92plus

Survey report

From budget battles to ***strategic wins***

Partner insights on selling cybersecurity in 2025

The cybersecurity market is on an unprecedented growth trajectory, with ***global spending projected to surpass $250 billion by 2026***. However, for resellers and MSPs, capitalising on this growth requires more than just selling solutions. It demands a strategic approach that addresses customers' evolving needs, budget constraints, and the increasing complexity of the threat landscape.

This whitepaper explores the findings of a recent survey conducted among cybersecurity VARs and MSPs by e92plus. It highlights ***key opportunities and challenges, providing actionable insights to help partners refine their strategies and achieve sustainable growth***.

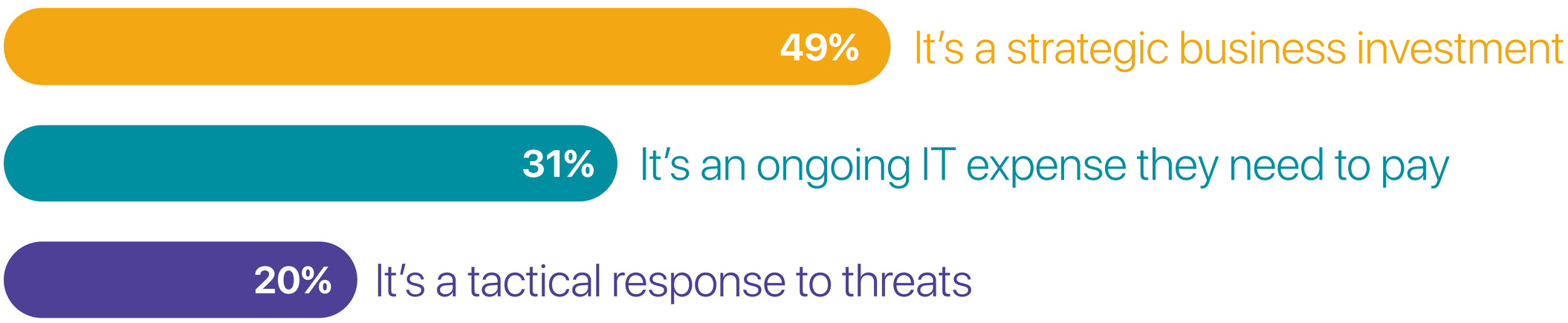
The growing ***cybersecurity market***

Cyber threats are becoming more sophisticated, but it's a complex and dynamic market which can present significant for challenges for partners looking to grow their cybersecurity business (especially where they don't have an established practice currently). ***The survey indicates that 46% of customers see cybersecurity as a strategic business investment, while 31% consider it an ongoing IT expense, and 23% view it as a tactical response to threats.*** This demonstrates a shift in perception, with a growing number of businesses understanding the value of cybersecurity beyond mere compliance.

Despite this growing awareness, budget constraints remain a significant barrier. ***Nearly 23% of survey respondents noted that annual predefined budgets limit flexibility, and 23% are influenced by broader economic factors.*** These challenges highlight the need for resellers to effectively communicate ROI and align solutions with business priorities.

The results
and the opportunity for partners 1 of 3

Question 1: How do your customers most typically see cybersecurity in terms of their business proprieties?



Key lesson: Specialisation in high-growth verticals

The importance of compliance requirements in 2025, as NIS2 and DORA are established and the new UK Cyber Security and Resilience Bill is introduced, mean that partners will also need to identify those solutions that are strategically important to different verticals.

Industries such as healthcare, finance, and manufacturing are among the top adopters of cybersecurity solutions. Resellers who specialise in these areas report higher win rates, as clients value their deep understanding of industry-specific challenges. ***Moreover, with IT teams (76%) primarily driving decisions, having tailored, easy-to-implement solutions for these verticals can streamline adoption.*** Cybersecurity requirements are also clearly expanding into areas that require more support and guidance from trusted partners in those sectors – such as the growth of IoT/OT and the frequent lack of ownership from IT, cybersecurity or operations teams – so there are strong opportunities.

Strategic implication: Resellers should invest in certifications, partnerships, and tailored marketing campaigns to establish themselves as experts

The results
and the opportunity for partners 2 of 3

Question 2: Who most often drives decisions on which cybersecurity solutions they invest in?

Key lesson: Offering cybersecurity services to bridge the gap

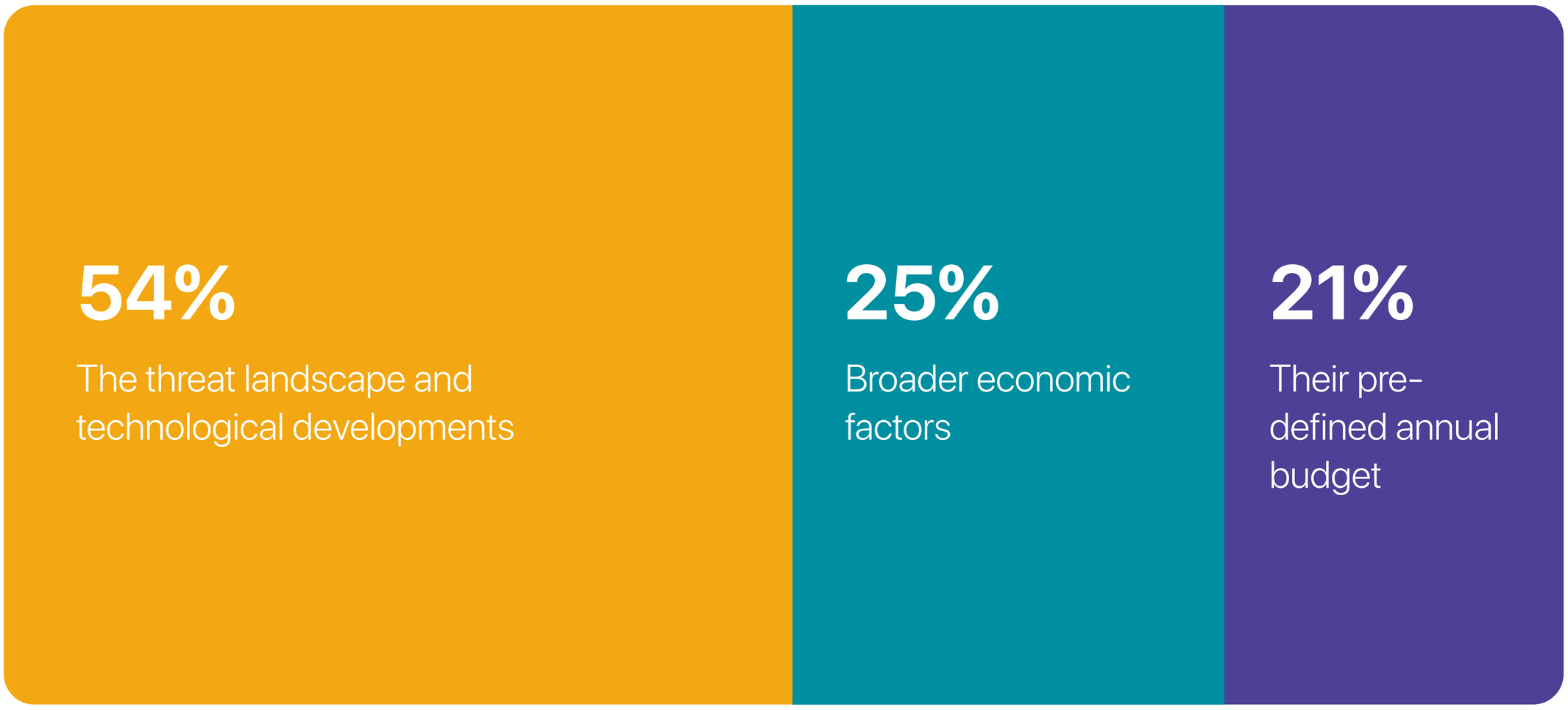
Cybersecurity may be important but budget constraints show that often it's still the IT team that is responsible. This highlights the essential role that partners can play in providing the guidance needed beyond just procurement – to how it secures and supports their overall technology stack, and integrates with their business so it's not simple an overlay or business prohibitor that slows efficiency.

The opportunity is around Managed Detection and Response (MDR) - emerging as a game-changer in the cybersecurity market. With the IT team being the driver, meaning in SMBs in particular there is often no dedicated cybersecurity team, or a lack of broader expertise and resources, MDR services can address these concerns. The report does show that procurement rarely sits outside the IT team, however, which gives confidence that purchasing isn't going to be driven down purely on price, and that value can play a strong role.

Strategic implication: Building or partnering to provide MDR services allows resellers to deliver proactive, value-added solutions that address customers' most pressing security concerns.

The results
and the opportunity for partners 3 of 3

Question 3: What is the most frequent influence of cybersecurity spend?



Key lesson: Focus on education and awareness

While economic factors will be an influence, and around one fifth will stick to their defined budget, it's essential that partners are flexible and continually engaging with their customers on market changes with the threat landscape a prominent driver of spend. This applies to training and education as much as technology, and also to ensuring that new IT innovations (from 5G or OT deployments) are secured as they represent not only a new attack surface, but also potentially new investment by their customers.

As an example opportunity, human error accounts for a significant portion of security breaches yet many organisations lack comprehensive cybersecurity training programs - and users are exposed to rapidly evolve range of threats. ***Partners who address this gap can differentiate themselves and build long-term client relationships, while helping ensure their customers do address the changes ahead.*** Nearly quarter of spend being held at pre-defined budgets highlights that cybersecurity budgets are far from unlimited, so introducing new solutions or services needs to be part of a long term development, and need to address the latest concerns

Strategic implication: Develop training programs and resources to educate clients about best practices, emerging threats, and the importance of a security-first culture.

Challenges to overcome

1. Budget constraints

Securing budget for cybersecurity investments remains a top challenge for many resellers. This is often due to competing priorities or a lack of understanding of cybersecurity's ROI. Resellers should focus on presenting clear value propositions, including cost savings from preventing breaches and compliance-related benefits.

2. Vendor proliferation

With an overwhelming number of vendors and solutions available, customers often struggle to navigate the market. Resellers must guide them through this complexity by curating and recommending the best-fit solutions. Build strong vendor partnerships and streamline your portfolio to focus on high-quality, interoperable solutions – the trend towards platforms can provide a starting point, and then add complimentary products.

3. Evolving threat landscape

The speed at which cyber threats evolve poses a challenge for both resellers and their clients. Stay ahead by investing in continuous training and adopting cutting-edge tools that leverage AI and machine learning for threat detection.

Building a ***winning strategy for 2025***

Diversity services

Expand beyond traditional solutions to include MDR, zero-trust frameworks, and cloud security.

Leverage analytics

Use data-driven insights to identify customer needs and personalize solutions.

Strengthen partnerships

Collaborate with leading vendors and cybersecurity distributors to access the latest tools and technologies.

The cybersecurity market offers immense opportunities for resellers, but success requires a proactive, customer-centric approach. By addressing budget challenges, focusing on education, and delivering specialised solutions, resellers can position themselves as indispensable partners in their customers' security journey. As 2025 unfolds, ***those who embrace innovation and adaptability will be best equipped to thrive in this dynamic landscape.***