Bitdefender DSM GROUP

Cloud and Cybersecurity Insights: Trends & Best Practices

Introduction

Building a cybersecurity strategy has never been more challenging – the rapidly evolving threat landscape, combined with the acceleration of digital transformation and a workforce distributed beyond traditional office networks to the home have radically altered how IT teams defend their network, data, users and applications.

The astonishing value of the cybercrime industry and move towards cybercrime as-a-service via online dark web marketplaces and commoditisation of malware has not just seen more advanced and complex threats, but an increasingly lower barrier for entry. Anyone can now gain access to the tools needed to deliver ransomware and take payments via anonymous cryptocurrency, while tactics have evolved to include PR and extortion threats that have further muddied the waters of how organisations can respond – further ramping up the potential financial returns.

The last two years have seen the added complexity of an accelerated shift in the infrastructure and strategy of many organisations, as distributed workforces and working from home became the default. This necessitated migration to the cloud at unprecedented speed and digital transformation that helped keep businesses going, but created new risks and opportunities for threats to exploit.

As we move into 2022, we’ve commissioned a survey across hundreds of CTO, CIOs, CISOs and industry leaders to get their perspective of this changing threat landscape, how much cloud has become the core of today’s network, and the priorities from the boardroom to the SOC in defending against the next threat.

About the survey

Working with our partners at Bitdefender, and Bitdefender Labs and Managed Detection and Response teams, we've pulled together key trends to provide insights that can help keep your networks, data and users secure. However, it's also essential for the community to work together, combining our experience and knowledge to help defend us all against bad actors and next generation threats.

This report is result of reaching out to over 200 senior IT decision makers and executives, from organisations across SMB, mid-market and enterprise sectors, as well as both public, private and third sectors. Respondents all had responsibility for IT and cybersecurity within their organisation, but varied from senior management like CIO and CTOs to those on the frontline, including network engineers, System Administrators and analysts.

Respondents could provide share their expertise and experience anonymously, helping give greater depth to the responses and provide unique insights into the key trends in cybersecurity, and in particular how to ensure the rapid shift to cloud computing remains secure for users and organisations alike.

93% of ransomware attacks are motivated by money, rather than espionage or fun

54% start with spam or phishing

50% of SMBs go out of business within 6 months after a ransomware attack

Key industry trends you need to know 1/2

Alongside the survey data, we've also spoken to the analysts at Bitdefender for their perspective on what they see are the growing trends.

You're not the target – but you're in the way

Supply chain attacks have long been a tactic, whether it was deliberate (the RSA breach) or accidental (such as Target), but increasingly it's now a popular method of going after high profile organisations through their weakest link. This will especially apply for major infrastructure or government bodies, and exploiting their service providers or suppliers where they use common or linked systems (such as the growing focus on API security), especially public cloud environments. This particularly includes workload and tool development in the cloud, such as around the ubiquitous Azure and Microsoft 365 services.

You can't defend what you don't know

Zero Day exploits have become a lucrative market in their own right, for both legitimate security teams and criminal actors who can sell them in underground marketplaces. The increased diversity of internet-enabled devices through IoT and smart systems has significantly broadened the potential exposure risk, making it challenging for IT teams to patch and protect those systems. When a zero day exploit breaks, the speed of response is key, and without vendor patches available for more complex, obscure or bespoke systems, those apps or devices will be left unprotected. This principle of defending what you don't know extends even to "trusted" technology on private and public networks – from blockchain technologies to web3, the rapid pace of change and lack of established cybersecurity principles could present significant challenges.

Key industry trends you need to know 2/2

The continuing threat of ransomware

From the Colonial Pipeline to Kaseya, ransomware continued to wreak havoc across 2021 and that shows no sign of changing with the US Treasury linking over $5 billion in payments to criminal ransomware. The increasing sophistication of criminal offerings will also see an increase in "as a service" offerings, enabling distribution on an unprecedented scale through smaller players, ad-hoc attacks and emerging bad actors looking to move into cybercrime.

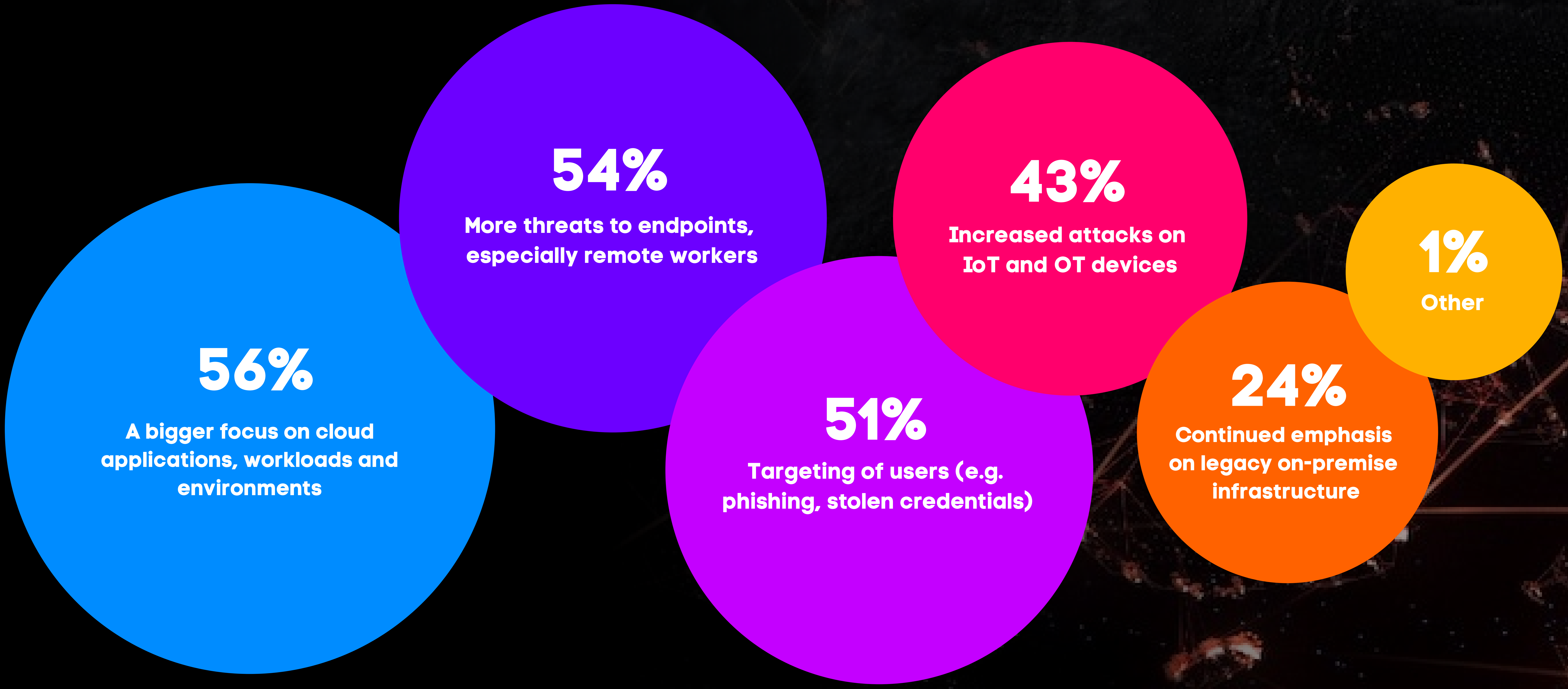
> **"Ransomware will continue to be the most lucrative type of cyber-crime in 2022. We expect to see an increase in Ransomware-as-a-Service (RaaS) attacks that will focus on data exfiltration for blackmailing purposes," said Dragos Gavrilut, director of the Cyber Threat Intelligence Lab at Bitdefender. "Just like any mature business, ransomware will have to constantly keep up with both competition and cyber-security vendors alike."**

Q1: How have you seen cyber-attacks evolve this year?

The biggest challenge for cybersecurity and IT teams are the evolving threats, with bad actors and criminals always looking to stay one step ahead of defences. The huge shifts in the technology landscape have provided increased opportunities for threats, and the feedback highlights that they have come from many different areas.

The most popular choice, of cloud applications and environments, highlights that move of so much data, infrastructure and investment to the cloud. It's closely followed by endpoints, which likewise has seen a huge shift, most significantly out of the more controlled, protective corporate network to the home, and often BYOD. With that comes a focus on users, increasingly isolated and with new applications to deal with, and the rapid growth of IoT within the corporate network (from smart warehouses to intelligent office buildings) sees it emerge as an evolving threat far beyond traditional networks.

Q1: How have you seen cyber-attacks evolve this year?



56% A bigger focus on cloud applications, workloads and environments

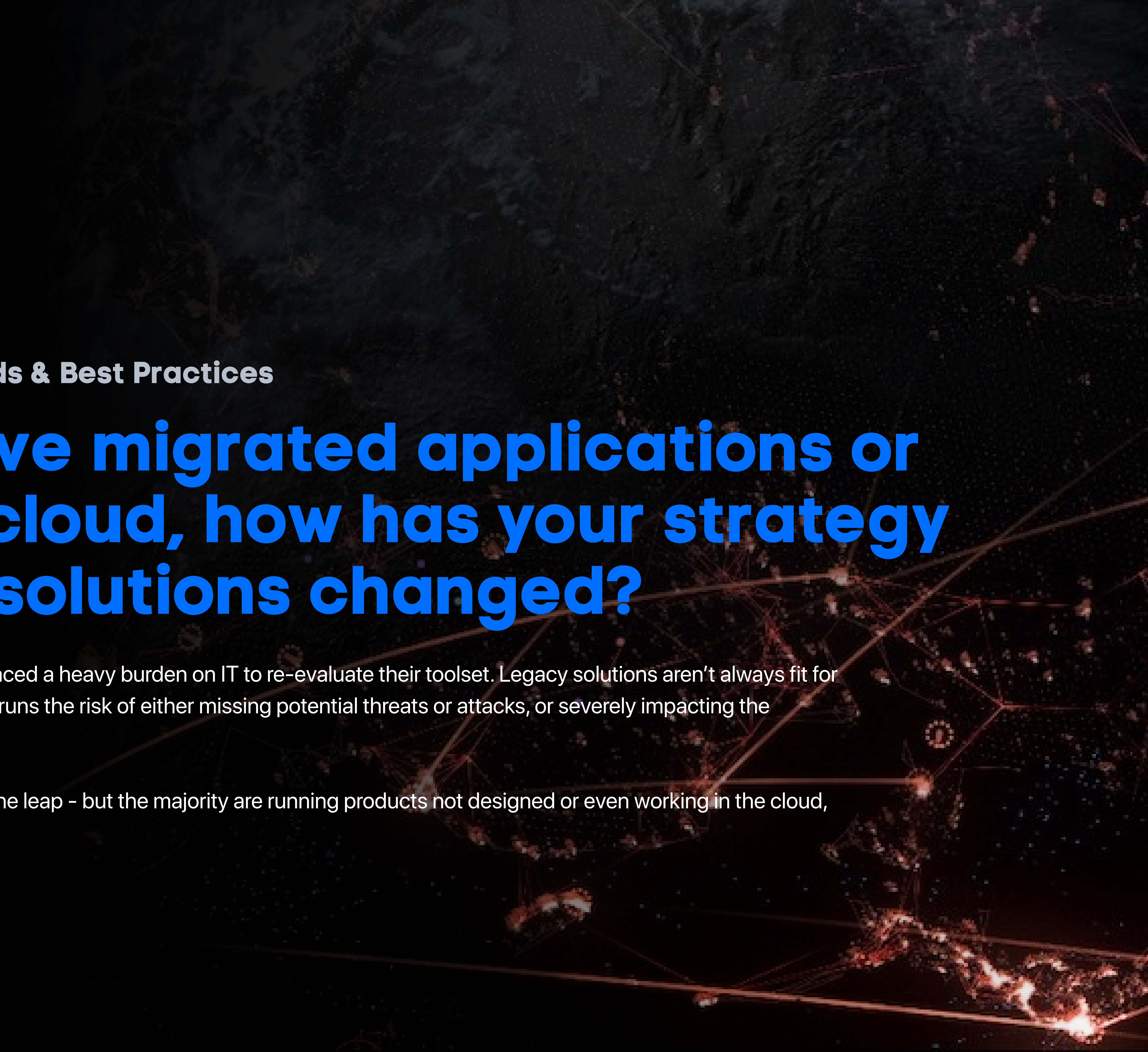
54% More threats to endpoints, especially remote workers

51% Targeting of users (e.g. phishing, stolen credentials)

43% Increased attacks on IoT and OT devices

24% Continued emphasis on legacy on-premise infrastructure

1% Other

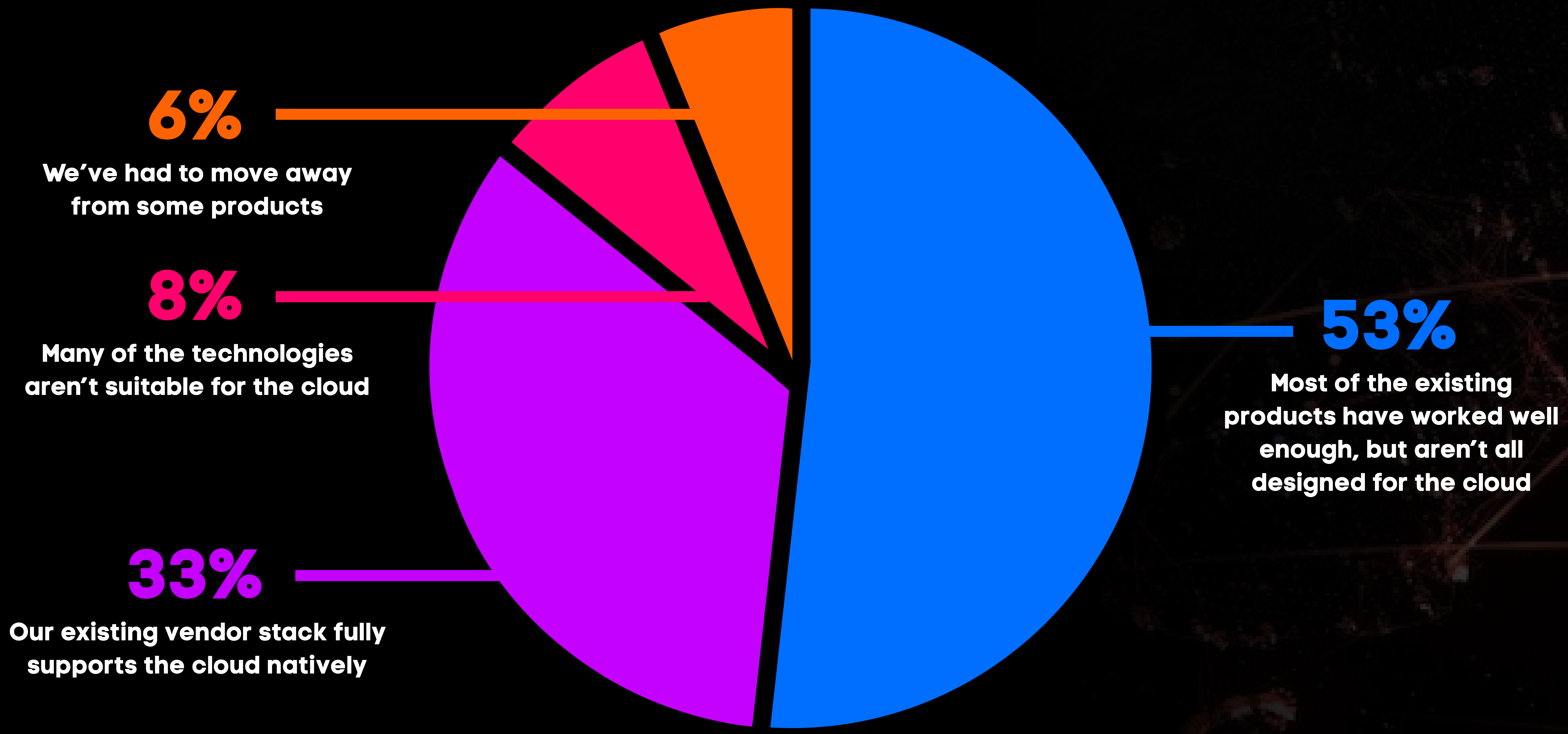


Q2: Where you have migrated applications or workloads to the cloud, how has your strategy on cybersecurity solutions changed?

With the rapid move to hosting infrastructure in the cloud, it’s placed a heavy burden on IT to re-evaluate their toolset. Legacy solutions aren’t always fit for purpose when deployed in the cloud, and for cybersecurity that runs the risk of either missing potential threats or attacks, or severely impacting the productivity or efficiency that the cloud can bring.

Fortunately, many respondents have solutions that have made the leap - but the majority are running products not designed or even working in the cloud, which can cause a significant impact on the business.

Q2: Where you have migrated applications or workloads to the cloud, how has your strategy on cybersecurity solutions changed?



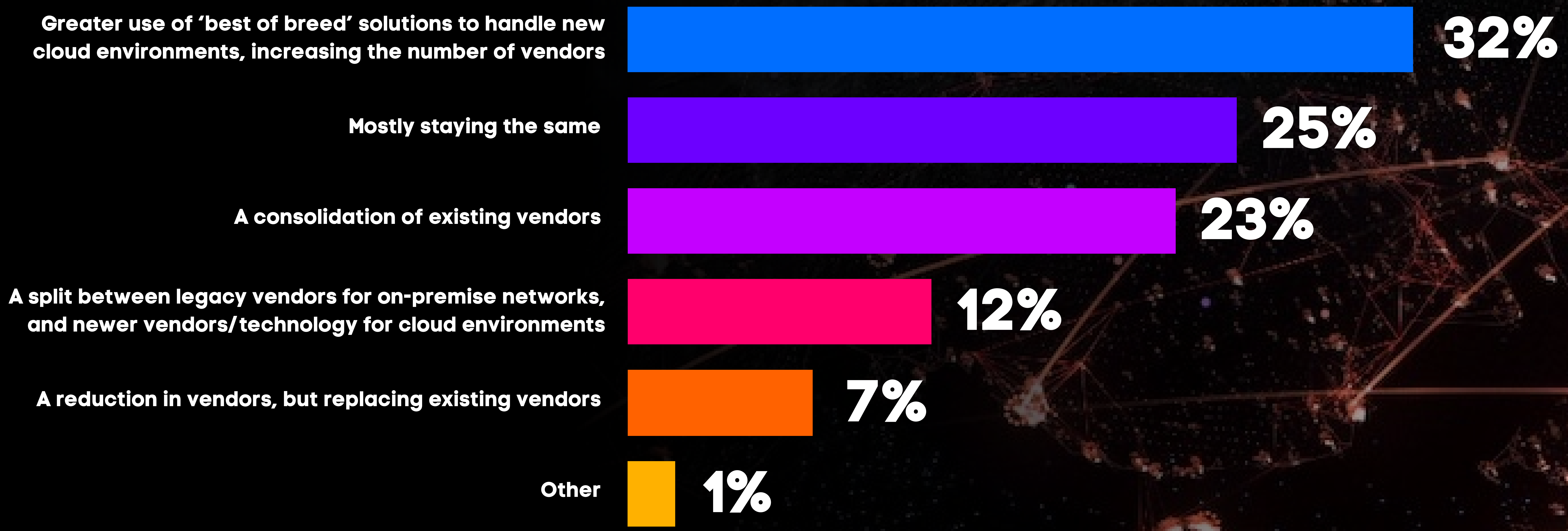
Cloud and Cybersecurity Insights: Trends & Best Practices

Q3: How do you expect your cybersecurity technology to evolve over the next 12 months?

When it comes to reviewing cybersecurity strategy, many organisations will look to consolidate their vendor portfolio due to the opportunities for rationalised purchasing and more streamlined operations with fewer management consoles and reporting systems to deal with.

However, the landscape is clearly mixed - so while just over 20% are expecting to consolidate, 25% expect it to stay the same while the majority see a likelihood for more vendors as the importance of cloud-native, best of breed technology becomes a more important factor. This highlights how many technologies have struggled to make the leap to the cloud, and so limiting the potential for their customers to truly deliver on the opportunities that digital transformation offers.

Q3: How do you expect your cybersecurity technology to evolve over the next 12 months?

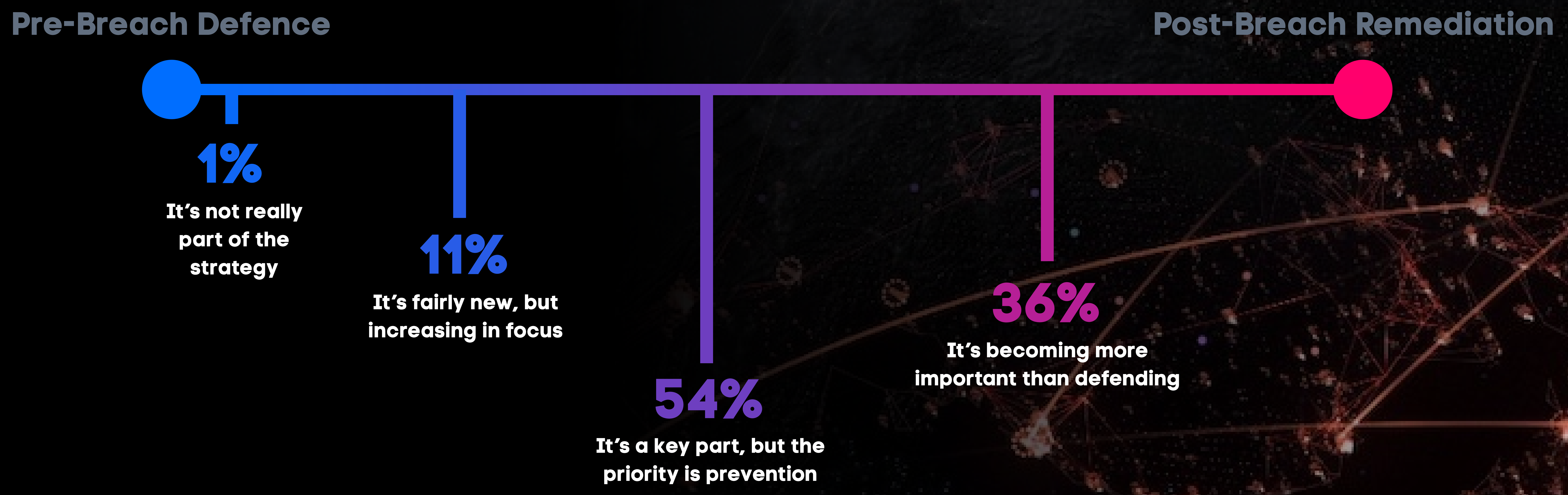


Q4: What's the importance of post-breach detection and remediation in your cybersecurity strategy?

When rather than if - it's a question about the potential for a successful attack or data breach that many CISO and CIOs have had to face when building their cybersecurity strategy, and defining their priorities. The responses were clear that it's a delicate balance with both being important, but while the majority still favour prevention, and third of organisations say they are now focusing more on post-breach detection and remediation rather than initial defence.

The consequences are significant, with IT teams requiring more advanced solutions with greater visibility and insight across a network, more integration with third party solutions to build up insights into attacks and the ability to proactively hunt malware or bad actors on a network before damage is caused, rather than stopping them in the first place.

Q4: What's the importance of post-breach detection and remediation in your cybersecurity strategy?



Pre-Breach Defence

Post-Breach Remediation

1%
It's not really part of the strategy

11%
It's fairly new, but increasing in focus

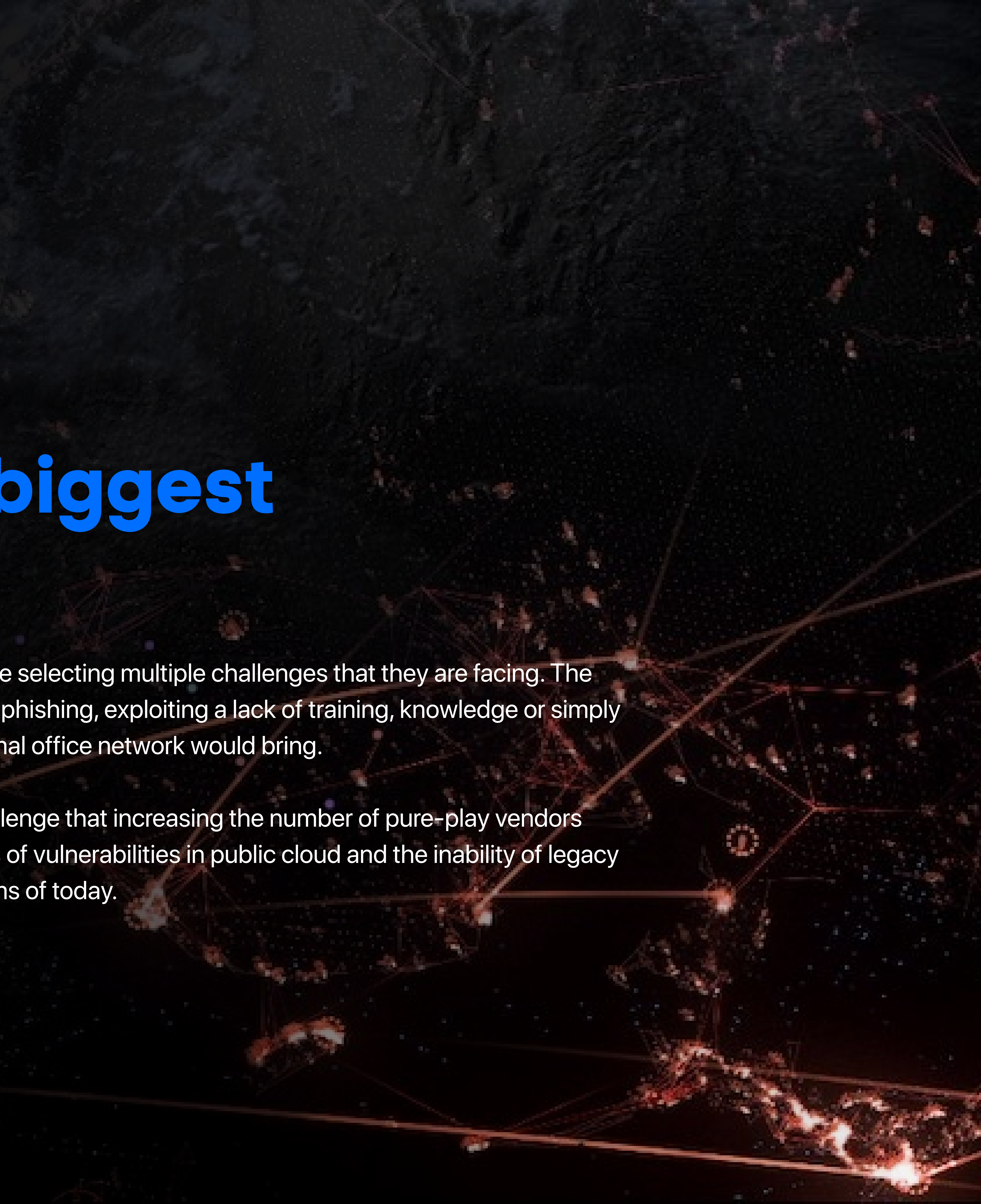
54%
It's a key part, but the priority is prevention

36%
It's becoming more important than defending

Q5: Where do you see the biggest risks to your organisation?

The huge variety of risks was highlighted by the spread of responses, with the majority of people selecting multiple challenges that they are facing. The most damaging risks both focused on employees - direct attacks through social engineering or phishing, exploiting a lack of training, knowledge or simply human error - and that so many people working from home lack the right protection than a normal office network would bring.

The third most popular choice, or gaps between cybersecurity technologies, highlights the challenge that increasing the number of pure-play vendors brings. Along with the difficulty of enforcing a uniform security policies, and the connected risks of vulnerabilities in public cloud and the inability of legacy solutions to migrate, demonstrates the need for solutions that are designed to solve the problems of today.



Q5: Where do you see the biggest risks to your organisation?

65%
35%
27%
27%
25%
19%
4%

65% Attacks on the user, such as phishing or social engineering

35% Gaps between different cybersecurity technologies, leaving exploits uncovered

27% Leveraging vulnerabilities in public cloud environments

27% Unpatched software or Zero Day attacks

25% The rapid migration to the cloud, and existing cybersecurity defences not being designed to scale or migrate

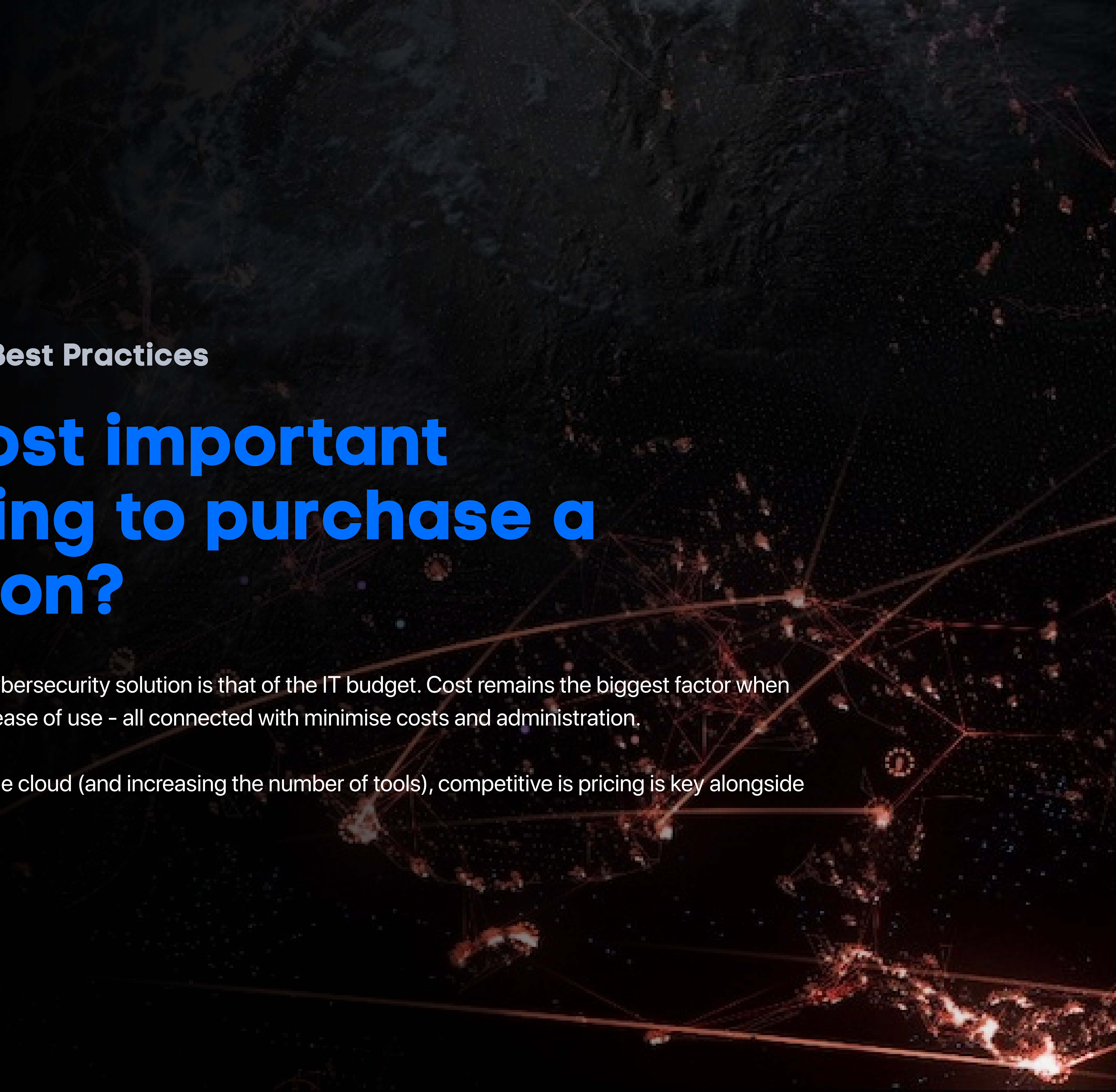
19% Insufficient in-house resource or expertise to deal with the volume of alerts/attacks

4% Exploiting insecure network connections, from home user routers to IoT

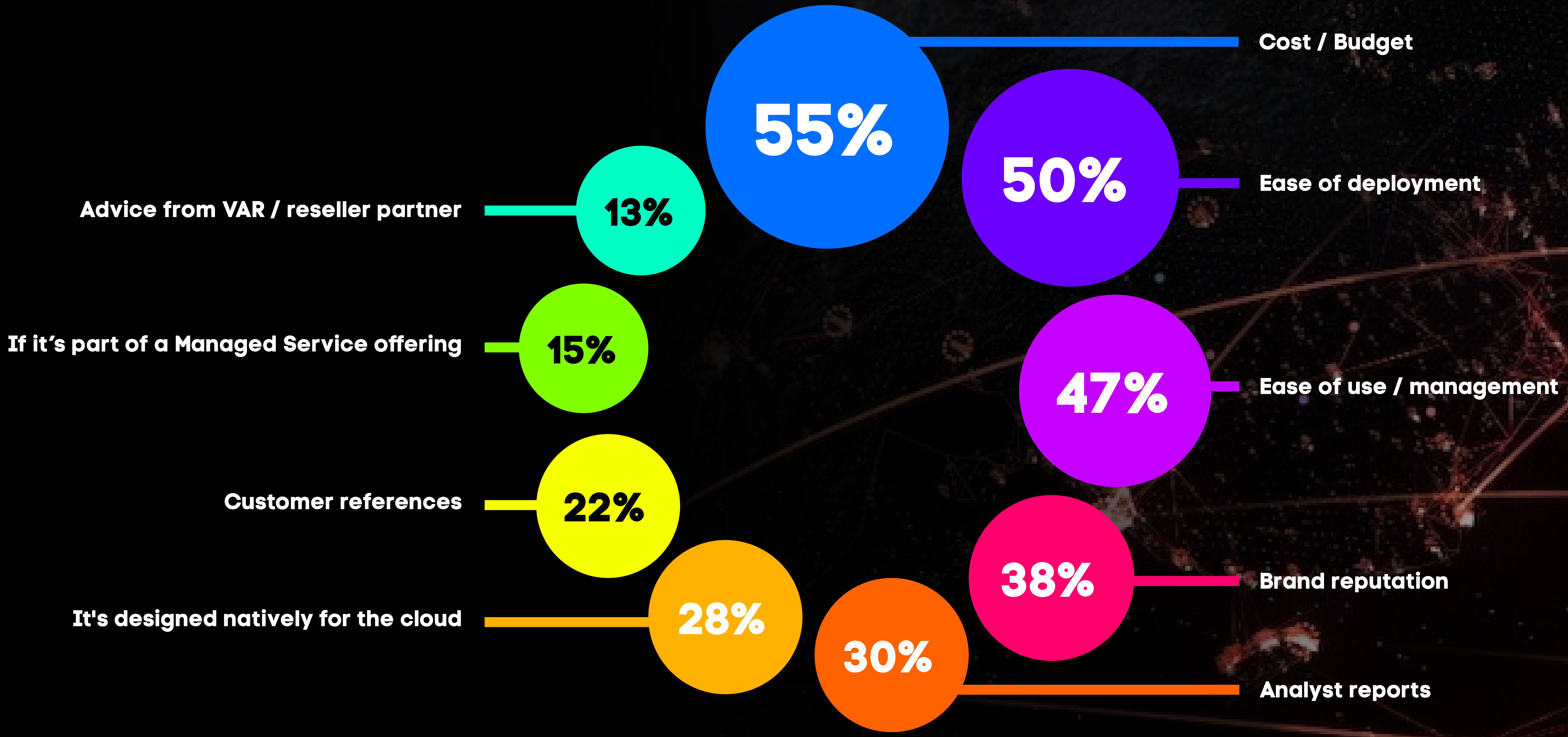
Q6: What are the most important factors when choosing to purchase a cybersecurity solution?

One thing that has not fundamentally changed when selecting a new cybersecurity solution is that of the IT budget. Cost remains the biggest factor when purchasing new products, closely followed by ease of deployment and ease of use - all connected with minimise costs and administration.

When connecting back to the need for solutions that are designed for the cloud (and increasing the number of tools), competitive is pricing is key alongside the ability to roll out these solutions quickly and simple.



Q6: What are the most important factors when choosing to purchase a cybersecurity solution?



What are the top cloud security threats?

Alongside the research with leading IT and infosecurity professionals, we also spoke to the teams at Bitdefender Labs about what they see as the major cloud security threats expected to grow in significance in 2022.

1

Data Breaches: with data being created on an incredible scale, the risk of data breach potentially exposes organisations more than ever as it's distributed across workloads, networks and applications. Breaches can come from direct attacks, but just as easily from mis-configurations or inconsistent policies.

2

DDoS: the reliance on cloud services to run critical, customer-facing or operational technologies represents a major risk to organisation. Heavy traffic might drive applications offline, cause poor performance or even act as a distraction to an attack running elsewhere. Having non-cloud defences can significantly response times, when organisations are in the midst of an attack.

3

Insecure APIs: while offering significant potential to automate business processes and reduce manual tasks, they do represent potential security risks, and research firm Gartner has predicted that by 2022 API attacks will become the most-frequent attack vector, causing the potential for data breaches from enterprise web applications.

In conclusion 1/2

In many ways, the fundamental challenges of cybersecurity remain the same – keeping defences ahead of emerging threats, evolving the strategy to support new technologies and ensuring a clear plan is in place for remediation and analysis to help feed into the plan.

However, the accelerated pace of change in cloud computing in the past few years has meant that reviews of cybersecurity strategy at any level, from boardroom meetings to hastily convened meetings by the server rack to discuss the latest zero day, are continual. The feedback to this survey highlights the diverse set of challenges that IT teams face, with cloud now the biggest focus but the importance of the new network edge – IoT, BYOD and users – now defining the first line of attack and defence.

The majority of the existing solutions deployed weren't built for the cloud, and that presents challenges – with budgets tightened and the skills shortage reducing the ability of many organisations to easily adapt, it's near impossible to seamlessly support the cloud migration projects that many have embarked on to cater for the shift to distributed workforces. Most respondents expect to see an increase in the number of cybersecurity tools deployed, putting a strain on budgets and resources, and that reflects the increasing number of potential vectors for attack as well as the view that cost remains the biggest factor in product selection. The presence of ease of use and deployment in the top 3 requirements for vendor selection confirms that too, as IT teams struggle to effectively ensure solutions are in place if they are too complex.

The biggest move in sentiment over previous research, though, was that over a third of respondents rated remediation as a greater priority than prevention. This sits alongside the biggest being viewed as being the user (and secondly insecure endpoints, which nowadays includes home networks) and highlights how the new perimeter edge is no longer just not on-premise, but often not within the control of IT. Third party cloud applications, IoT and shadow IT all contribute to the maelstrom of unmanaged activity to control and manage, with the cloud accelerated that change. Digital transformation has transformed how technology is viewed by organisations, with line of business now driving IT as an enabler for growth and productivity. The consequences for infosec professionals is a more diverse, complex and fluid environment to manage, one centred on the user more than ever (both internal, plus external users such as customers or suppliers using cloud applications), and a threat landscape that can operate at both greater scale and precision than ever before.

Cloud and Cybersecurity Insights: Trends & Best Practices

In conclusion 2/2

What are the key takeaways to consider?

1 The accelerated adoption of the cloud by organisations has been replicated by the rise in cloud-focused threats, increasing the scale of assets that IT need to defend.

2 The distributed remote workforce and confidence in using IoT in business environments has further broadened the number of potential exposure points.

3 Many solutions work in the cloud - but fail to support it natively, leaving gaps in both security and efficiency.

4 The acceptance of working in a post-breach world has become standard, and having a strong strategy to target threats already on the network and then remediate is essential.

5 Organisations can see significant opportunities in increasing the number of specialist, cloud-native vendors - but cost and ROI continue to define the selection process.

In return, the cybersecurity market is equally advanced at great pace – and cloud native technologies are empowering IT teams to deliver and secure the potential of the cloud.

This report was produced in association with Bitdefender, the home of award-winning Threat Prevention, Detection & Response Platform and Managed Security Services. We surveyed over 1,000 senior IT executives and decision makers in organisations across the UK, ranging in size from 50 users to over 5,000.

For more information on Bitdefender's solutions, visit www.dsm-gb.co.uk or contact us today on +44 3333 22 11 00

Bitdefender

DSM GROUP