VansonBourne

How brands know

What drives trust, consideration and confidence in tech buyers today

As far as sectors go, cybersecurity is about as dynamic as it gets. Markets are crowded, customer expectations are shifting, and the pressure to make the right decisions is growing.

At the same time, vendors are competing harder than ever for attention in a landscape where messaging, positioning, and product claims increasingly blur together. The rise of AI-generated content is only accelerating that challenge.

For B2B technology marketers, keeping up with this pace of change is becoming increasingly difficult. Strategies and priorities evolve quickly, but many teams still lack a clear view of how their brand is actually perceived in the market.

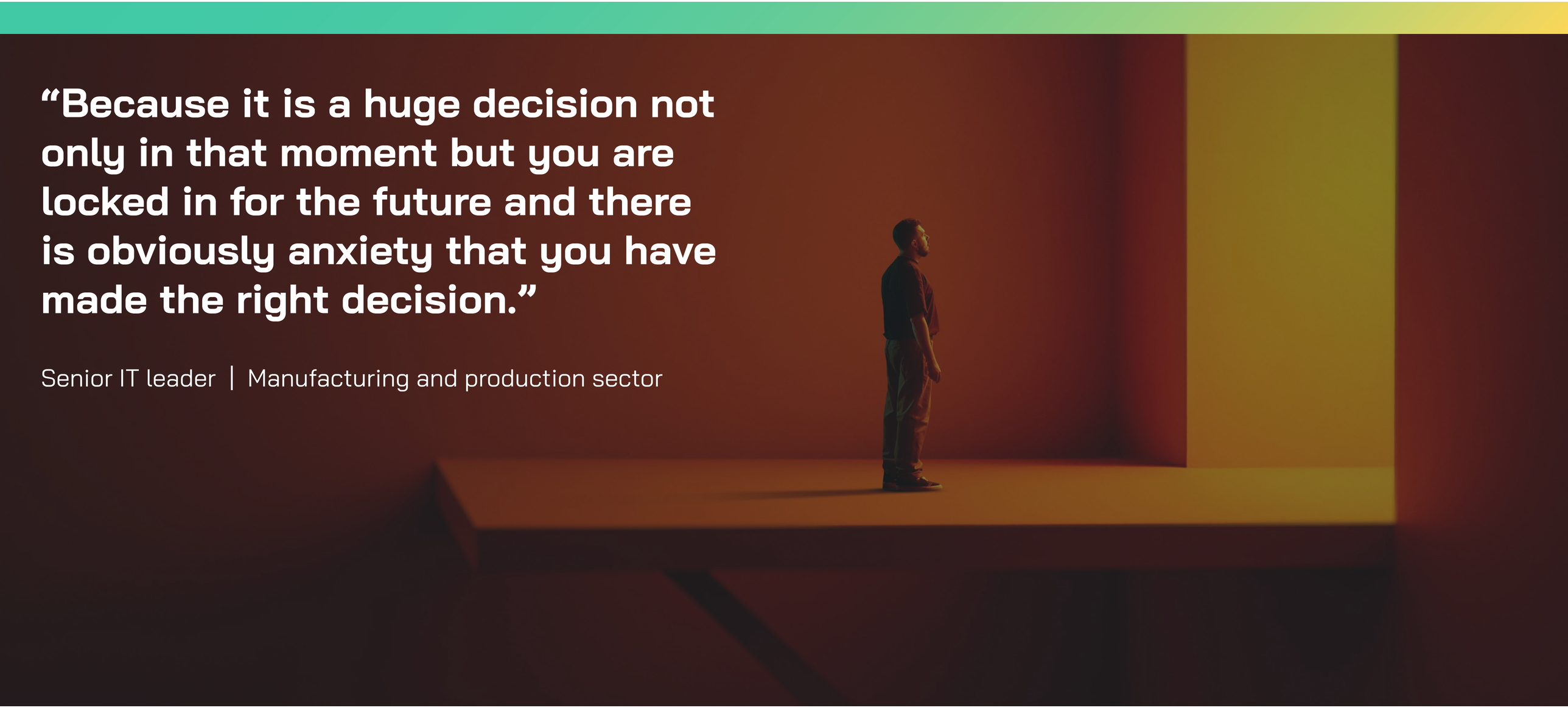
Do brands know what makes buyers see them as credible and trustworthy?
Do brands know what shapes awareness and consideration?
Do brands know what helps them stand out, and what causes them to blend in?
Do brands know what builds confidence during the buying process?

Without clear answers to these questions, brands risk making decisions based on assumption rather than evidence.

To explore these challenges, we surveyed 300 senior IT and IT security decision-makers across the UK and US to better understand how cybersecurity buying decisions are being shaped today.

This research identifies the factors influencing how cybersecurity vendors are perceived, evaluated, and selected: from internal pressures and changing buyer expectations to the signals that build trust and credibility.

Five factors shaping cybersecurity decision-making today



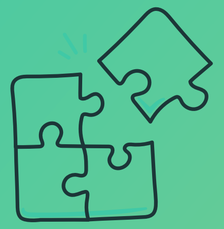
“Because it is a huge decision not only in that moment but you are locked in for the future and there is obviously anxiety that you have made the right decision.”

Senior IT leader | Manufacturing and production sector

Scrutiny 1

88%
of IT decision makers agree internal scrutiny on the purchasing of new solutions is higher than it used to be

Capacity 2



79%
agree that limited internal capacity is forcing them to depend more heavily on vendors to inform and influence security decisions

Expectations 3

88%
say their expectations of cybersecurity vendors are higher than they were 1-2 years ago, making it harder for vendors to meet them

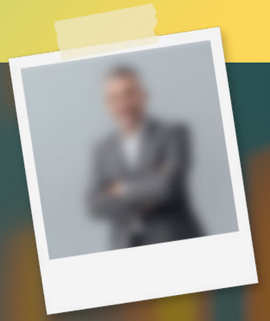
Is there a role in business today that comes with the same level of pressure as a cybersecurity decision maker?

Our research highlights five factors shaping their role and decision-making process. A purchasing journey that was never straightforward to begin with is becoming even more complex to navigate.

Let's start with the growing pressure from within. 88% told us that **internal scrutiny** on the purchasing of new cybersecurity solutions is higher than ever. The high-profile impact of cybersecurity incidents places these decisions under closer inspection than almost any other area of the business.

In addition to this, the question of capacity. 79% of IT leaders state that **limited internal capacity** is forcing them to depend more heavily on vendors to inform and influence security decisions. While the scrutiny on cybersecurity products and vendors grows, so too does the reliance on them, and that's a shift vendors need to be aware of. The ability to build confidence and reduce uncertainty is becoming just as important as product capability.

However, that trust is becoming harder to earn as our third factor shows. Almost nine in ten (88%) say that their **expectations** of cybersecurity vendors are higher than they were one to two years ago, making them harder to meet.

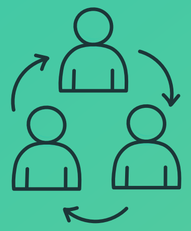


"Trying to decouple the marketing blurb from vendors vs. the tangible value due to lack of evidence across industry and also limited time to test products"

Senior IT decision maker | Public sector

Friction

4



72%

agree that purchasing cybersecurity solutions has become more challenging due to shifting priorities among stakeholders in their organisation

Compounding the extra scrutiny and the rising expectations is the growth in the buying committee within organisations. This is making purchasing decisions even more challenging.

In fact, 72% of our ITDM respondents point to shifting stakeholder priorities as a growing source of **friction**. Chief among the many reported causes of friction were risk and compliance concerns (49%), conflicting priorities (40%) and difficulties comparing vendors objectively (39%).

Together, these pressures are reshaping how organisations evaluate vendors and approach vendor selection.

Evaluation

5

92%

of those who've faced vendor selection challenges say they have changed their approach to evaluation

Among those facing vendor selection challenges over the last two years, the vast majority (92%) say they have changed their approach to **evaluation** (more on that later...).

And so it's in this environment that B2B tech marketers and vendors now need to operate. To build awareness and trust, to cut through the noise, and to make confident decisions in increasingly complex markets.

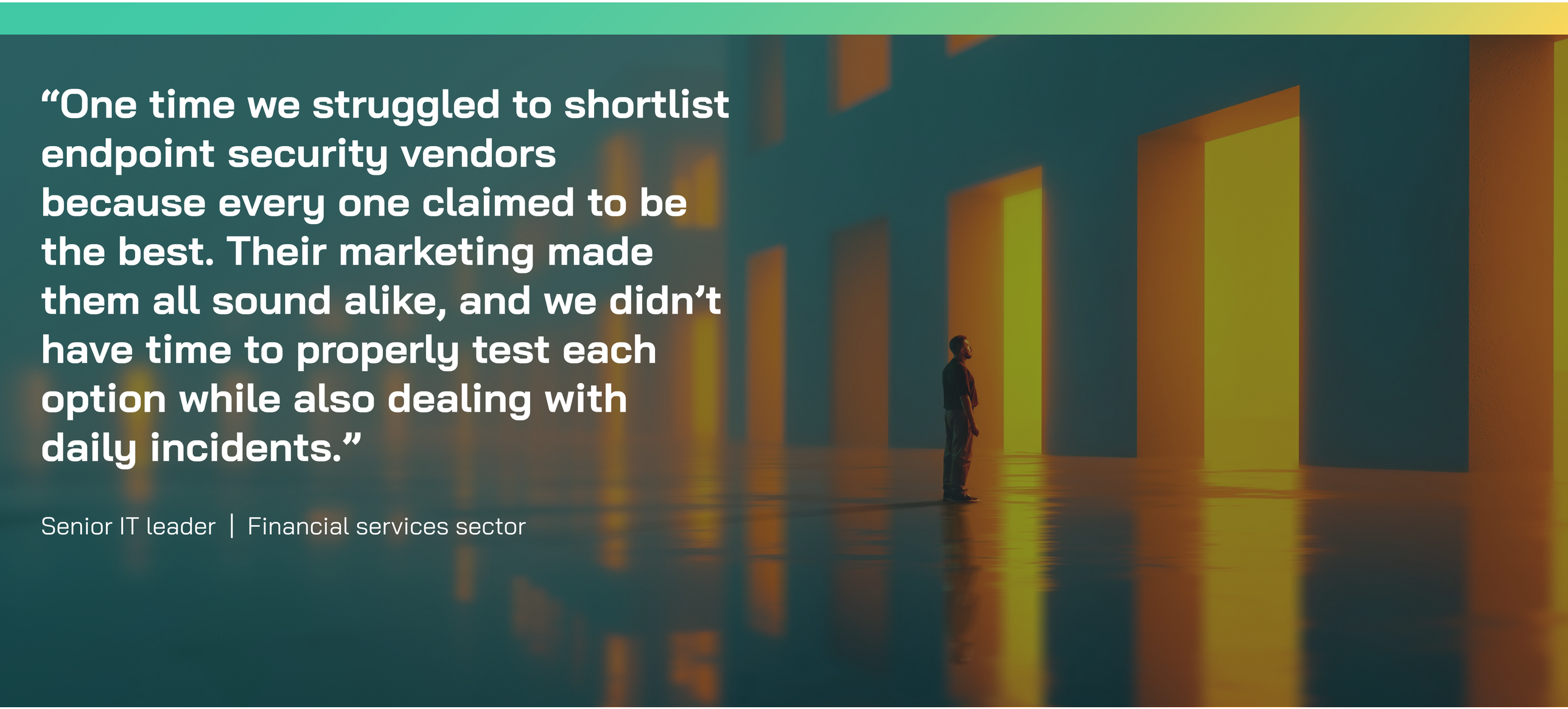
Knowing how decisions are being shaped has never mattered more. In the next section, we go inside the cybersecurity buying process.

"There was a time when our security team struggled to define priorities for a new cybersecurity vendor because different departments had conflicting requirements.

This led to delays in shortlisting vendors, multiple rounds of internal meetings, and difficulty presenting a clear, unified business case to executives for approval."

Senior IT leader | Professional services

Inside the decision



“One time we struggled to shortlist endpoint security vendors because every one claimed to be the best. Their marketing made them all sound alike, and we didn’t have time to properly test each option while also dealing with daily incidents.”

Senior IT leader | Financial services sector

Shortlists are swayed by known brands, but the door's not fully closed

Given the five factors we've just explored, it's little wonder that cybersecurity buyers are drawn to brands they know.

71% told us they're less likely to consider a cybersecurity vendor they have not heard of before.

For brands that already come readily to mind for buyers, this creates a clear advantage. Once organisations begin formally evaluating vendors, much of the decision has already been shaped by what they know, who they trust and can easily recall.

In addition, the internal capacity struggles we observed earlier are reflected in almost a third (32%) who rank finding and shortlisting suppliers as one of their top three most challenging stages of the procurement process. Buyers may rely on vendors they already know, but they are also struggling to invest time in researching unfamiliar brands, especially when resources are limited.

But there are nuances – and therefore opportunities – for less well-known brands to enter the fray. While a mix of known suppliers and formal research (58%) is the most commonly used source when considering which vendors to invite forward, there are still significant portions of buyers who turn to independent research and industry reports (53%) or recommendations from trusted peers and partners (50%).

What's more, buyers are changing how they evaluate vendors. As we saw earlier, in the last two years over nine in ten (92%) have changed their approach to vendor research and selection, while almost all (97%) expect clear, credible proof from cybersecurity vendors much earlier in the decision process.

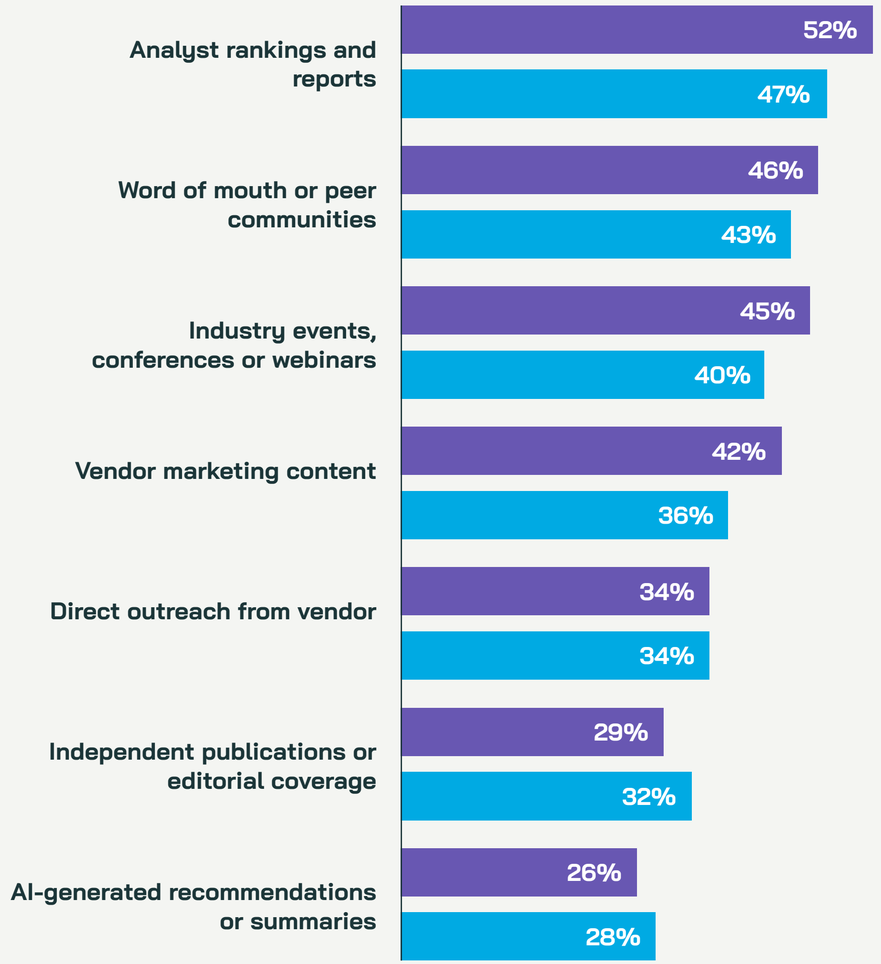
So while 40% report suppliers they already know or that come to mind immediately as a common source for building their shortlist, it's certainly not a closed shop. But with such a small proportion of buyers in-market at any one time, brands must seize their chance to build awareness and trust. Up next, we'll explore how.

What builds awareness and trust in cybersecurity?

If a shortlist is largely (though not entirely) built from memory, an important question is how vendors get into that memory in the first place. For cybersecurity buyers, awareness is built through a mix of trusted sources, most commonly analyst reports (52%), peer recommendations/communities (46%), industry events (45%) and vendor marketing content (42%).

What makes this particularly interesting is that these sources do more than build awareness, they also shape trust. Our findings show that the same common sources that make a brand known are often the ones that make it credible, meaning they have a direct influence on consideration.

Sources that have been most influential in building awareness and trust in cybersecurity vendors over the last 12 months



This reinforces the importance of showing up consistently in the places buyers already trust, with clear and credible messaging. Awareness and reputation are more than metrics. They influence which brands buyers trust, remember, and ultimately consider.

The challenge for brands is that awareness and trust are shaped by multiple influences, often working together. Without a clear understanding of how buyers perceive them, it becomes difficult to know where to focus, what to reinforce, and what is driving consideration.

So what matters most to cybersecurity buyers and their teams?

When it comes to cybersecurity, you cannot skip the fundamentals. By the time vendors reach evaluation, their criteria are already identified. Buyers aren't unsure about what matters, but they are unsure about who can deliver it.

By far the factor that matters most to cybersecurity teams when researching a new vendor is that they can meet security, risk and regulatory requirements (48%). And yet in the vendor assessment challenges they report, many are struggling to identify and agree internal priorities for what they need (53%) or to compare vendors in terms of value, risk and long-term impact (52%).

In total, 90% admit they struggle when evaluating cybersecurity vendors.

The main challenges organisations experience when evaluating cybersecurity vendors

38%

Difficulty in distinguishing meaningful differences between vendors

34%

Budget constraints or cost justification challenges

32%

Difficulty validating vendor claims

28%

Conflicting priorities among stakeholders

25%

Complexity of procurement or governance processes

25%

Too many vendors to assess effectively

The opportunity for brands is there, but to effectively seize it requires standing out in a crowded market with more than just a solid product. 94% of cybersecurity leaders agree that clear messaging and credible proof often matter as much as product capability when gaining internal buy-in.

And that for many brands is where the difficulties lie.

Buyers are searching for meaningful differences

Seven in ten (70%) say it's getting harder to see how cybersecurity vendors stand out from each other in meaningful or relevant ways.

This challenge runs throughout the evaluation process. Of all the obstacles buyers report when assessing cybersecurity vendors, difficulty distinguishing meaningful differences between providers (38%) ranks highest. Around a third (32%) struggle to validate vendor claims, while one in four (25%) say there are simply too many vendors to assess effectively.

The result is a market where buyers often know what they need, but find it increasingly difficult to identify which vendor is best placed to deliver it. Similar claims, overlapping positioning, and a lack of clear proof make comparison harder than it should be.

"Difficult to articulate and position different vendors and their actual capabilities (and differences) internally due to many outward similarities across vendors. This leads to a challenge in building internal confidence."

Senior IT decision maker
Technology sector

What this means for brands

Cybersecurity buyers are under more pressure than ever. Internal scrutiny is rising, stakeholder groups are growing, and expectations of vendors continue to increase.

Buyers are struggling to distinguish between vendors in a market where similar claims, overlapping positioning, and limited time make comparison increasingly difficult. The result is that buying decisions are becoming more risk-sensitive. Buyers are not evaluating every option equally. They are relying on familiarity, trust, credible signals, and the ability to justify decisions internally.

This creates a clear advantage for brands that are already known, trusted, and easy to defend. Familiar vendors are more likely to make the shortlist, more likely to be considered, and more likely to move through the buying process with less friction.

The challenge for marketers is not simply building awareness. It is **knowing** what buyers think, **knowing** what drives trust, **knowing** what influences consideration, and **knowing** where their brand stands relative to competitors.

Without that understanding, decisions about positioning, messaging, and investment are often based on assumption rather than evidence.

Brand research is **how brands know**.

Five key takeaways for tech marketers

1. Buyers are under pressure, and that is changing how decisions are made
Scrutiny, stakeholder friction, and limited capacity are making cybersecurity buying decisions harder to navigate. Buyers are increasingly looking for confidence and reassurance alongside product capability.

2. Familiarity creates an advantage before evaluation begins
Known brands are more likely to be recalled, shortlisted, and considered. In many cases, buyers are making decisions from a subset of vendors they already know and trust.

3. Trust is built long before procurement starts
Analyst reports, peer recommendations, industry events, and vendor content do more than build awareness. They help shape credibility and influence consideration.

4. Buyers know what they need, but struggle to identify who can deliver it
Security, risk, and compliance requirements are clear. The challenge is comparing vendors, validating claims, and identifying meaningful differences between providers.

5. Markets move, and buyer perceptions move with them
What drives awareness, trust and consideration today may not do so tomorrow. Brands need to understand and keep pace with changing buyer expectations.

Expert view: the strategic power of brand research in B2B tech

Kate Harrison-Whitcombe & Richard Wyllie | Vanson Bourne Brand Research Product Leads

As our research shows, by the time buyers enter the decision-making processes, some brands have a clear advantage as they are known, trusted, and easier to justify. Decision-makers are looking for signals that reduce risk when faced with pressure and uncertainty. Familiar vendors are those that provide reassurance before formal evaluation even begins which makes it much easier for them to sway a decision in their favour.

This is where brand research becomes critical. Understanding how your brand performs across the funnel, and how that compares to competitors, gives you clear view of where you are gaining traction (brand growth) and where you are falling behind.

Brand research can help you to answer key questions: are you known, but not understood? Considered, but not trusted? Or trusted, but losing out at final stage?

Each of these points to a different problem, and without the clarity from research, it becomes difficult to know where to focus. In practice, this means knowing where to invest, whether that is building awareness, strengthening positioning, or providing clearer proof and credibility. Your efforts are at risk of being misdirected, and opportunities being missed.

The brand funnel is a measure of performance, but it also reflects how decisions are made. It shows that buyers do not assess every option evenly, that known vendors are easier to trust and defend internally, and that unfamiliar vendors face a clear barrier to entry.

This aligns with what we have seen throughout the report:

- *Buyers commonly default to what they know*
- *They rely on credible signals*
- *And avoid unnecessary risks wherever possible*

So while many vendors focus on differentiation at the point of decision, the reality is that much of the outcome is determined before that stage begins.

Get in touch to learn more about Vanson Bourne's brand research services.

enquiries@vansonbourne.com

Discover how brands know
with brand research built for the tech sector

Find out more

VansonBourne

Stronger insights. Smarter strategy.

© Vanson Bourne 2026