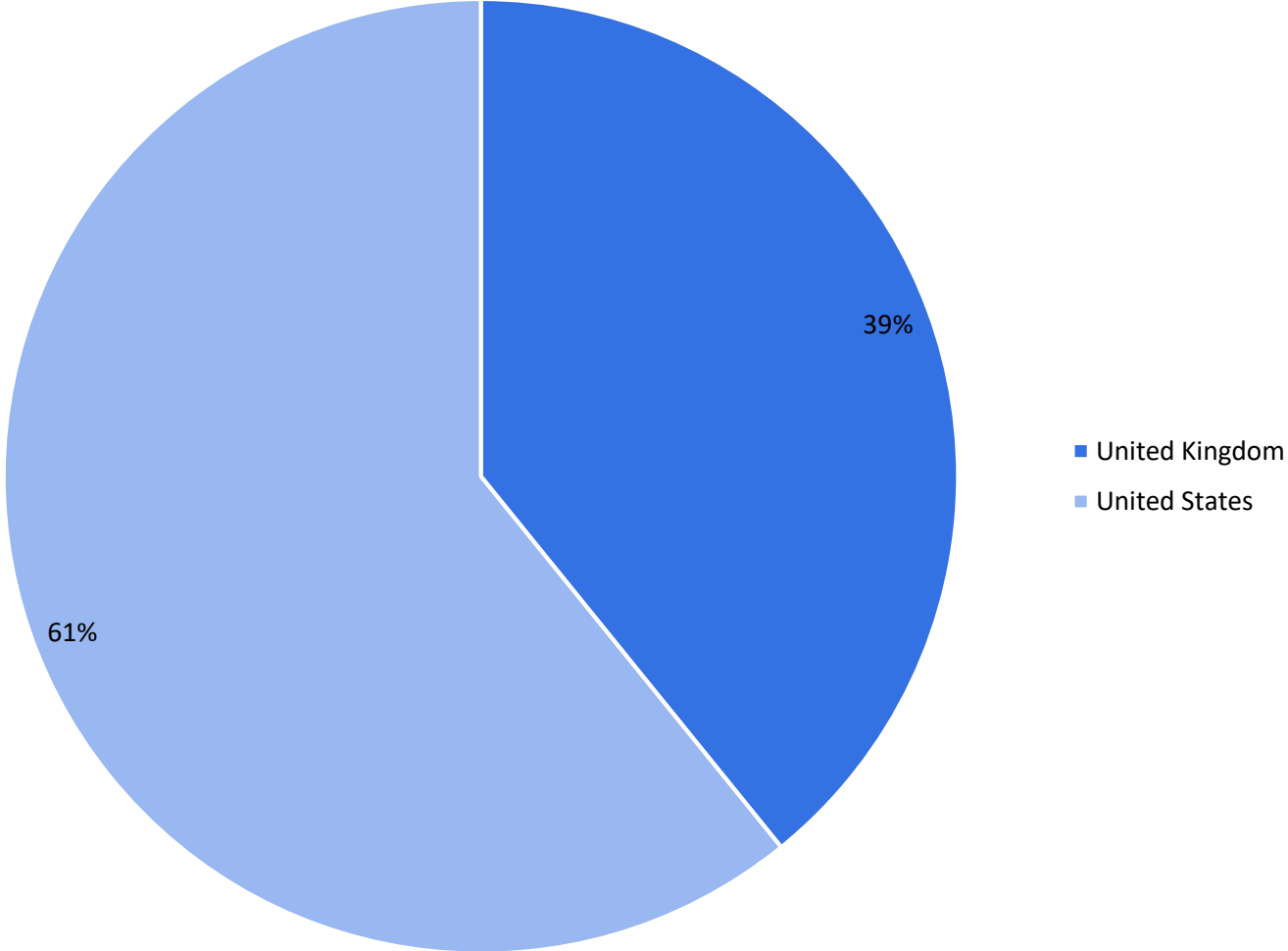
Sponsored By

Acronis

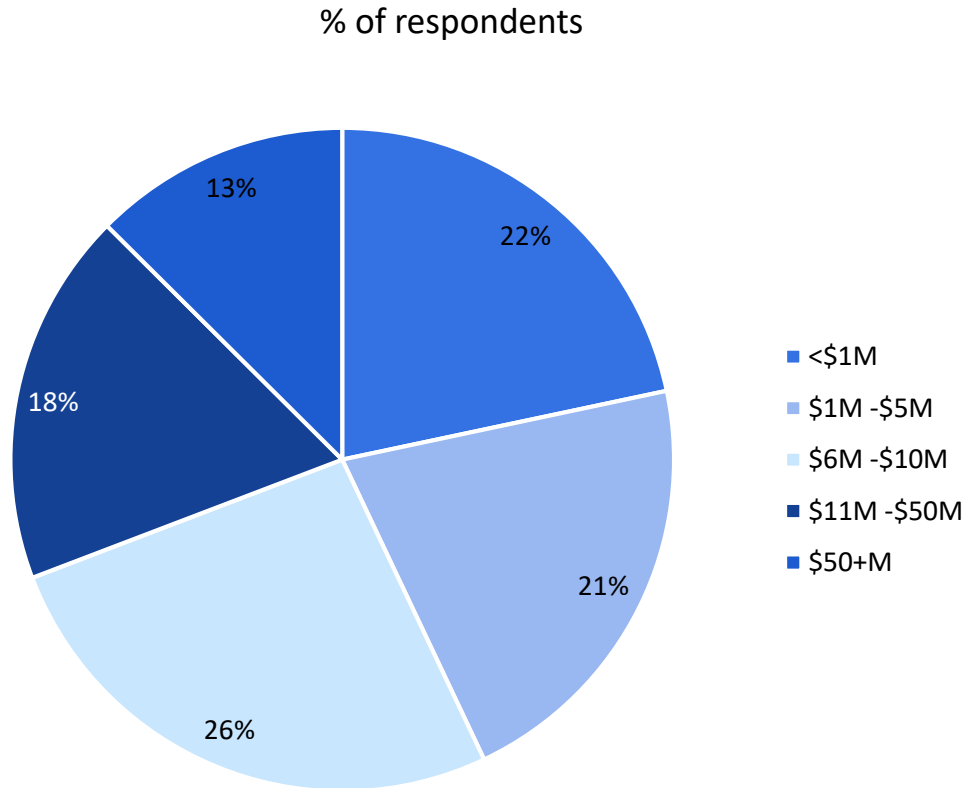
Learn more about
Acronis Cyber Protect Cloud,
the AI-powered integration
of data protection and
cybersecurity.

Survey demographics

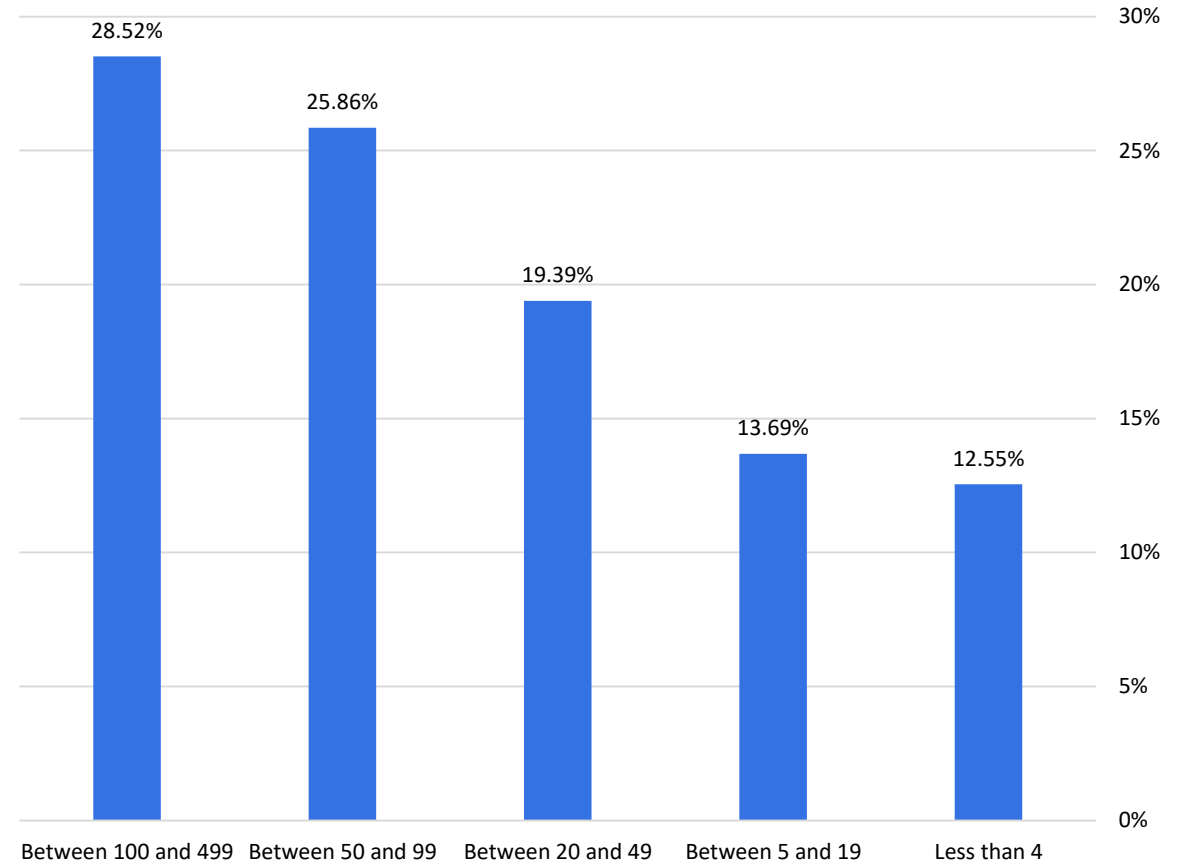
Split between UK and US



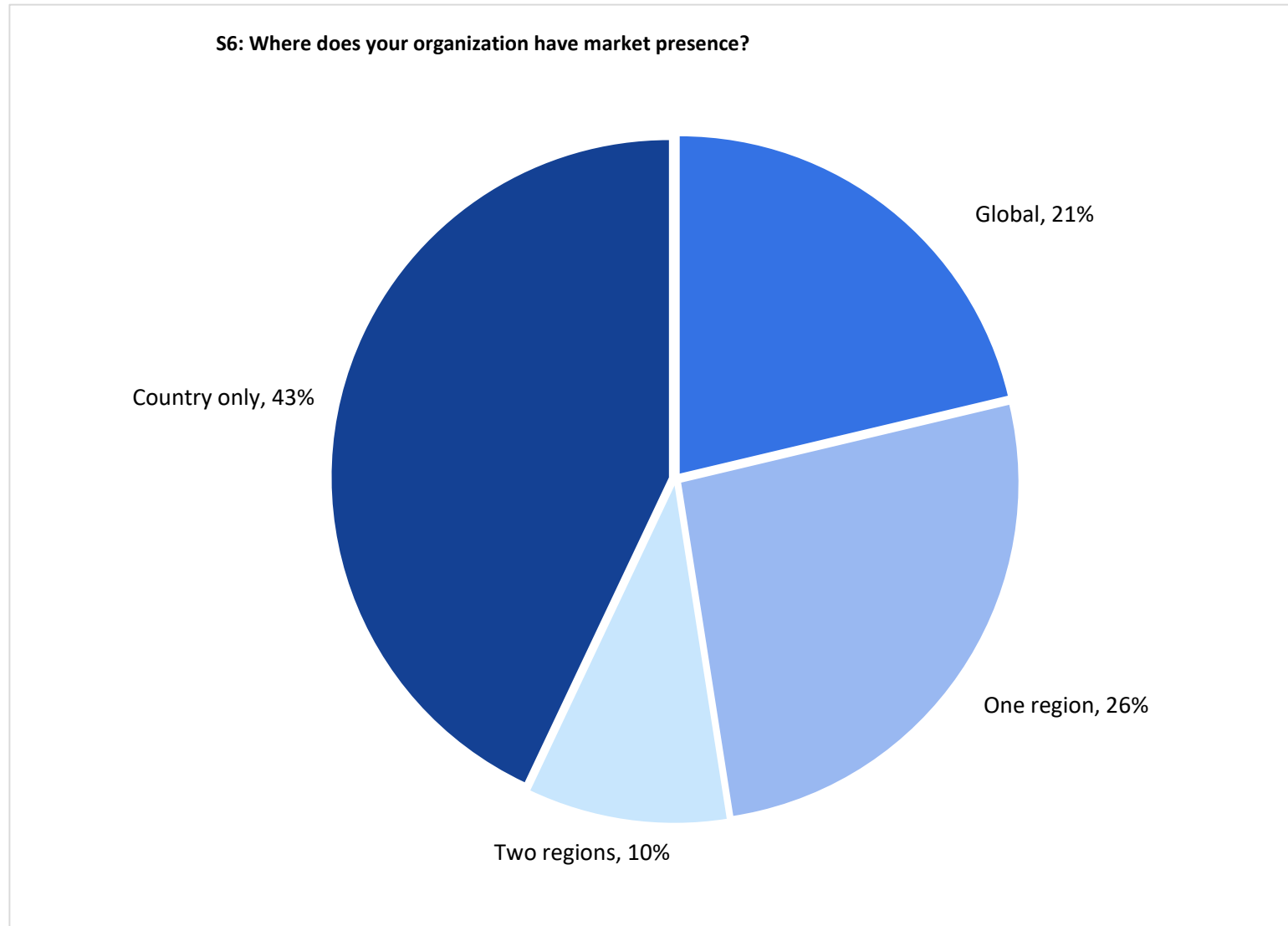
MSP's revenue profile



Number of employees at MSP



Geographic presence



Thank You

Sponsored By

Acronis

Learn more about
Acronis Cyber Protect Cloud,
the AI-powered integration
of data protection and
cybersecurity.