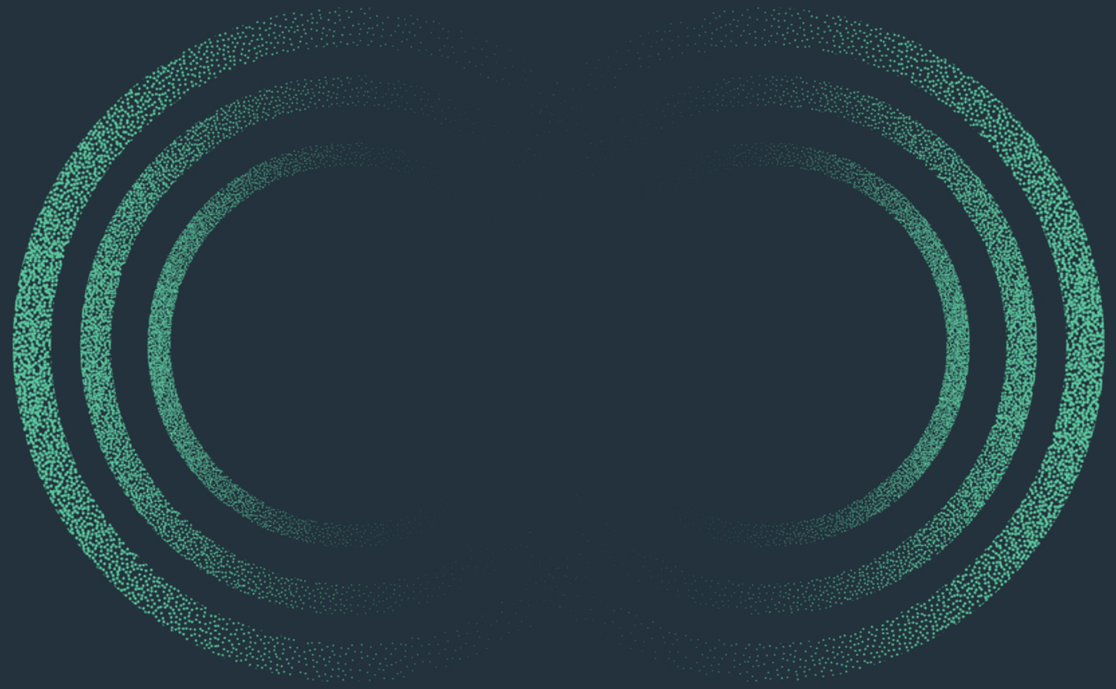
WithSecure™ Pulse 2023

All you need to know about the latest IT and cyber security trends

W / T H secure

Contents



Executive summary

Introduction

Our global market research survey asked thousands of IT professionals a series of questions about their jobs, organizations, and priorities for the upcoming year. The resulting data can be used to inform your IT and security strategies in 2023 and beyond.

Pulse 2023 reached 3,072 respondents across 12 countries: the UK, France, Germany, Belgium, Netherlands, Denmark, Finland, Norway, Sweden, as well as the US, Canada and Japan. All respondents were security decision makers and influencers in IT, network, and cloud spaces, responsible for purchasing IT security products and services for their organizations.

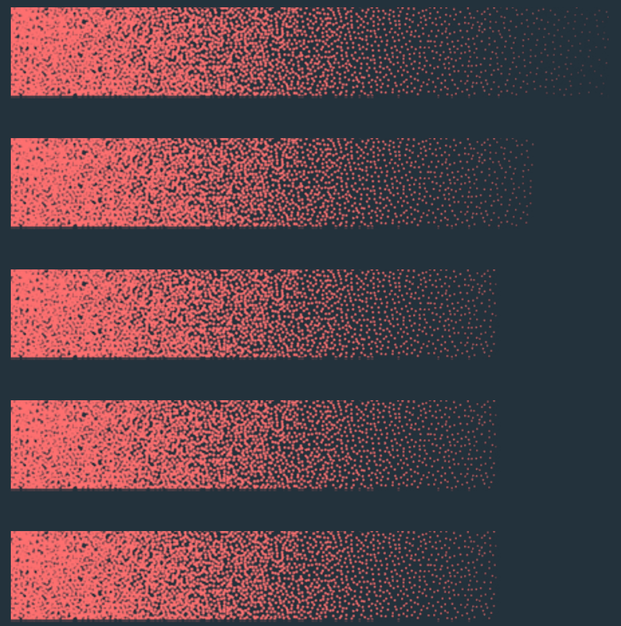
To get the insights most valuable to you, use our personalization features to see data that is relevant to your industry, region, and role type.

Security Priorities for 2023

Our survey respondents told us their biggest business and technical priorities for the coming 12 months. The top five priorities for cybersecurity leaders are:

Our deep dive article on security priorities (starting on page 10) outlines the trends we saw in our Pulse 2023 survey.

Biggest technical security challenges (Top 5 responses)



34% Preventing data breaches

29% Ensuring protection against malware and ransomware

27% Preventing advanced e-mail based threats, such as phishing or business email compromise (BEC)

27% Ensuring security of cloud-based collaboration applications, such as Office 365 and Salesforce

26% Ensuring the security of an increasingly diverse pool of devices, services and software

"The interesting point is that the options that no one chose as their priorities are the things that make the most difference when it comes to security posture; from experience, these are the competencies and practices that many organizations are missing."

Peter Page, WithSecure™ Head of Solution Consulting

Security Spend

Amid all the noise around cybersecurity, perhaps the most important issue for companies is the bottom line. Just how much are we supposed to spend on security? Is any amount enough? Does it depend on how many seats we have, our geographical location, or the type of industry we are in? Are my peers as concerned about how much they are spending – and how much of their budget are they allocating to this?

Our research produced interesting insights into how organizations spend on cyber security. The data suggests that as companies evolve their strategy, cost is becoming a less critical factor.

86% of respondents say their security budget intentions will increase in the coming 12 months.

“I always say you should start at an absolute minimum of 5%. Now, that is without any caveats: the more vital security is for the customer, the higher the percentage. And vice versa."

Teemu Myllykangas, Director, B2B Product Management at WithSecure™

“Companies need to decide how much security they want. They need to agree how much risk they're willing to accept, how much business disruption they can tolerate and what appetite they have for taking risk. Based on what they decide, rational security spending decisions can be made.”

Paul Brucciani, Head of Product Marketing at WithSecure™

Data Residency

Our 2023 Pulse survey showed that people in IT have strong opinions about where their organization's data is stored and processed. Not surprising: rules and regulations about data – and plenty of examples of data misuse and abuse – make this topic both heavy with consequence and emotive for many.

Opinions tended to differ among people from organizations of different sizes, as well as those working in different regions and industries.

When there is so much disagreement about the right way to handle data, how can a consensus be reached? Does an organization's data residency policy affect its relationship with customers? More often than not, regulators and privacy campaigners are powerful influences.

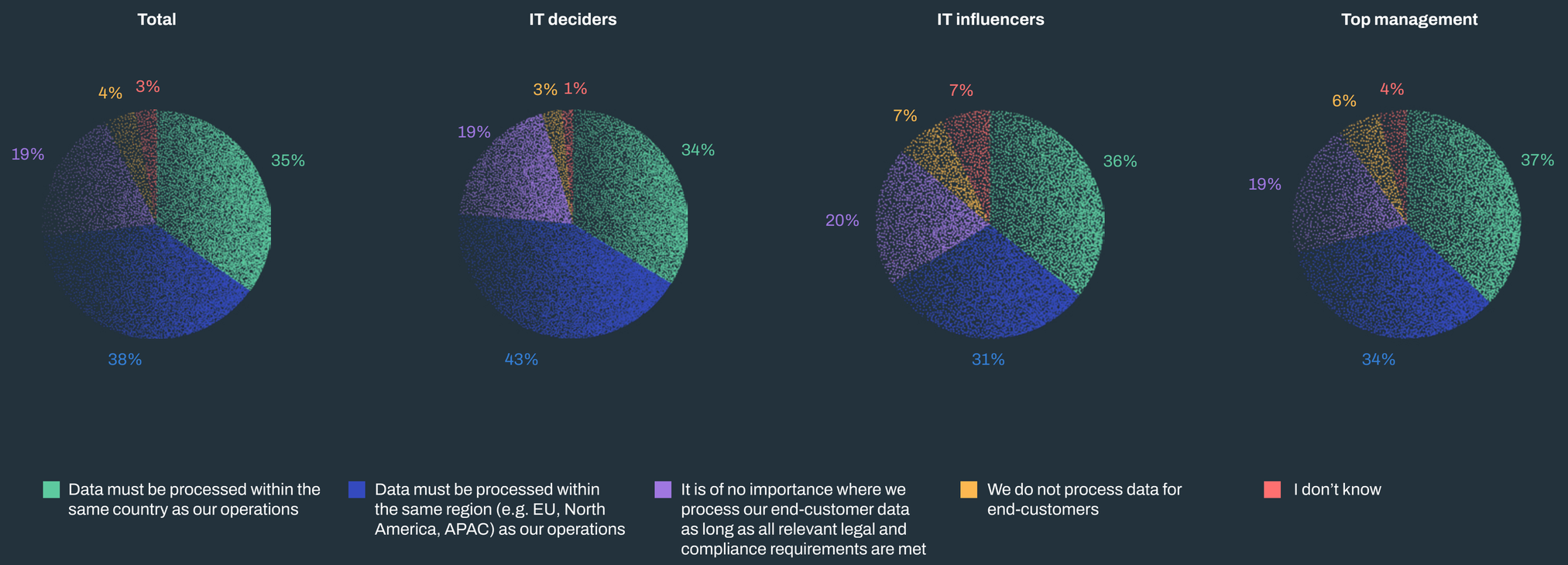
Perhaps the most important question is why differences in opinion exist at all. Disagreements and misunderstandings can cause problems, particularly between IT influencers and deciders in the same organization. When it comes to privacy and protection, there is no room for error.

"Data residency is something you have to consider as a company operating today. The reason being is that you might have customers who care about national security issues, and you as a start-up, for example, might have provided your software as a service product utilizing American cloud service providers. Is that something you can continue doing, can you continue to innovate at the same pace as previously, or do you have to find an alternative solution to that? That is something you need to consider."

Albert Koubov Gonzalez, Consultant, WithSecure™

Where you keep the data

How important is geographic location to data processing in your role?

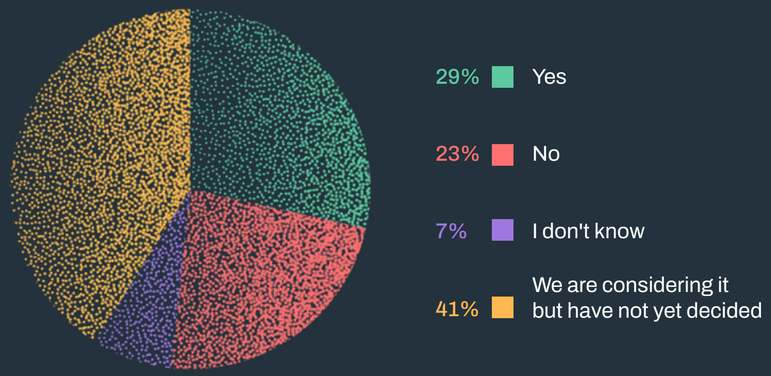


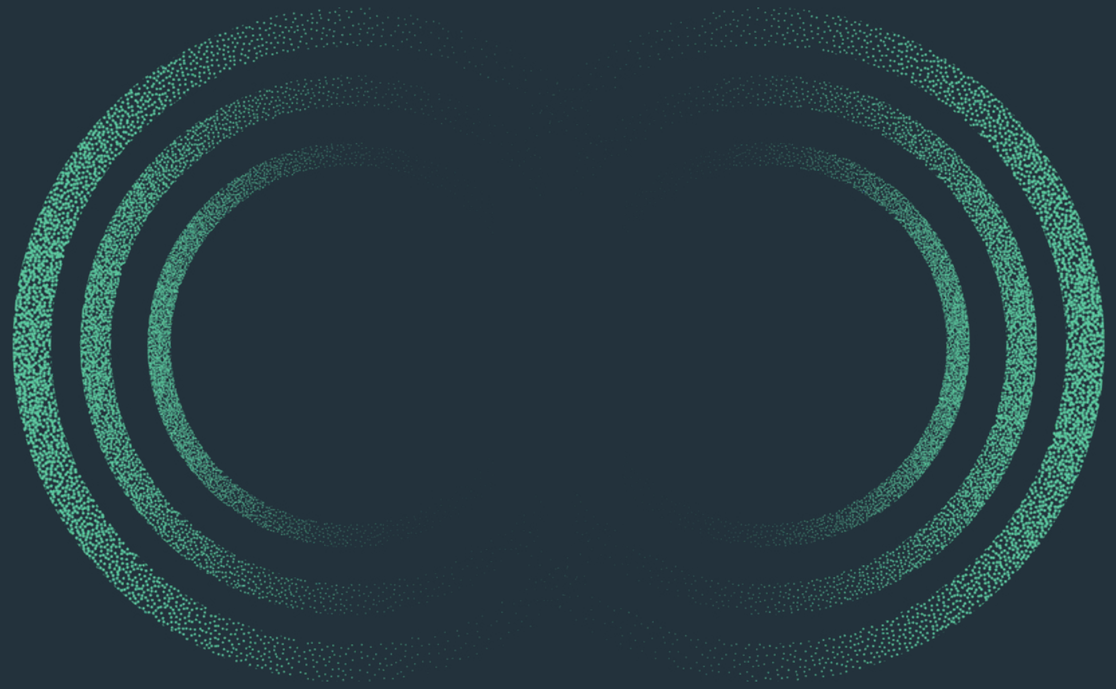
Vendor Migration

Changing security vendor is an enormous undertaking. It is a huge time and resource investment. Despite this, our Pulse 2023 survey shows that more 30% of respondents changed their vendor in the last six months, and the same proportion are planning on changing their vendor in the coming six months.

This indicates that a massive wave of vendor migration is underway. Why - and what - will be the cost?

Does your company/organization plan to change your business IT security solution/vendor in the next six months?

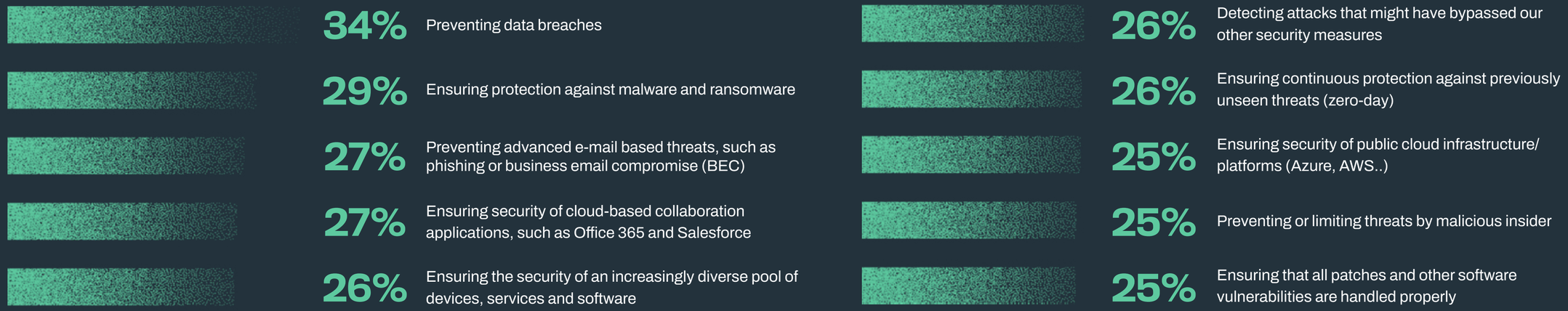




1. Security priorities for 2023

Technical security priorities

Biggest technical security priorities

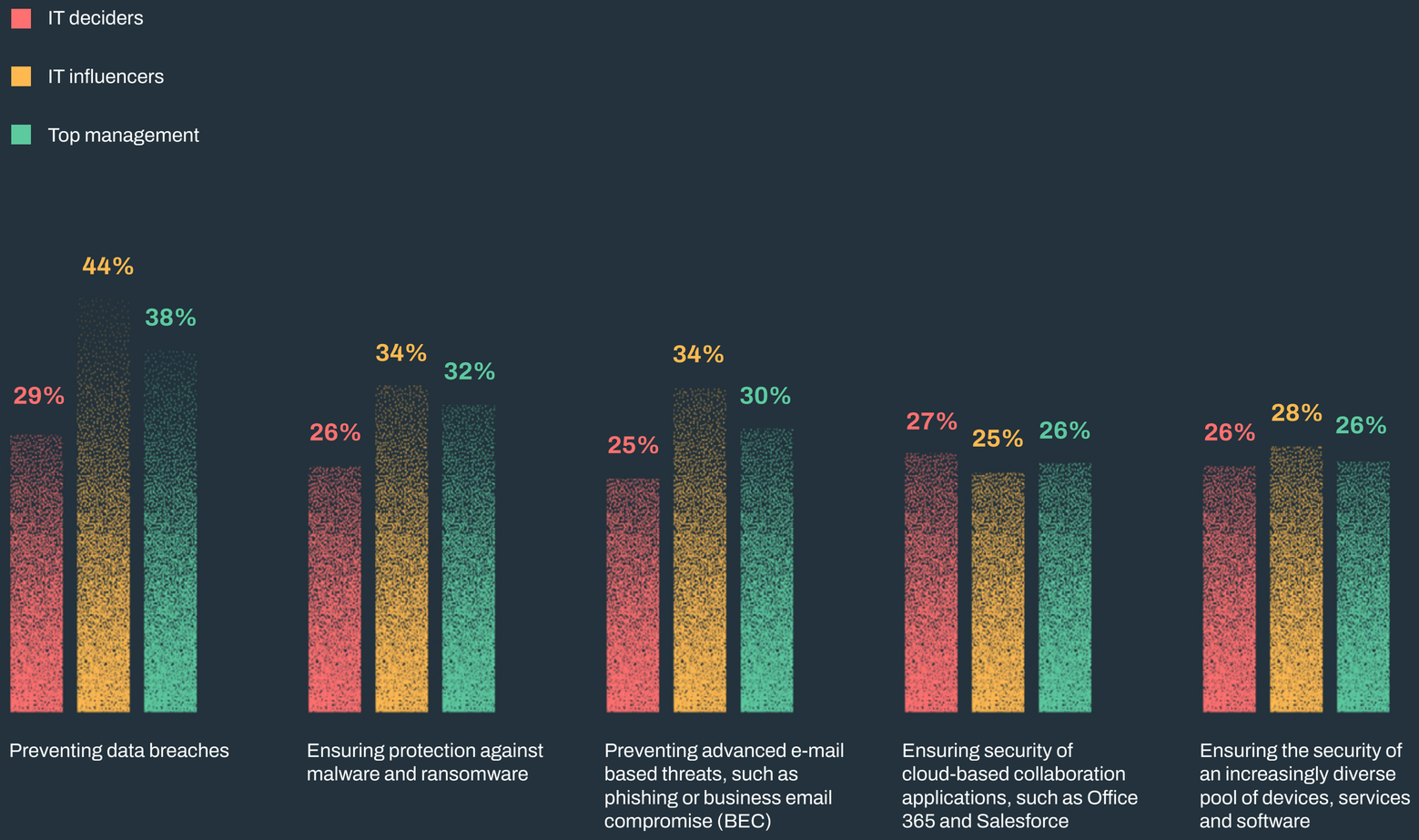


The results show that there was a broad consensus about which technical priorities are the most worrying. The top challenge is predictably 'preventing data breaches' (33.7%). Preventing e-mail based threats and ensuring the security of cloud-based collaboration applications, such as Office 365 and Salesforce, also score high on the list. The other priorities that were chosen generally fit the theme of threat detection and response.

"The interesting point is that the things that make the most difference when it comes to security posture are missing from the top priorities; from experience, these are the competencies and practices that many organizations are missing. Everyone is concerned about preventing attacks using solutions such as EDR and consulting, but both are crucial. EDR is something that needs to be in place in addition to EPP in order to create a watertight solution. Further, the BAU stuff that has real lasting impact is overlooked because it needs to be driven internally and is often a lot of really difficult work—building a security culture is not something you can outsource."

— Peter Page, WithSecure's Head of Solution Consulting

Top 5 technical challenges 2022/3 split by role type



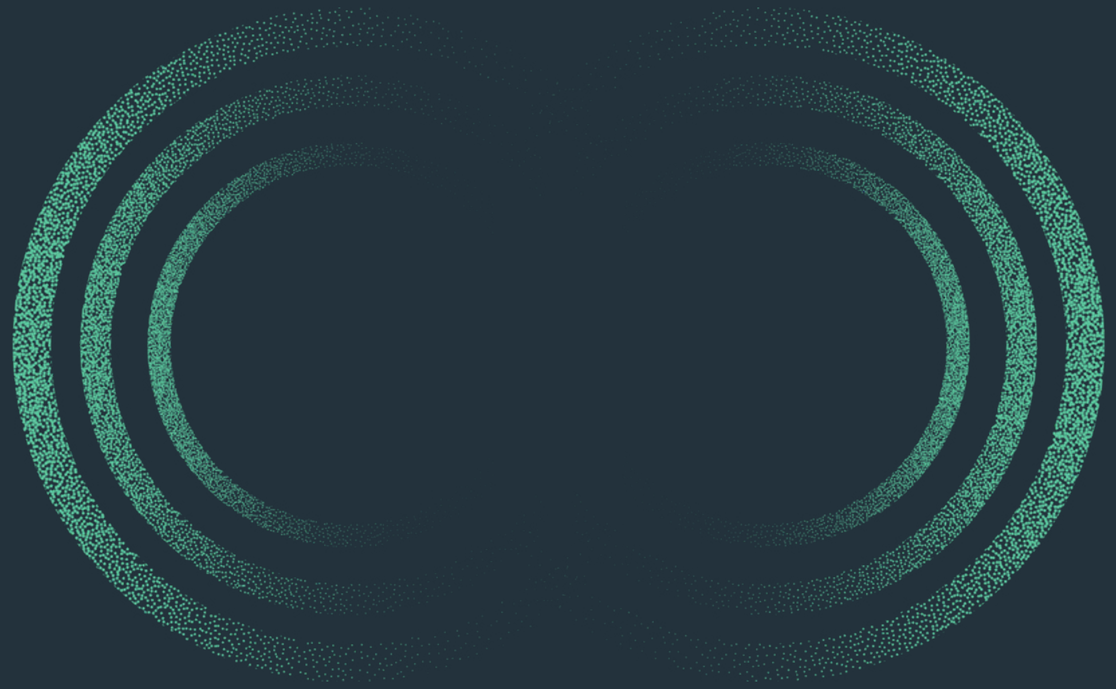
This data show the proportions of IT Deciders, IT Influencers, and Top Management prioritizing the overall top five technical priorities in 2023. Again, there seems to be broad agreement between our respondents on what the biggest priorities right now are. Where there are discrepancies (for example, between IT Deciders and IT Influencers about ‘preventing data breaches’), it might be worth checking in and ensuring that everyone on your security team is on the same page.

Business security outcomes

Biggest business challenges

“It’s not surprising that people are most concerned about the challenge of securing remote workers. There was a massive shift in ways of working in 2020, and there has been a lot of guidance and advice in this area to help organizations adapt. That has meant large scale projects for many people, involving changing IT architecture (for example, migrating to cloud) and re-educating employees. But while this is obviously a prevalent concern right now, I would hope and expect that by the time this survey is repeated in 2024/5, most organizations will have reached a stable point where they have adapted and everyone is used to the new ways of working.”

— Peter Page, WithSecure’s Head of Solution Consulting



2. Security spend

How much should I be spending on security?

It's a question asked the world over by thousands of companies, but how much of your IT budget should be put aside for cybersecurity?

The global information security market is expected to be worth USD 174.7 billion by 2024. This is a stunning statistic that shows the increased importance of cybersecurity as the world continues to change. This would suggest that companies are reacting to the raised threat by investing more in their security.

Due to a number of factors, such as more sophisticated attackers, remote work continuing and the global geopolitical situation, just how much security is enough and what should companies pay to obtain it?

WithSecure's research revealed that 87.9% of EU-based companies are planning to increase their security budget over the next 12 months. Perhaps more surprising was that 8.3% feel they are adequately covered or will actively look at reducing their cybersecurity spend.

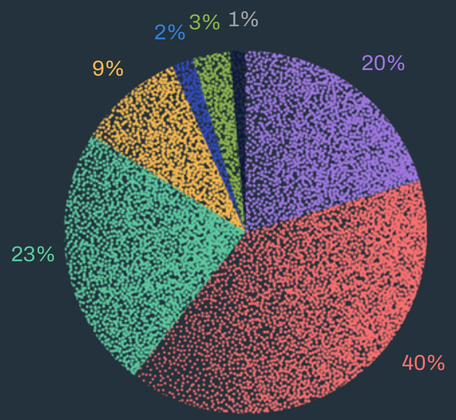
There also appears to be a disconnect between the groups as to what the budget will look like for the next year; while IT Deciders and Top Management respondents seem broadly in step, IT Influencers sometimes have significantly different budget expectations. Early and clear communication to your stakeholders on this topic is vital to avoid confusion or last-minute decision making.

Teemu Myllykangas, Director, B2B Product Management at WithSecure™, is well versed in this area. *"When you ask a company if they are spending enough, they have a hard time answering. If they say yes, then any breach will come back to bite them hard as people will want to know how they were breached despite the investment that was supposed to protect them. If they say no, then those same people should question whether they are doing their job correctly and securing the business. There is no easy answer to this question – anyone who says otherwise is either lying or trying to sell you snake oil."*

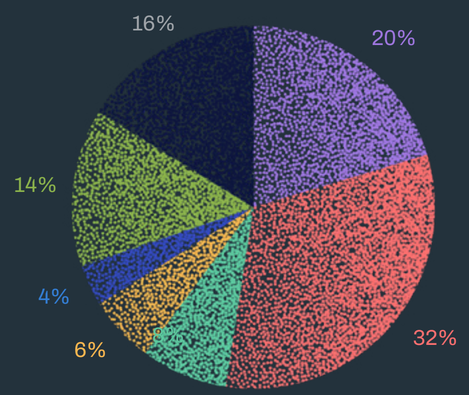
Within the industry, it is generally accepted that businesses are spending between 3% and 15% of their budget on security each year. When pushed by customers on where they should fall in this category, Myllykangas is wary. "*I always say you should start at an absolute minimum of 5%. Now, that is without any caveats: the more vital security is for the customer, the higher the percentage. And vice versa. I usually break it down into three steps: start with risk assessment and threat modeling to define ROI, decide how you use that money in an appropriate way using a well-known, basic security framework; review numbers one and two annually to identify the point of diminishing return and manage your budget.*"

Security budget intentions by role

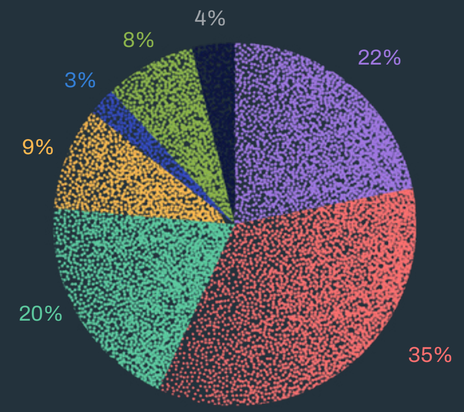
IT deciders



IT influencers



Top management



- In the coming 12 months our budget will increase by 1-5%
- In the coming 12 months our budget will increase by 6-10%
- In the coming 12 months our budget will increase by 11-15%
- In the coming 12 months our budget will increase by more than 15%
- In the coming 12 months our budget will decrease
- In the coming 12 months our budget will neither increase nor decrease
- I don’t know

Risk assessment is crucial

“*It is very hard to create a rule of thumb for determining security spend sufficiency. There are too many variables. As a proportion of IT budget there can be as much as a tenfold difference, depending on circumstances. Around five years ago, the percentage of security spending was about 10% of a company’s IT budget but that has risen since. Companies for whom security is critically important are spending about 12-15% of their IT budget on security,*” says Paul Brucciani, Head of Product Marketing at WithSecure™.

The first question you must ask is: what threatens you? So, if the worst-case scenario were to happen, what would the consequence be? You need to work out what an Annual Loss Expectancy (ALE) is and the probability of this happening.

This is where WithSecure™ comes in, as a company generally won’t be aware of what the answer is to the question. With significant experience in incident response, we are able to plot the ALE against the risk factors and work out what that company should be spending on security.

“*Once you've identified your risk, you then have to determine what to do with these risks and there are three options. First, you can transfer the risks, which would, for example, involve taking cyber insurance. Secondly, you can reduce the risk, using suitable security controls, technologies and services. Finally, you can just accept it, live with it and deal with things when they happen,*” Brucciani continues.

“*Essentially, you are looking at how much you can reduce the risk and therefore make a value judgement on how much of your budget you need to set aside for security. You need to decide how much risk you're willing to accept, your level of risk tolerance and whether your company has the ability to absorb,*” according to Brucciani.

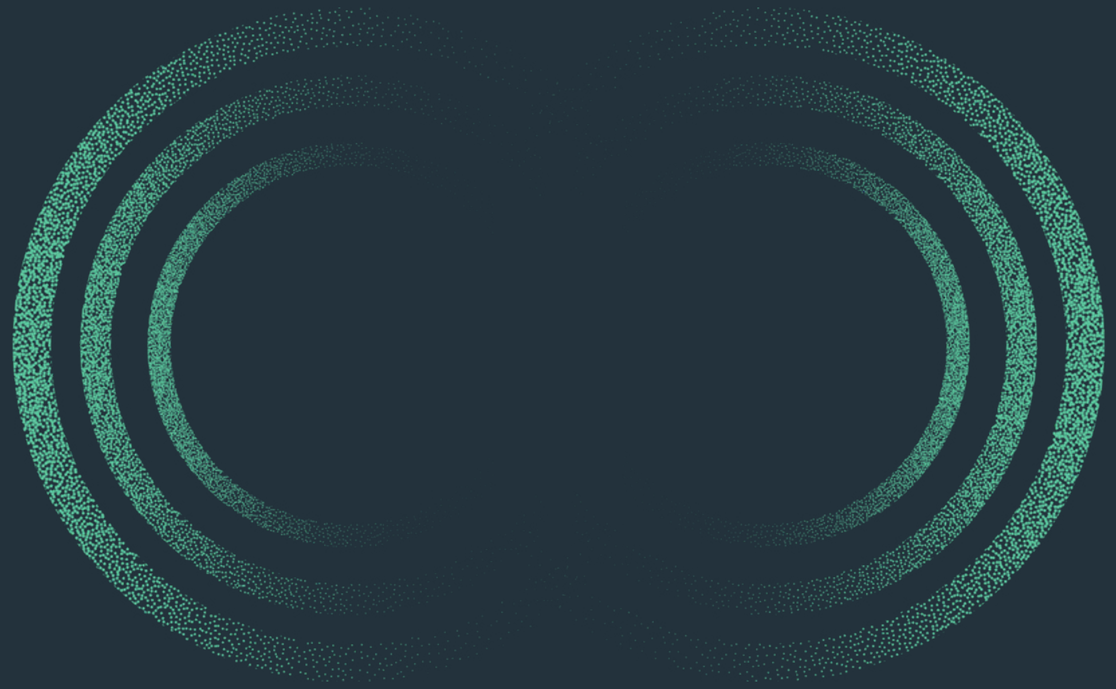
These are issues that the CFO must decide upon. Only then can you determine budgets, contingency amounts and how to deal with risks.

Not simply cost-related

It is important to point out that securing your company goes far beyond cost. There are numerous factors and WithSecure's research has proved exactly this point. Just 13.2% of respondents in WithSecure's survey said that the lowest price is the most critical aspect when selecting a vendor. In contrast, more than a fifth (21.8%) believe that 24/7 support is the most critical aspect, with a further 16.7% seeking trust in a vendor.

While there is no silver bullet when it comes to deciding how much you should be spending on security, WithSecure™ can provide a logical, defensible path you can take to ensure your company is as well protected as it can possibly be. Further, while price is and always will be, a major issue, security goes far beyond the bottom line.

WithSecure™ Elements can help you reduce risk, complexity, and inefficiency. It combines powerful predictive, preventive, and responsive security capabilities – all managed and monitored through a single security center.



3. Data residency

Do you know where your data is?

People really care about where their data is stored and processed.

The results from our 2023 Pulse survey highlight a keen interest in where data is stored and processed. Nearly 73% of respondents said that their data must be processed within the same country or region as its operations. Less than a fifth said this was of no importance.

How important is geographic location to data processing in your role?

- Data must be processed within the same country as our operations
- Data must be processed within the same region (e.g. EU, North America, APAC) as our operations
- It is of no importance where we process our end-customer data as long as all relevant legal and compliance requirements
- We do not process data for end-customers
- I don’t know

Where you keep the data

When these answers were broken down, a disconnect emerged. 42.8% of IT Deciders see regional processing as a requirement, compared to only 30.9% of IT influencers. This response suggests that the question of regional or national processing is not clear cut, or that different groups have different priorities.

Specific company sizes (500-999 and more than 5,000 employees) prefer regional processing, with more respondents agreeing that it's not important where customer data ends up.

This sentiment varies across company sizes: respondents from larger organizations were more likely to say they thought data must be processed in-region than that they thought it was of no importance.

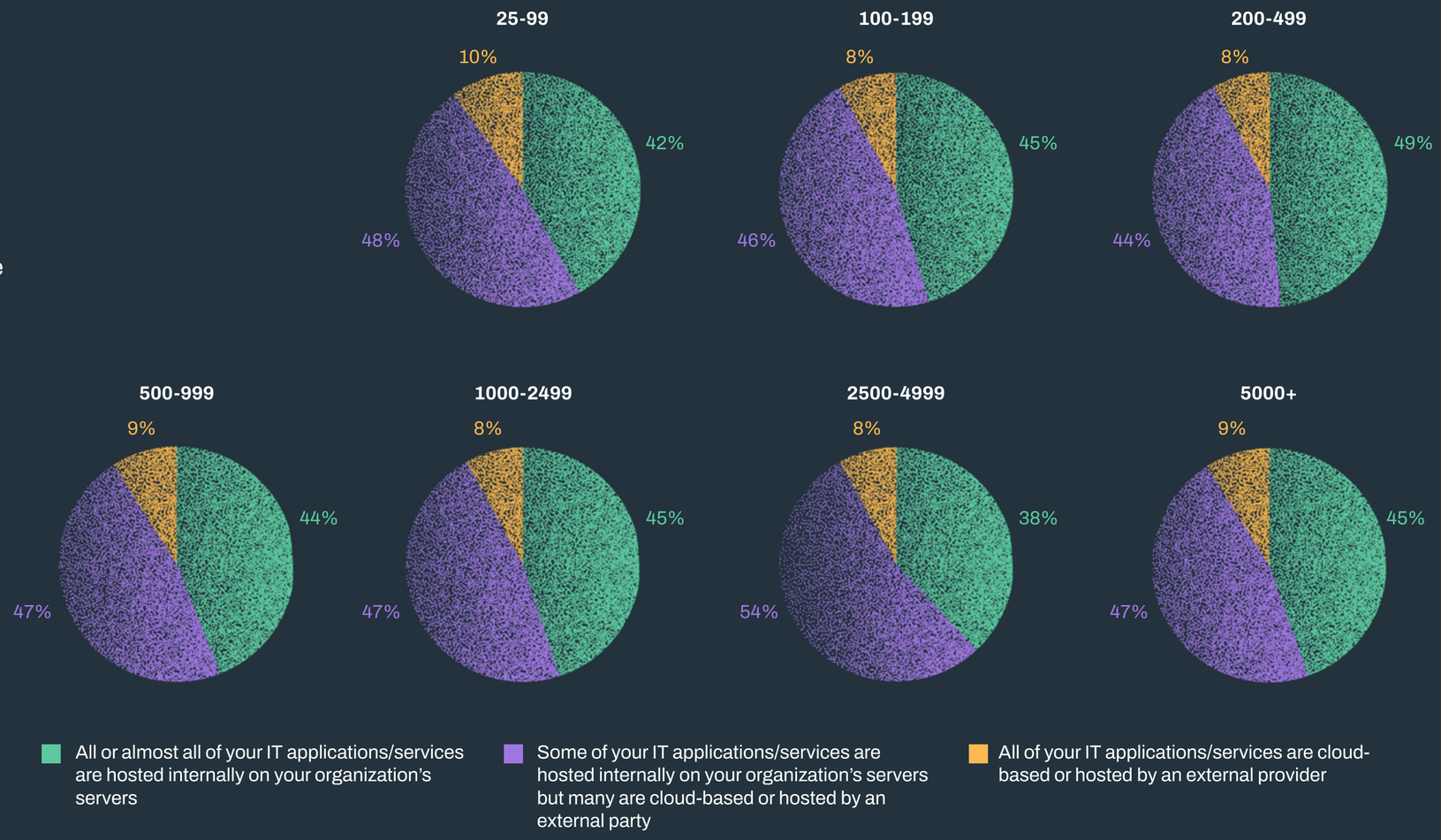
The preference for strong data residency may be the result of significant upheaval and change, both in terms of rules and in terms of physical events. Data sovereignty – the rules by which individual countries handle data within their borders – has been pulled between competing forces including globalization of computing and data processing, regional regulation, geopolitics, war and political upheaval and a consequent desire to reduce risk. All of this adds up to deep focus on where one's data sits and where it moves to or through.

Where you process the data

Here's where it gets a bit counterintuitive: we're constantly told how the Cloud Changes Everything™ – yet it doesn't seem to influence attitudes amongst our respondents.

Regardless of whether apps were more or less likely to be hosted internally or in the cloud at an organization, attitudes remained the same. Organizations of over 2,500 employees (and organizations in North America) were slightly more likely to host applications on site, while the Danes, Swedes, Germans and respondents from the UK were more likely to be more cloud than on-prem. Bubbling under at between 12.1% and 6.2% were those freaky forward-looking types doing everything in the cloud.

IT environment by company size

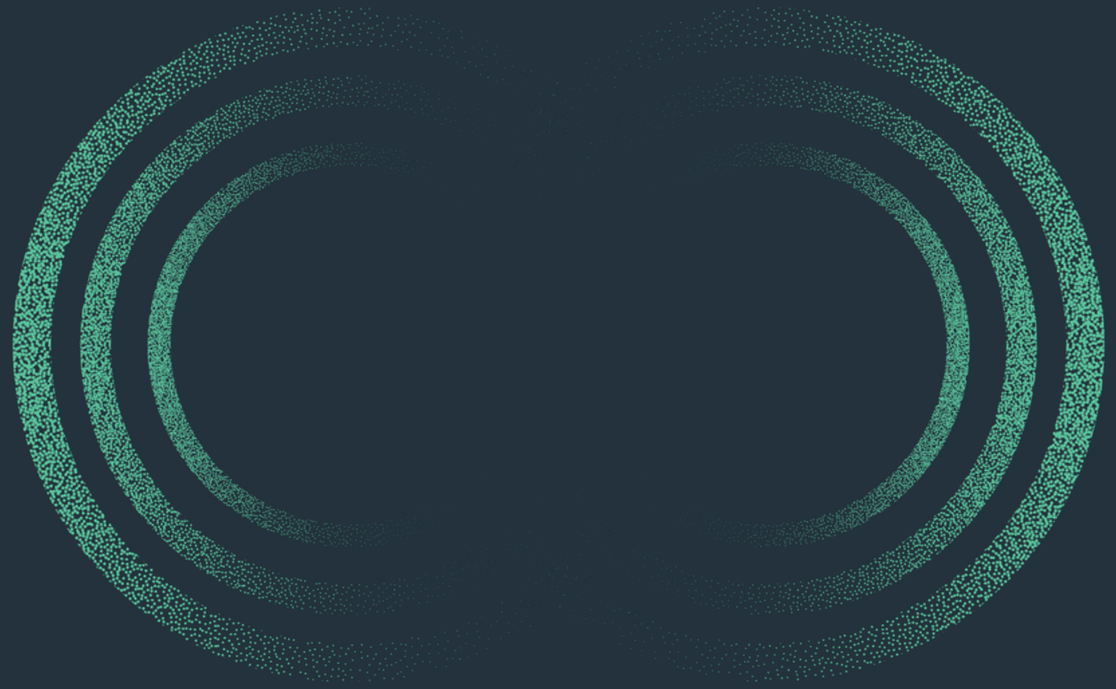


Conclusions and recommendations

Residency is important – something our Countercept MDR customers were so vocal about last year that we introduced a Europe-only version of Countercept to meet their requirements. The levers and drivers for this desire are complex – but it's interesting that there's a broad consensus across respondents of all stripes.

Ultimately, it's up to individual organizations to both meet regulatory requirements and ensure their customers are well-served. The practicalities of this can be complex, to say the least. Ditching cloud and switching to on-premises data storage and processing comes with its own compliance, security and technical overheads. Our consultants' advice is to follow national data protection regulatory requirements in the first instance, and then add in customer concerns and requirements on top.

The only area that may require significant action is internal communication: between the IT Decider types and the more strategic influencers and top management there is a bit of a disconnect around regional data processing. Understanding the differences between national and regional requirements – and why these differences of opinions seem to exist in organizations – should be an area of immediate investigation for readers.



4. Changing cyber security vendors

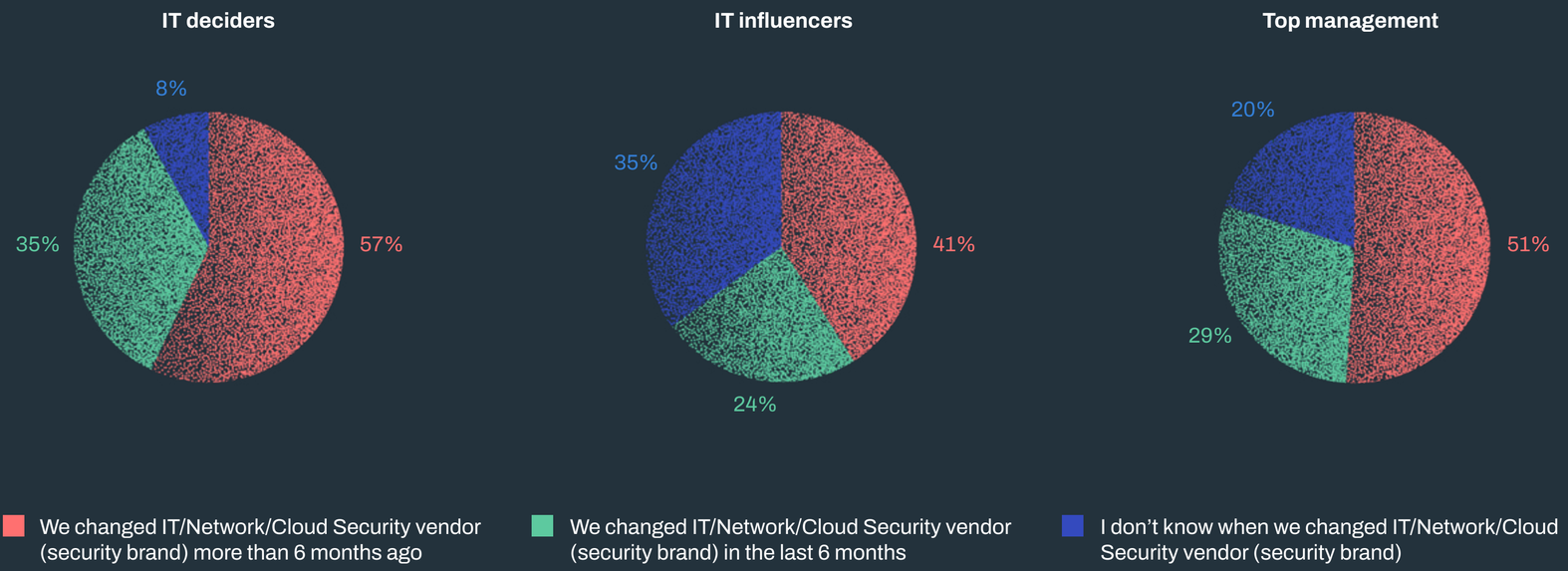
Vendor change is the constant

It's all change for security organizations – or rather, their suppliers.

Our survey shows that nearly a third (31.9%) had changed their security vendor in the past six months, while 32% expect to change IT security solution or vendor in the next six months.

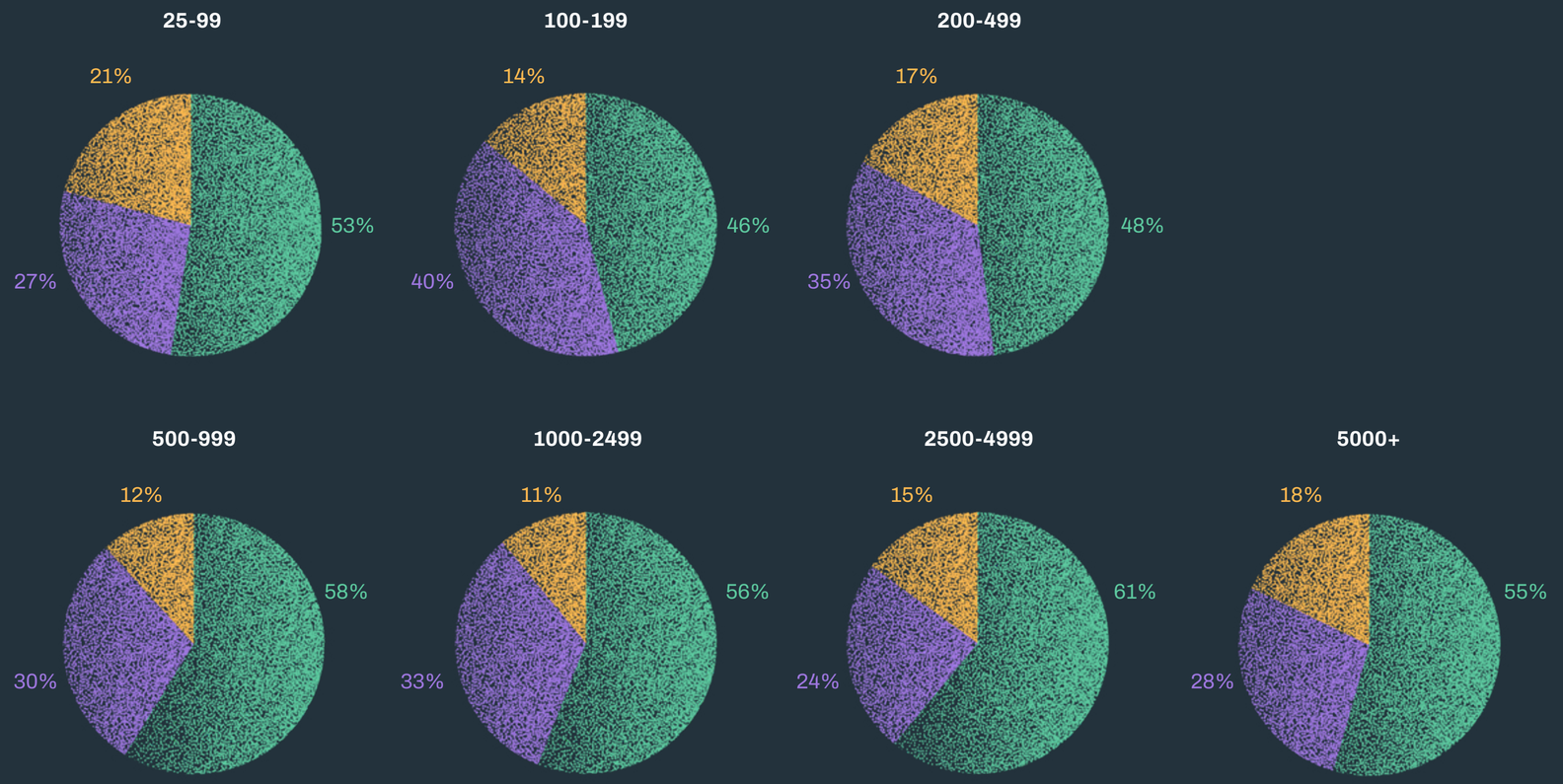
Respondents in the Finance and Insurance sectors and IT services and Technology vertical were both more likely to have changed vendors more than six months ago (59.4% and 58.4% respectively) and more likely to expect to change in the next six months – at a rate of 45% and 41.1% respectively.

Brand Vendor change intentions and criteria by role type



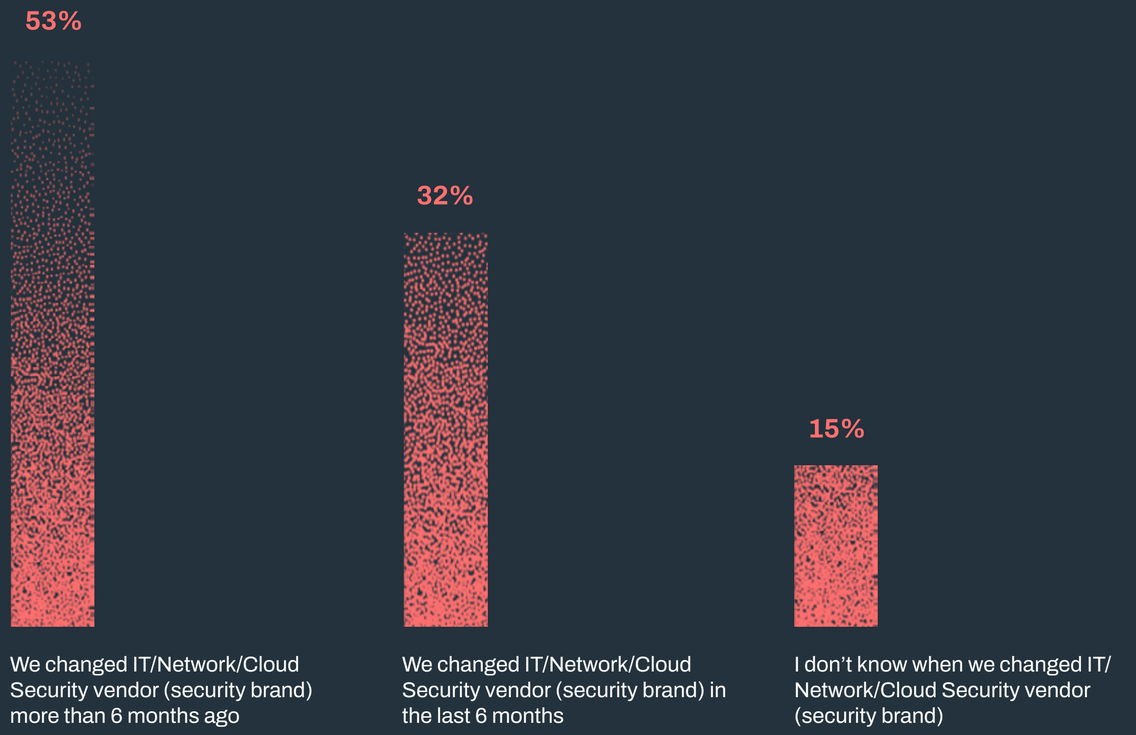
Looking at this from the perspective of company size (n=1,800) suggests a lot more movement in small-to midsize businesses than in larger organizations.

Brand Vendor change intentions and criteria by company size

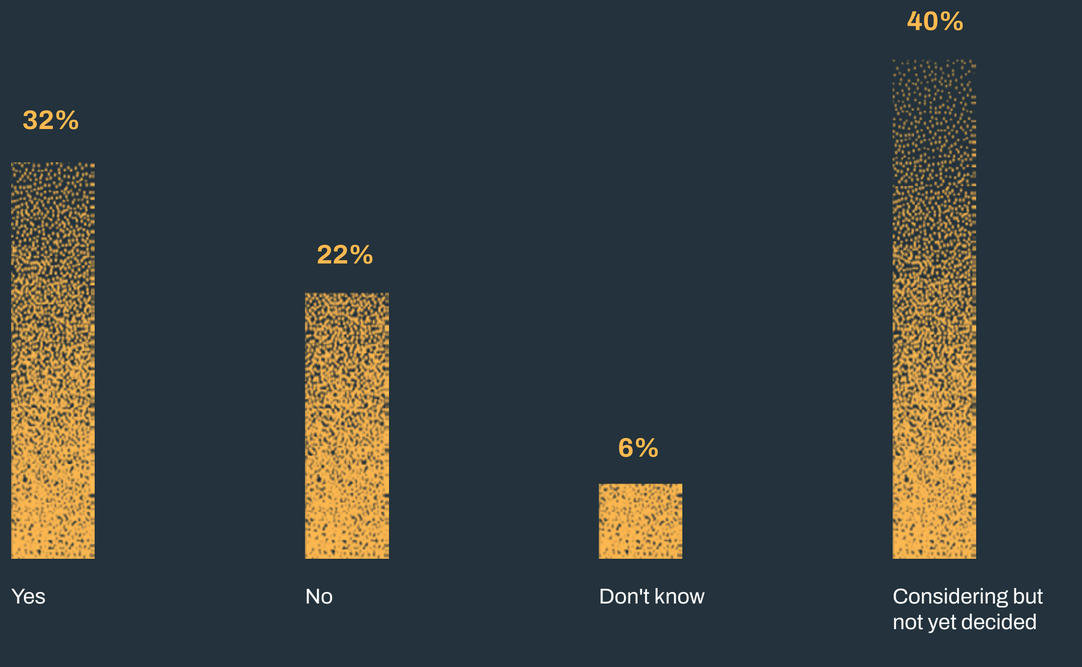


While ‘all change’ may be the norm for many organizations, hopping between different providers on a rolling basis, this process is complicated and time-consuming. We asked WithSecure’s Head of Solution Consulting, Peter Page, to give his thoughts on how companies tackle supplier change. We also explored the key to building and maintaining trust between vendors and their clients.

Regarding a change of IT/Network/Cloud Security vendor (security brand)



Does your company plan to change your business IT security vendor in the next 6 months?



What do clients fear most from transition projects?

Finite or constrained resources are familiar foes – and they make the effort needed to switch from one vendor to another an overwhelming effort for many organizations. Simply: sometimes it is too much effort to dump an underperforming supplier. This is no longer the case, judging by what our survey respondents told us.

"Security teams often aren't the people who implement new services", says Page. *"They must call upon project management (and) IT teams to roll out software, they have to rely on the networks team as the change they are making is affecting more parts of the business than they are responsible for, and they have to get that buy-in from all of the different stakeholders."*

Does the advent of cloud services make it easier to switch?

We've talked before about the Cloud changing security needs and challenges. Changing providers is becoming easier, but not because of the nature of the cloud: users are more comfortable with switching between Cloud services, much as they would between on-premises services.

For Page, it comes down to people: "*There's now a great talent pool who have skills in developing, implementing, and securing the cloud. Security providers need to have that capability as well. But as your perimeter changes, your security service changes, and it's helping customers to understand that risk and that is where things like Cloud Security Posture Management come in.*"

Why are contract durations getting shorter?

Shorter contracts are likely the result of two factors: the state of products and services in the cyber security market, and the trend towards shorter terms for Chief Information Security Officers (CISOs). These senior IT security managers typically spend under two years at an organization before moving on.

As new CISOs come and go, this can drive a pattern of ever-changing requirements and decisions and is likely to partly contribute to this instability in the market and the consequent regular change of vendors.

"*There is also a constant drive towards this 'new thing' or the next best thing, and that is the way the market is driving behaviors,*" says Page. "*Sometimes the resources put into buying the latest and greatest might be better spent on the basics – or tuning what you already have.*"

"*Because of the amount of noise in the market, it is hard to understand what the best approach is. A CISO committing to an expensive multi-year service has to be confident they'll get the outcomes they need – and the outcomes their board is looking for.*"

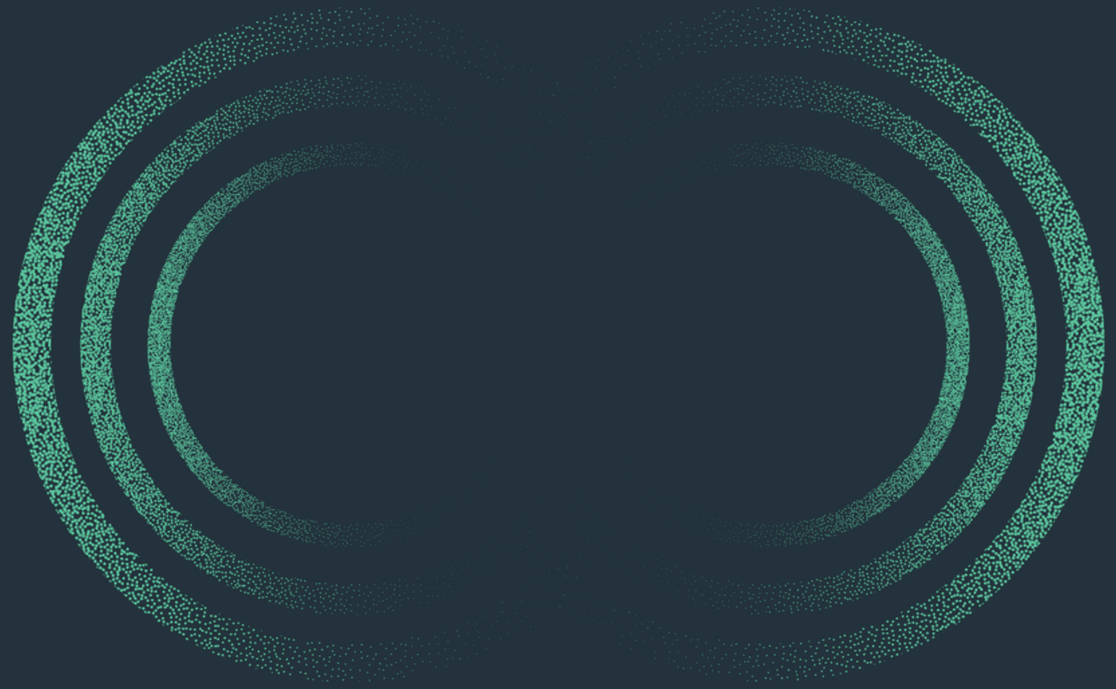
Is it becoming harder or easier for CISOs to make the decision to transition?

“It used to be hard for a CISO to get the buy-in of the board to spend big on cyber security. That’s now easier: the board, the CFO and the CEO are seeing breaches and ransomware infections at organizations and can appreciate the financial and outcome impact.

“But, because of the state of the market, there are so many different ways that CISOs can tackle the problem: Where do they spend their money? Do they insource or outsource? What about MDR versus EDR versus SIEM versus something else? So, it is almost like ‘analysis-paralysis’. There are too many options, and that means that they spend a lot of their time doing RFIs, speaking to vendors – it becomes a full-time job just to do that.”

Time is of the essence

Despite the noise in the current cyber security market, Page infers that for security’s sake, any decision is better than none: *“If you’re going from nothing to something, then making a decision is important because you haven’t got visibility or coverage of your estate. But in managed services, the end of contract is the deadline. The question becomes: how early do you start talking to alternative vendors? CISOs do well when they’re looking 12 months ahead of their contract end dates and starting to think about their options – and that’s where we see the best results.”*



5. Conclusion

This year's survey takes a fair bit of time to digest. It's clear that those who make the decisions about cyber security have diverse opinions and expectations. Sorting through the data to find what is actionable, rather than what is merely interesting, is tricky. That said, here are what we think are the insights that are most relevant. Some are, inevitably, already clear to clued-up readers, but they bear repeating, and our data supports these inferences, too.

1) Perceived priorities may not be the ones that make the most difference to security posture. Check which practices and competencies your organization is missing and compare them to perceived priorities. Look for mismatches.

2) Security spend is a matter of opinion. Our survey showed a big difference in perceptions of security budgets for the coming year, and misaligned expectations are a recipe for confusion, conflict and hasty decision making. Ensuring there is clarity – and that, if budget is not yet confirmed or indicated, every stakeholder knows what a level of budget will allow them to change, buy or achieve – is a recipe for calm and collected decision making.

3) Data residency is a hot issue, and it's absolutely imperative for more than 70% of our respondents. But it's equally important to consider the implications of ditching a cloud-based app that can't guarantee residency for an alternative; is a local or in-house solution going to be as secure, or offer the capability you need?

4) When you come to change vendors – decide early. It's notable that successful transitions seem to kick off at least 12 months before the contract expiry or renewal, and deciding to decide is, well, probably the best decision to make first. Don't get caught out by analysis paralysis.

Finally: our data showed significant agreement and consensus amongst the groups surveyed – something that points to good organizational harmony. Yet there are also points in the data where opinions of deciders, influencers and management diverged significantly. It is these areas that should concern us all, and where clear and open communication will be the most effective tool for the year ahead.

Methodology

WithSecure's 2022 B2B Market Research study reached 3,072 respondents (2,098 from Europe) through an online survey during May 2022 across 12 countries, including nine European countries: the UK, France, Germany, Belgium, Netherlands, Denmark, Finland, Norway, Sweden, as well as the US, Canada and Japan. All respondents are IT/Network/Cloud Security decision makers and influencers for the purchase of IT/Network/Cloud Security Products and Services in their organizations.

Who We Are

WithSecure™, formerly F-Secure Business, is cyber security's reliable partner. IT service providers, MSSPs and businesses – along with the largest financial institutions, manufacturers, and thousands of the world's most advanced communications and technology providers – trust us for outcome-based cyber security that protects and enables their operations. Our AI-driven protection secures endpoints and cloud collaboration, and our intelligent detection and response are powered by experts who identify business risks by proactively hunting for threats and confronting live attacks. Our consultants partner with enterprises and tech challengers to build resilience through evidence-based security advice. With more than 30 years of experience in building technology that meets business objectives, we've built our portfolio to grow with our partners through flexible commercial models.

WithSecure™ Corporation was founded in 1988, and is listed on NASDAQ OMX Helsinki Ltd.

WITH secure™