Fast decisions, high stakes

How to sell to cybersecurity buyers in a crowded, fast-moving market

The Hoffman Agency

Index

01

Introduction

Introduction

Good cybersecurity defense has never been as critical as today.

It's easy to become used to dire warnings, with new threats, new threat actors and new vulnerabilities making headlines every day. But the use of AI in cyberattacks is changing the game.

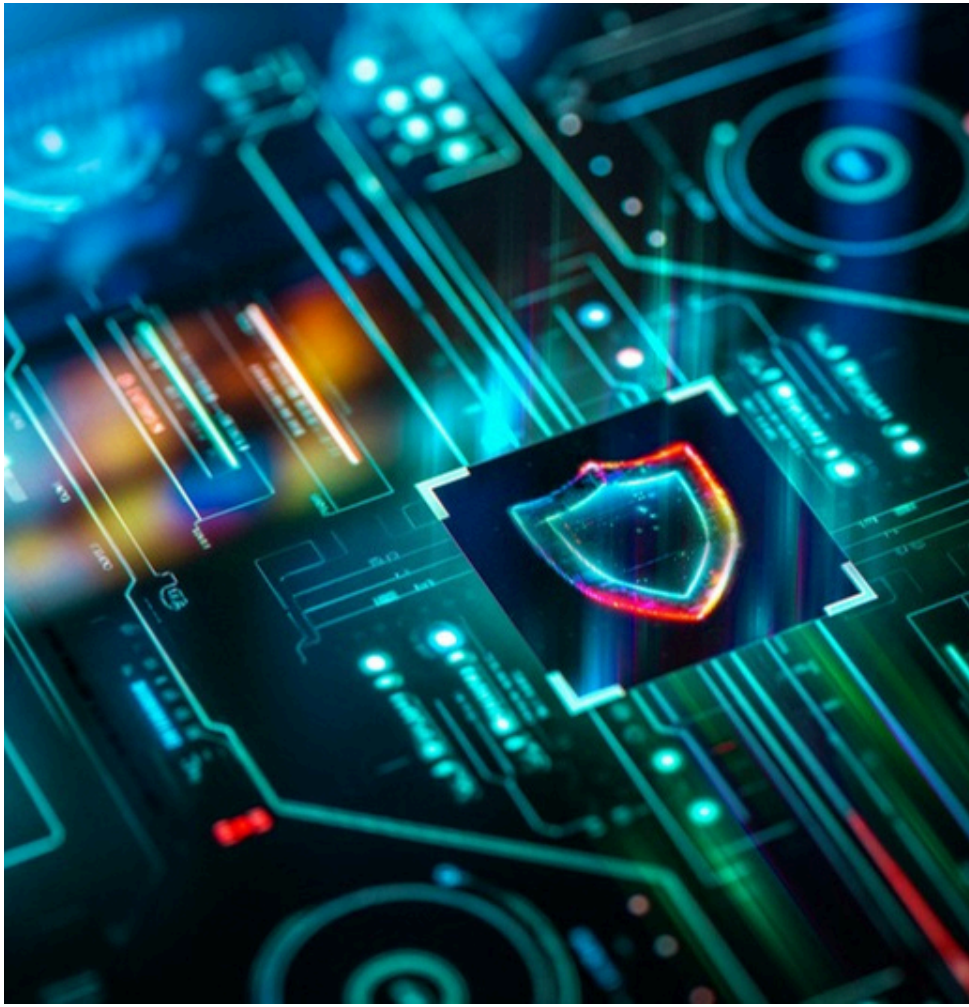
Claude Mythos has, in tests, found thousands of previously unknown vulnerabilities in software, some undetected for decades. If this ability can be used by threat actors to find vulnerabilities, every organization is at risk, no matter how quickly they patch.

Describing cyberthreats as "evolving" is common enough to be a cliché. But this is different — it could be a revolution.

As a result, many organizations will be reviewing their cybersecurity vendors and the solutions they provide and asking some difficult questions of their current providers. They may decide that they need more protection, or even that they need a new provider that can offer better value for money.

If the answer is yes, then we can expect many organizations to start the search for new and replacement solutions. What does that process look like? Where are buyers finding the information they need to make a good decision?

To understand how buyer decisions are changing, The Hoffman Agency surveyed 500 cybersecurity decision-makers in the U.S., U.K., France and Germany.



Executive summary

Cybersecurity is a fast-moving market, and one that may be undergoing radical change thanks to AI-assisted vulnerability discovery. There are more vendors than ever, but also higher budgets and more demand for products and services that address specific needs. Many are planning to invest in securing their AI models next year, but there is also a focus on the cybersecurity *"basics"* — better identity management, endpoint protection, and more.

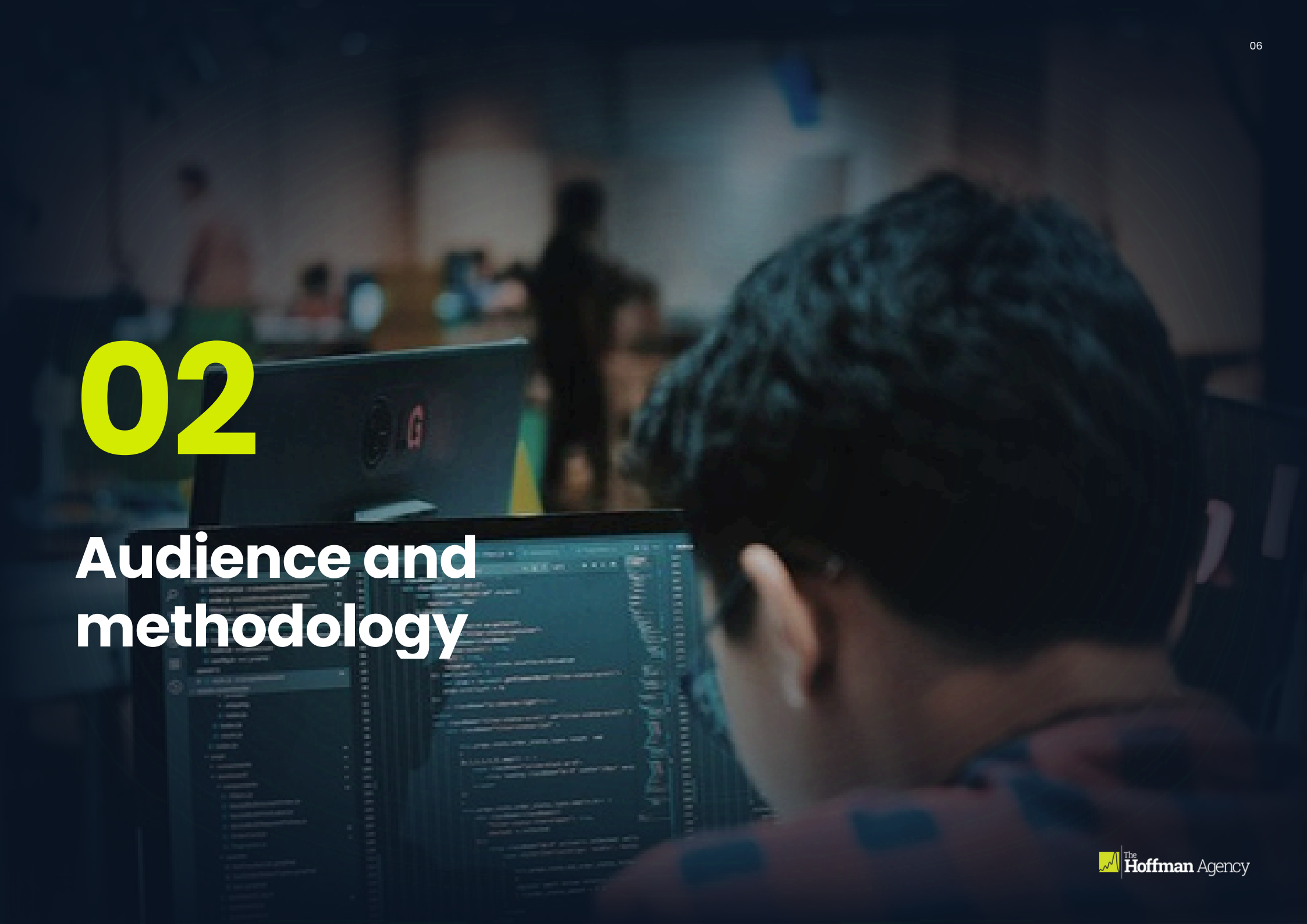
The need to put protection in place quickly is compressing the buying process — organizations cannot wait until they suffer a breach to do something, they need to act. For most cybersecurity buying journeys, the time from the identification of a need to final selection is a mere six months, a very short period of time when the average ticket price is over half a million pounds.

Buyers are also happy to replace vendors if they feel their current providers aren't up to the task — good news for those looking to increase market share, but it does mean loyalty isn't enough to keep customers happy.

To make fast decisions, buyers are looking for evidence. Case studies, customer wins, and third-party endorsement are incredibly valuable, not just in getting a sale over the line, but when buyers are researching potential vendors. Marketing activities that are thought of as "bottom of funnel" are just as useful at the top.

Buyers are also engaging vendors early in the process, looking for responsive partners who can provide answers quickly and demonstrate their flexibility and willingness to meet a buyer's needs. Many are also using LLMs to get quick answers, and a small but significant minority are using AI throughout the whole buying process. This complicates matters for marketers, who need to provide the materials that feed LLMs, not just the material that buyers are engaging with directly.

Cybersecurity buyers are moving quickly to make decisions — but they still want to choose vendors that are rated highly by analysts and consultants, can back up their claims, and offer good value for money. Vendors need to tick all the boxes they used to, they just have less time to do it.



02

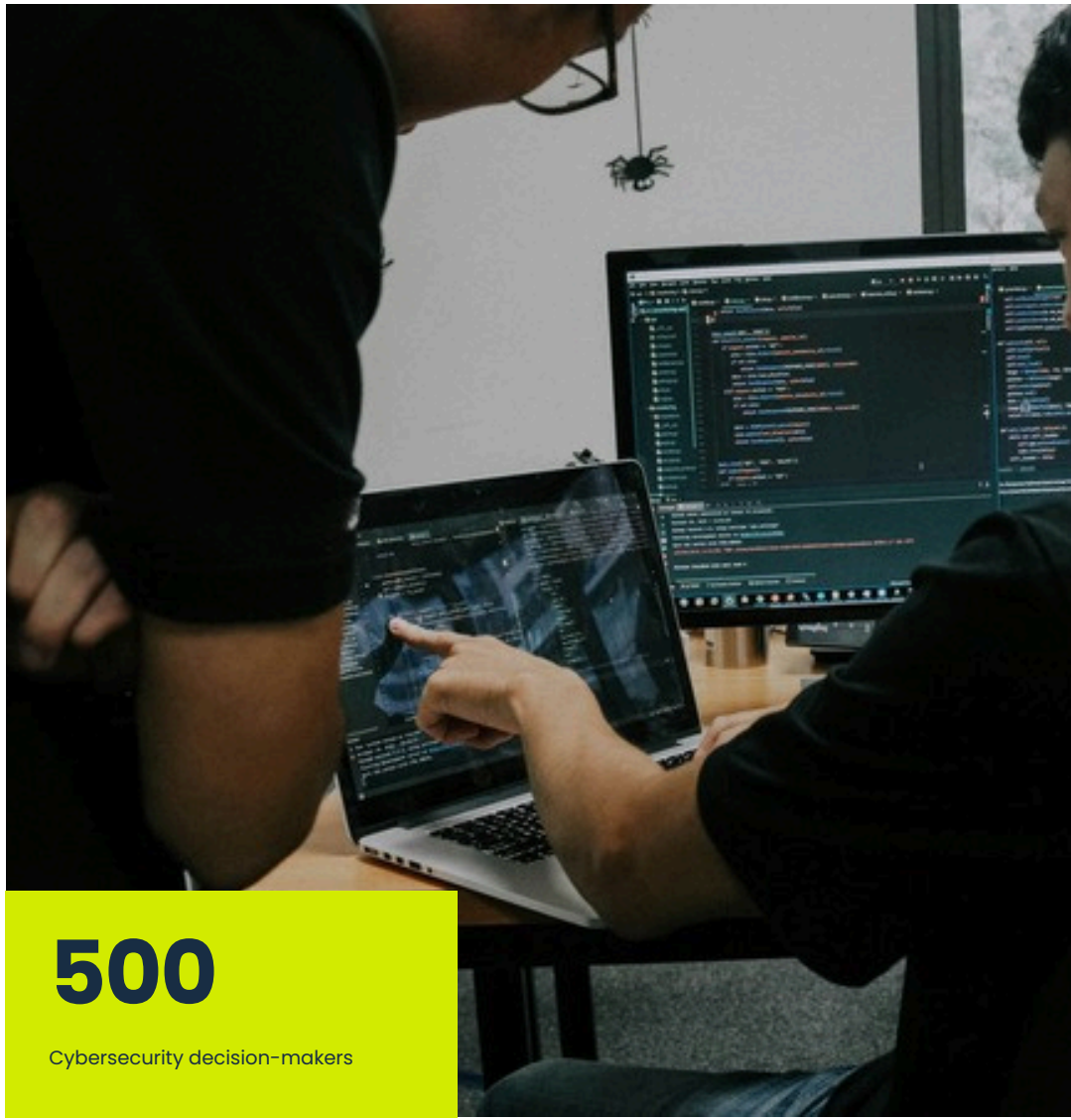
Audience and methodology

Audience and methodology

This research is based on the responses from senior cybersecurity decision-makers across four leading markets.

The research was conducted by Coleman Parkes Research, via an online questionnaire of 500 cybersecurity decision makers (C-levels and heads) across the U.S., U.K., France and Germany, who have made major technology purchases in the last 12 months.

The sample was split between the financial services, technology, telecoms, media, healthcare, retail, and the public sector. The research took place in April 2026.



500

Cybersecurity decision-makers

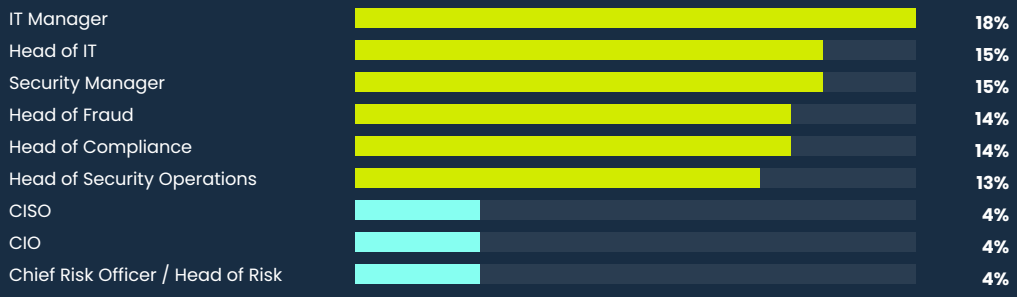
Respondent profile

Industry

Markets

40%	20%	20%	20%
USA	UK	FRANCE	GERMANY
n=200	n=100	n=100	n=100

Job title



Global employee numbers

Average: 4,600 employees

03

The state of cybersecurity investments

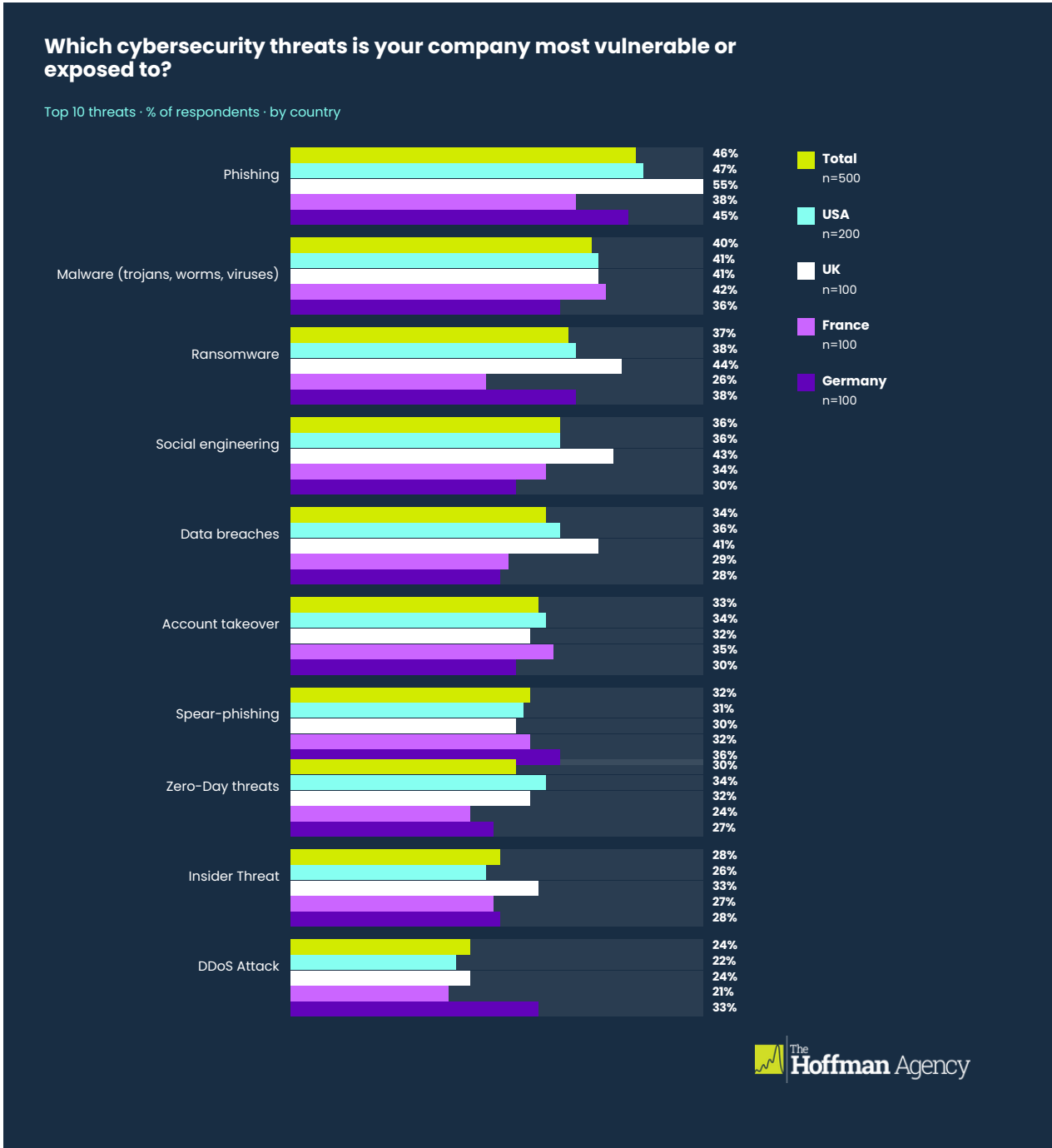
Buyers' perceptions of cyberattacks

Key to understanding the current market is understanding how buyers perceive cyberattacks — particularly where they think they are currently weak and may need to shore up their defenses.

We asked organizations about what cybersecurity threats they were most vulnerable to or exposed to. The most common answers were as we might expect: phishing, malware, ransomware, and social engineering.

With the threat that AI poses, we might expect zero-day threats, supply chain attacks, and AI-powered attacks have greater prominence. One possibility is that these news stories of AI-driven attacks may not have filtered through — more likely, these threats are the most seen and it is unknown if AI has a hand in them.

Vendors that specialize in protection against less visible or less understood threats may have to work harder to convince potential customers of their worth.



Some parts of the IT estate are seen as more at-risk than others.

Some of the areas where organizations say they need cybersecurity technology relate closely to the threats they are the most vulnerable to, particularly endpoint security and identity and access management.

AI systems and governance, and remote workforce security are close behind, seen as priorities for more than a third of organizations.

Remote work and AI cybersecurity being so close in need shows how quickly securing AI has grown in importance — remote working has been a priority for at least five years, and AI has already caught up.

What areas of your company need cybersecurity technology the most?

Top 5 priorities · % of respondents · Base: 500

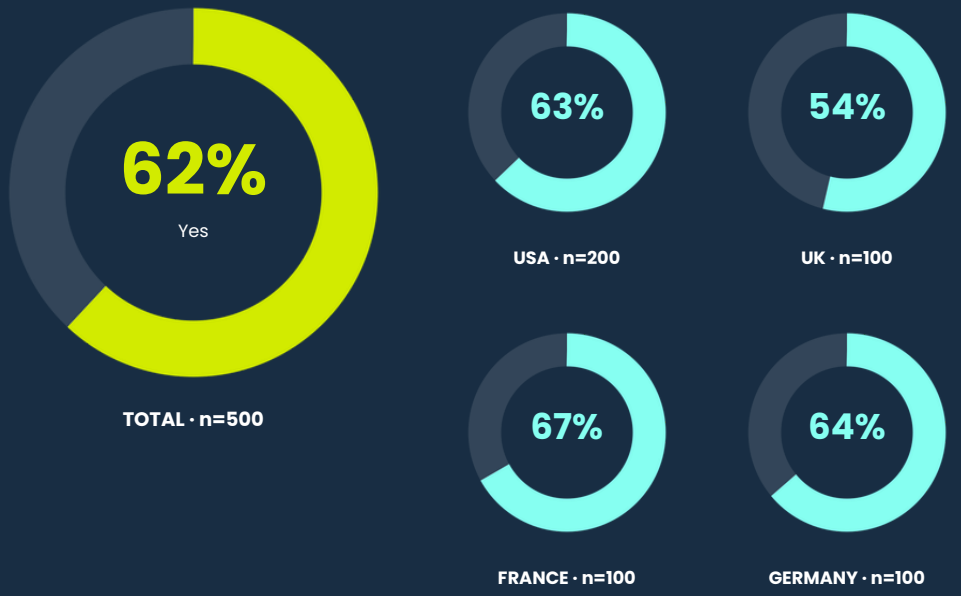
Cybersecurity investments: all change?

Three-in-five organizations are looking either for a new provider, or to switch provider, in the coming year.

In other words, most organizations are either starting or are some way along the buying journey. Cybersecurity is a crowded market but there are a lot of potential buyers out there.

The most common reason cited for those preparing to invest is "the need to respond to threats", highlighted by 55%. But the need to secure AI systems is cited by 38% — higher than the need to reduce costs or cope with talent shortages.

Are you looking to work with new cybersecurity technology suppliers in the next year?

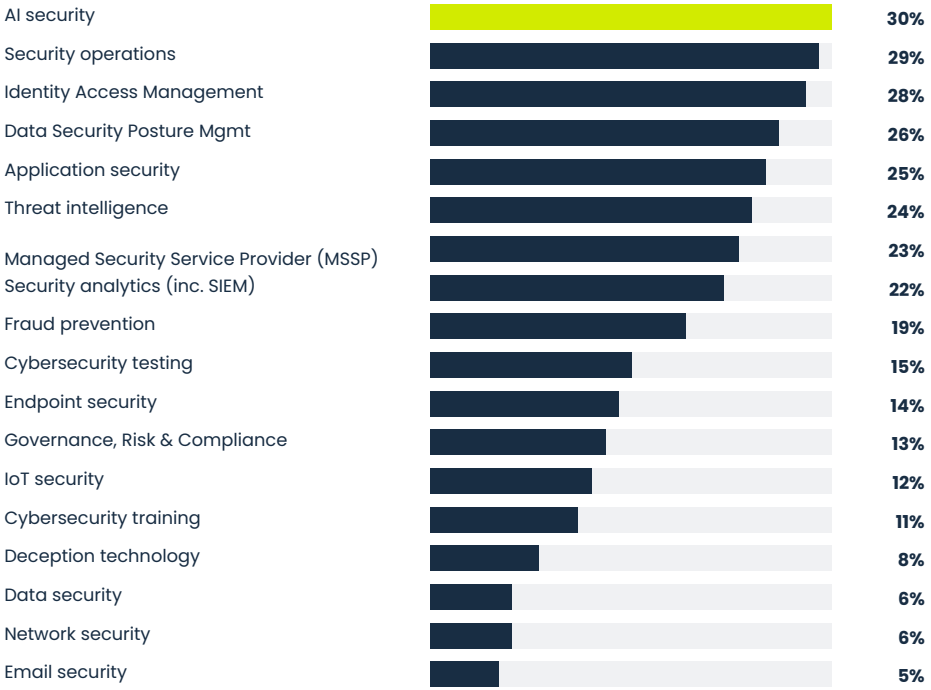


What cybersecurity products are being bought?

Organizations see the next year as one of changing priorities. Only 8% invested in AI security last year, but 30% expect to invest in a new solution.

PAST 12 MONTHS

NEXT 12 MONTHS



The area of “AI security” has exploded alongside AI, whether that’s securing AI models or AI-assisted security. Analyst Richard Stiennon of IT-Harvest is now tracking over 400 vendors categorized as “AI Security”. 325 were founded in the last five years, rather than companies that pivoted to AI.

What drives the need to purchase new cybersecurity technology?

As well as these new purchases, there are also plans to replace solutions in the next 12 months, in particular network security, endpoint security, and security analytics.

Advancing technology and new threats are the main reasons to make a new purchase, but almost half of organizations said that their buying choices are driven by an attack. Combined with 62% "in-market" for new solutions, that means a lot of organizations are looking to solve ongoing problems as well as future ones.

Outside of this top five drivers were demands from clients, increased revenue and reduced costs. Dissatisfaction was the least popular driver for new cybersecurity purchases — yet still reported by a substantial 31% of organizations. That's nearly a third of organizations threatening to move because their current provider isn't good enough.

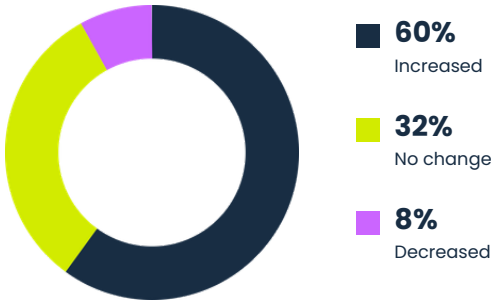
What factors drive the need to purchase new cybersecurity technology?

Top 5 drivers · % of respondents · Base: 500

Organizations are not just shifting money around. Many are also increasing their budgets.

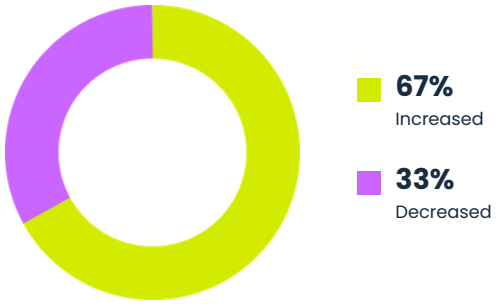
LAST 12 MONTHS

How budgets changed



NEXT 12 MONTHS

How budgets are expected to change



Most organizations have increased their investments in cybersecurity over the last year, with only around a third deciding this is an area where they can tighten their belts. Even more expect this investment to increase in the next year. Plus, organizations are spending big.

This is clearly good news for vendors. Cybersecurity is an increasingly crowded market, it is serving customers that are willing to spend, switch vendors if necessary, and invest in new products and services. Vendors looking to increase sales are fishing in an abundant pool.

The key to making the most of this market is to better understand the buyer journey – how do they make decisions from initial research, to shortlisting, to that final choice of vendor? And where and how can a vendor make the biggest impact?'

AVERAGE TICKET PRICE

£574,400

Typical ticket price for cybersecurity technology investments (last 12 months)

USA

$708,332

UK

£554,000

FRANCE & GERMANY

€715,975

The Hoffman Agency

04

The buying journey

How long from need to selection?

Before looking at the content and channels that influence a buying journey, it's worth looking at that journey, who influences it, and when vendors are contacted.

Measured from the time from the decision that a cybersecurity solution is necessary, to deciding what vendor can deliver, purchases take, on average, seven months — but some outliers are skewing this number. Most take less than six months. Just 15% take more than a year, and 15% take less than three months.

Given the level of investment, these are fast decisions.

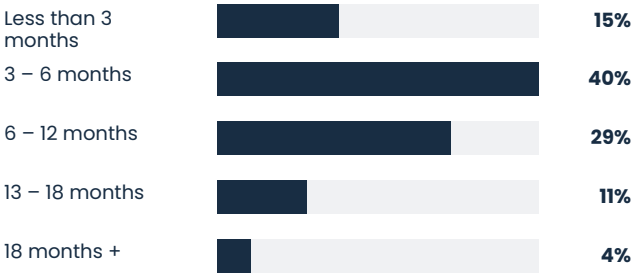
AVERAGE BUYING CYCLE

7

months on average

How long from "need identification" to "vendor selection"?

% of respondents · Base: 500



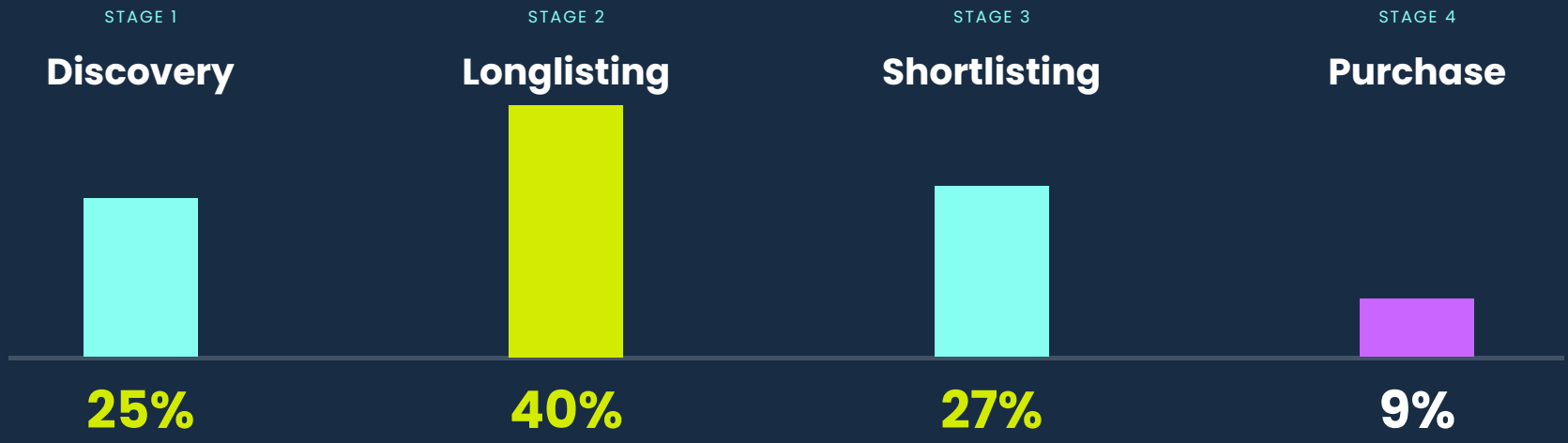
Who's involved in the decision?

Those most involved in making decisions are, as we might expect, IT and IT security teams. But cybersecurity is so important that C-level executives are often involved.

While others are involved, such as finance and legal teams, this is a vendor's main audience — mostly technical, but not exclusively.

Buyers engage vendors early in the process.

At what stage in the buying cycle do you ask for information from, or engage with a vendor?



65% of potential buyers make contact with vendors before the shortlisting stage.

This audience is looking to engage early in the buying process, perhaps as a result of compressed decision time.

Just 9% wait until they are making a final decision to get in touch. This is even higher in Germany, with 71% of buyers connecting with vendors early.

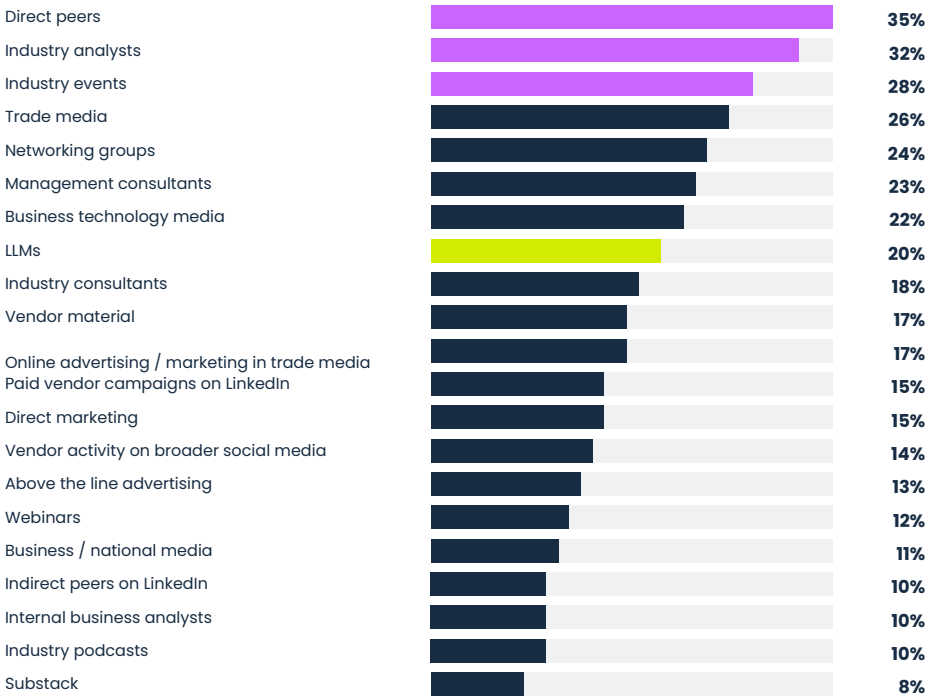
Resources and insights need to reflect this. Vendor content can't be focused on the reasons to buy from a particular vendor, but needs to be broader in scope and speak to a buyer that is still in an early research phase.

Source: Q12 — Coleman Parkes / Hoffman Agency Cybersecurity Buyer Survey, April 2026

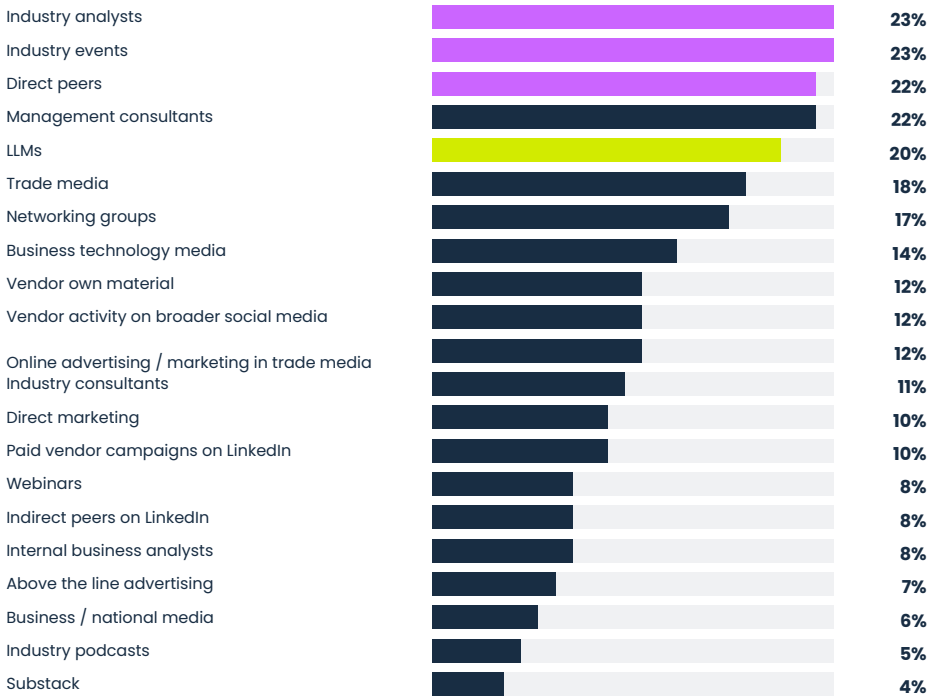
From awareness to selection: which channels and content types influence the buying journey?

Understanding the buying journey means not just understanding who is involved in decision making, but what sources, channels, and content types organizations use to research and better understand potential vendors – and reach a final decision.

AWARENESS



SELECTION



When making a cybersecurity purchase, buyers rely on a wide number of sources and channels for both initial research and final selection. But these stages are not the same. When researching, the net is cast wide for as much information as possible. At selection, organizations limit the number of sources to the ones they trust most or find more useful for that final stage.

The top three sources/channels of information for initial awareness are direct peers, industry analysts and industry events. For final selection, the top sources are similar: industry events, industry analysts, direct peers, and management consultants.

Rather than shift to different sources to make that final decision, buyers are mostly using the same, albeit fewer sources. This may be due to shorter buying cycles – buyers need information quickly, and so will begin with a focus on what they see as authoritative sources.

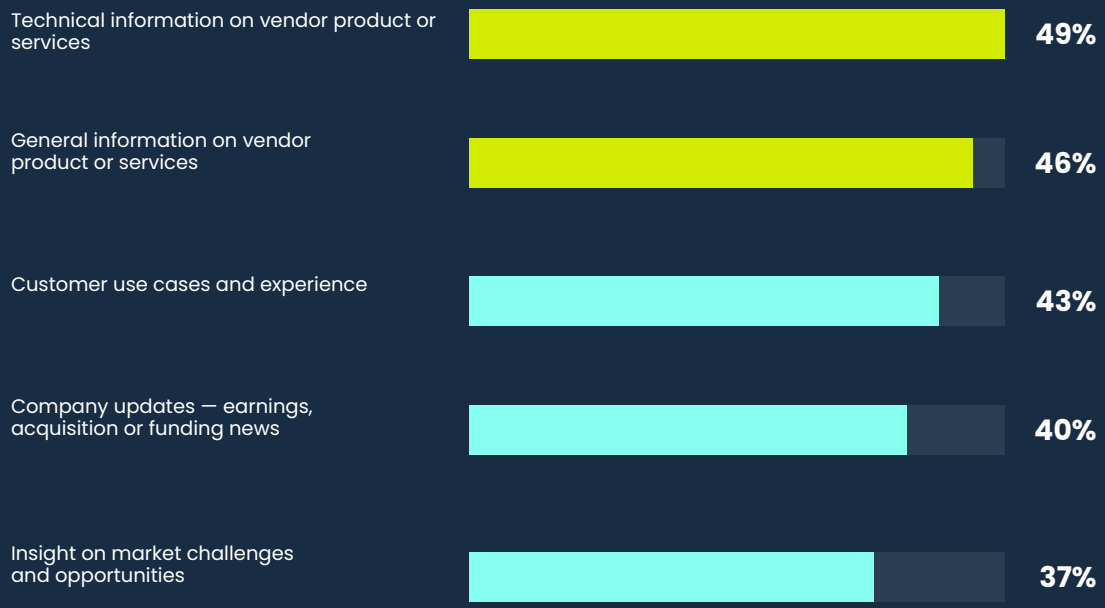
LLMs are the exception, used by 20% for both awareness and selection. This is likely due to LLMs having a keen user base who will rely on and trust these tools throughout the process.

Vendor content and content types

The most valuable vendor-produced content is information on services, particularly technical information, reflecting the technical audience involved in decision making. Customer use cases give buyers evidence that they are making a good choice, and company updates reassure buyers that the vendor will be a viable long-term partner.

What types of content from vendors do you find most valuable when making your purchasing decision?

Top 5 most valuable · % of respondents · Base: 500

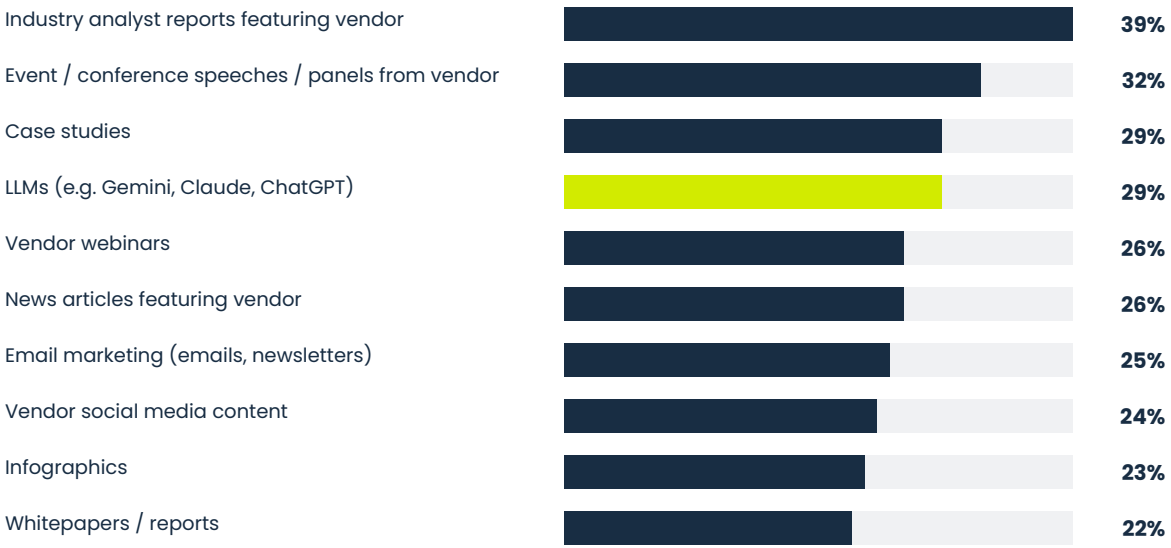


The Hoffman Agency

CONTENT TYPES

Which content types have the biggest influence on selection of a cybersecurity technology vendor?

Top 10 · % of respondents · Base: 500



There is no marketing "silver bullet".

When looking at specific content types, almost everything is influential. Even the least influential content type, vendor blog posts, is seen by 13% of buyers as having an effect on their final buying decisions.

LLMs feature again here, higher than popular marketing techniques such as email marketing, but below case studies and webinars. Right now, only 8% of buyers say that they use LLMs "all the time", but only 10% never use them, meaning that the majority use them some of the time.

As LLMs become more important, so will the material that feeds them — including those deemed less important here, such as press releases and blog posts. Buyers are influenced by everything from industry analyst reports to podcasts, from news articles to opinion content. A mix of different approaches and content types is the only guaranteed way to reach everyone — especially as LLMs become more important and pull in information from all different sources.

Third parties are vital to buying decisions.

Less than 1% of buyers do not consult with an outside agency.

The overwhelming majority use industry analysts, system integrators and consultants to help shortlist potential vendors — with most buyers using more than one third party.

Again, this is likely, at least partly, a result of making big purchasing decisions in a short timeframe – third parties can help reassure buyers that they are making a good choice.'

DO NOT CONSULT ANY OUTSIDE AGENCY

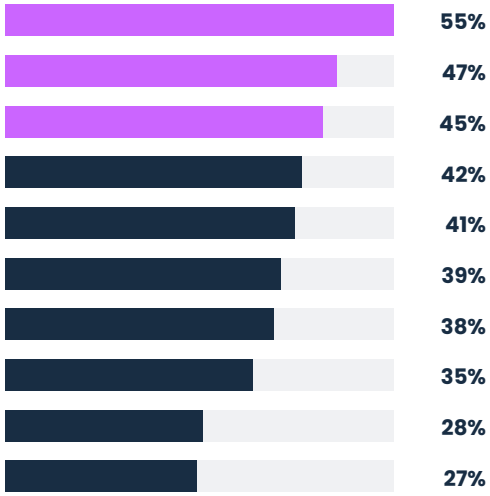
<1%

of cybersecurity buyers

Which third parties do you use to help identify and shortlist vendors?

% of respondents · Base: 500

What types of information in industry trade media are of most interest?



Buyers are looking for a better understanding of what they need to stay up to date.

We can see the need for information to help make quick decisions in the media that buyers find most interesting: industry news, peers investing in new services, and regulatory news. The popularity of data-driven research gives buyers insight into trends that can quickly back up their decisions.

The desire for technical data is reflected in media habits. The publications that are most read are not the most influential.

MOST READ NATIONALLY

CSO Online — U.S.
Infosecurity — U.K.
Journal du Net — France
Heise — Germany

05

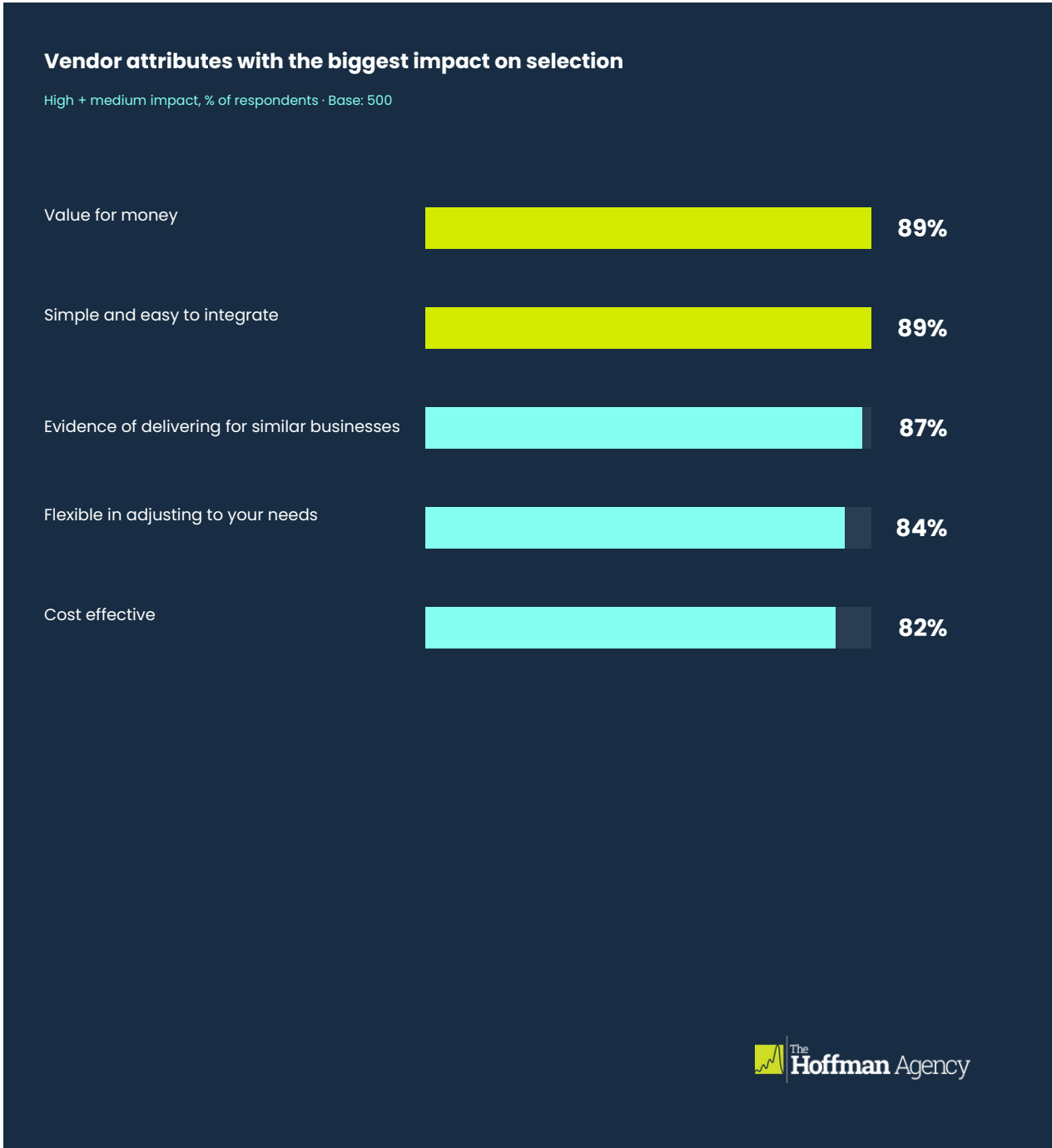
The final decision

Which vendor attributes have the biggest impact on selection?

What, ultimately, are buyers looking for in vendors' products and services that could make or break a buying decision?

Integration and value for money are top concerns, however it is important to note that value for money is more important than cost effectiveness, showing that buyers are happy to spend if they feel it is worth it.

One of the lowest impacts on buying decisions is a previous working relationship, showing that loyalty is far from enough to keep customers happy.



What would make you not want to select a vendor?

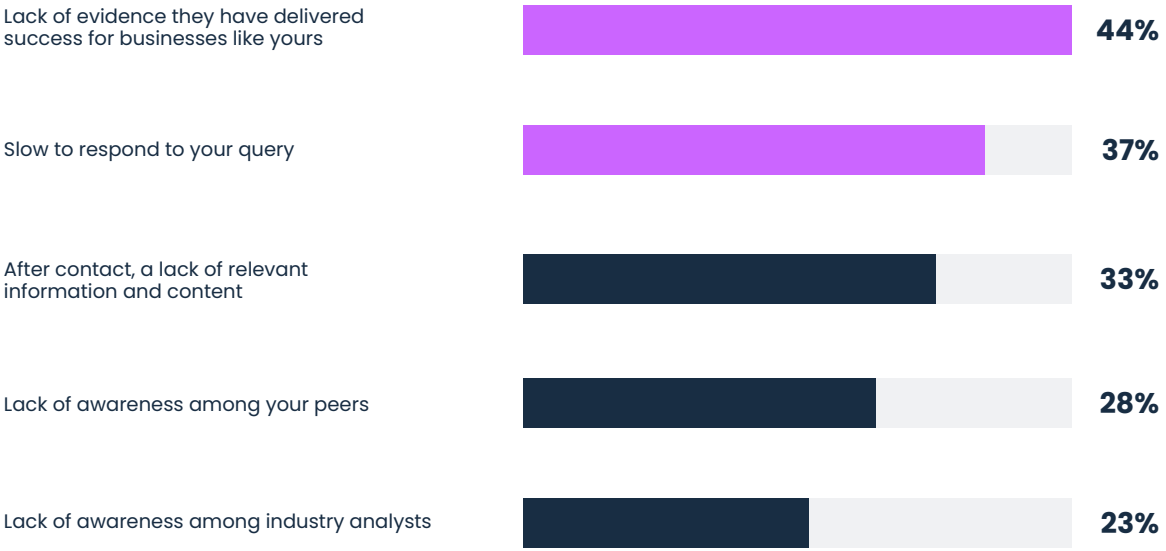
Lack of evidence through case studies and slow responses are the biggest reasons to reject a vendor.

Negative comments in the media or social channels are not — a poor review is not enough to sway most buyers.

They want to draw their own conclusions, but they need evidence to do so.

Top 5 vendor rejection factors

% of respondents · Base: 500



THE TWO FATAL FLAWS

No proof of delivery, or a slow response. Everything else, buyers can live with.

06

Fast-moving times mean fast decisions.

Fast-moving times mean fast decisions.

How fast is "fast"?

Six months may seem a long time to take a decision, but not when deciding on a vendor contract worth hundreds of thousands of pounds. The nature of cybersecurity today means that organizations need protection as soon as possible, and the amount they may lose to a data breach or similar event is far bigger risk than making a less-than-perfect choice.

To get to a decision quickly, the usual process of awareness, longlisting, shortlisting, and decision is being streamlined. Those on the front line, in IT and security, are more involved in the decision-making process than C-level execs or finance teams. Organizations are increasing budgets and happy to switch to a new vendor if they feel they aren't getting enough value for money.

That doesn't mean that decisions are being reduced to the basics of comparing costs and feature lists. Buyers still want vendors that understand the market, are responsive, and offer value for money over the lowest cost. Most of all, they need proof.

This is good and bad news for marketing teams. Getting these messages out has never been more important. Unfortunately, buyers are looking for these messages everywhere, with no clear delineation between the start and end of the buying journey when it comes to sources.

Complicating this, the growing use of LLMs means that those sources that are not as directly impactful, may have a greater impact when used by LLMs as a source.

THE BOTTOM LINE

Buyers want to make fast decisions to help keep their organizations safe from a growing and changing number of threats. Vendors need to reassure buyers that they are making the right choice.

The Hoffman Agency

What is the Cybersecurity Buyers Insight Report?

At The Hoffman Agency we don't want to guess how cybersecurity buyers make decisions. We need to know — so we can give our clients the best advice on where to focus their marketing communications efforts. Where do decision makers get their information on vendors? What are the most influential types of content they engage with? How is the market changing and what are the effects on buying cycles, budgets, and buying priorities?

This research provides the insight into how decisions are being made today, but how they have changed and will continue to change.

Who is The Hoffman Agency?

Defining communications broadly to include digital, content marketing, thought leadership as well as traditional PR, The Hoffman Agency knows how to differentiate brands and deliver air cover for sales. With a heritage in the tech sector, our work today cuts across a range of industries.

For clients with global needs, we operate in Asia, Europe and the United States. Unlike traditional agencies handicapped by their silo structure, The Hoffman Agency applies a collaborative approach to implementing multi-country campaigns. This leverage of content and thinking across geographies ultimately generates better results (and considerable less bickering).

While campaigns vary by client and industry, all share one theme: the creation of content that reflects the tenets of storytelling. This means developing narratives that prompt journalists to write and target audiences to read.

GET IN TOUCH

Talk to our cybersecurity experts:

Florie Lhuillier

SVP - Head of Cybersecurity

flhuillier@hoffman.com in

FOLLOW US

in