AI at Work 2024

C-suite perspectives
on artificial intelligence

okta
The World's Identity Company

Executive summary

Artificial intelligence is transforming how companies approach security, innovation, and efficiency

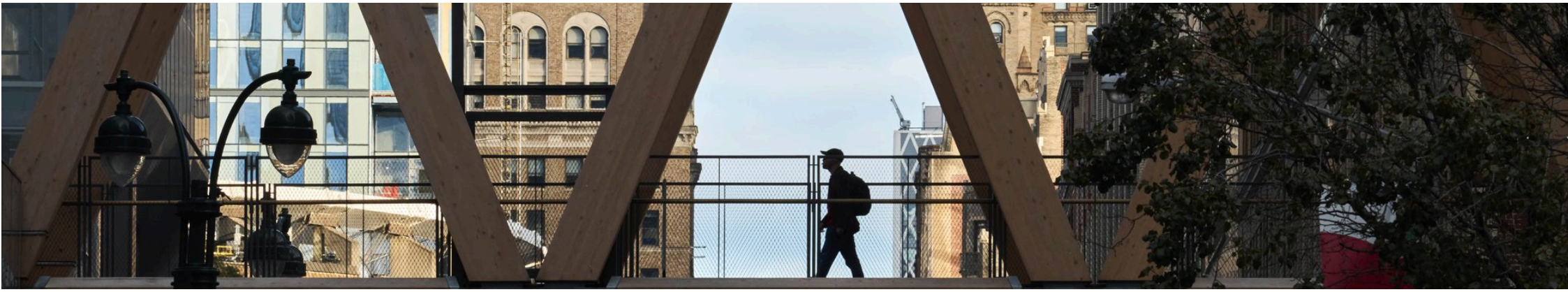
EXECUTIVE SUMMARY

Prepare for impact: AI is in the building

Our survey reveals executive sentiment, concerns, and priorities around artificial intelligence.

Although artificial intelligence (AI) has existed since the 1950s, the public release of OpenAI's ChatGPT in November 2022 propelled the technology into the forefront of just about every conversation. AI is featured everywhere, from newspaper headlines and social media takes to team stand-ups and board meetings. And that discussion hasn't quieted.

That's because every week seems to bring about a new leap in either the technology itself or how organizations infuse it into their products and internal systems. But legitimate businesses aren't the only ones taking advantage of AI to accelerate innovation, boost efficiency, and ignite productivity.



Bad actors have also embraced the tech, using it to develop, scale, and launch increasingly sophisticated attacks. The topic of security and how it relates to AI is inextricable from any conversation regarding this fast-moving technology.

In the age of AI, driving a business forward requires balancing three very significant considerations: growth through innovation, productivity through operational efficiency, and trust through security. While AI has the potential to ignite innovation and optimize operational efficiency, it has also expanded the attack surface.

With so many considerations at play — from AI's promises to its very real risks — we wanted to know how leaders in business are navigating the AI landscape. What are their perceptions of AI, how is AI factoring into their decisions, and do they feel prepared to leverage its capabilities and protect against its risks?

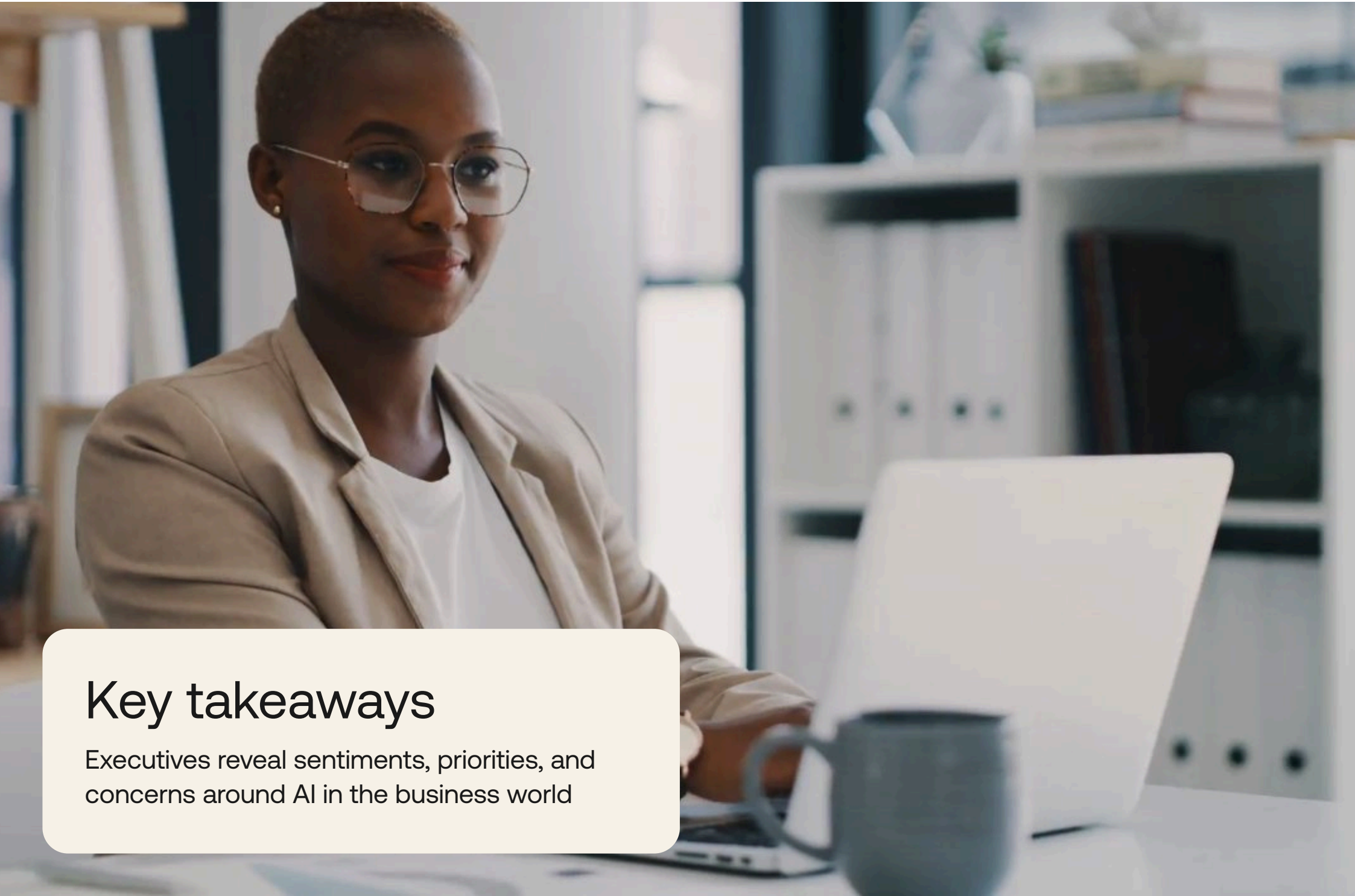
To better understand how AI impacts the intersection of security, innovation, and operational efficiency, we commissioned an AlphaSights survey of 125 executives across three regions, targeting the decision-makers typically tasked with helming those efforts at companies:

- CSOs/CISOs for their focus on security
- CTOs for their focus on innovation
- CIOs for their focus on operational efficiency

Responses from these executives offer insights into where companies across sizes, industries, and regions find themselves in today's AI landscape and where they aim to be in the future.

Who we surveyed: **Learn more about our respondents.**

okta
The World's Identity Company



Key takeaways

Executives reveal sentiments, priorities, and concerns around AI in the business world

KEY TAKEAWAYS

The executive perspective on AI

The outlook is positive

More than half of executives (58%) view AI as a **positive** force in the world, with nearly one-third (31%) characterizing their outlook on AI's impact as **very positive**.

Security colors everything

Security isn't just a top strategic priority; it's also the focus of executives' near-future plans. **Improving security and threat detection** is the top-prompted AI-related priority for leaders in the next 12 months.

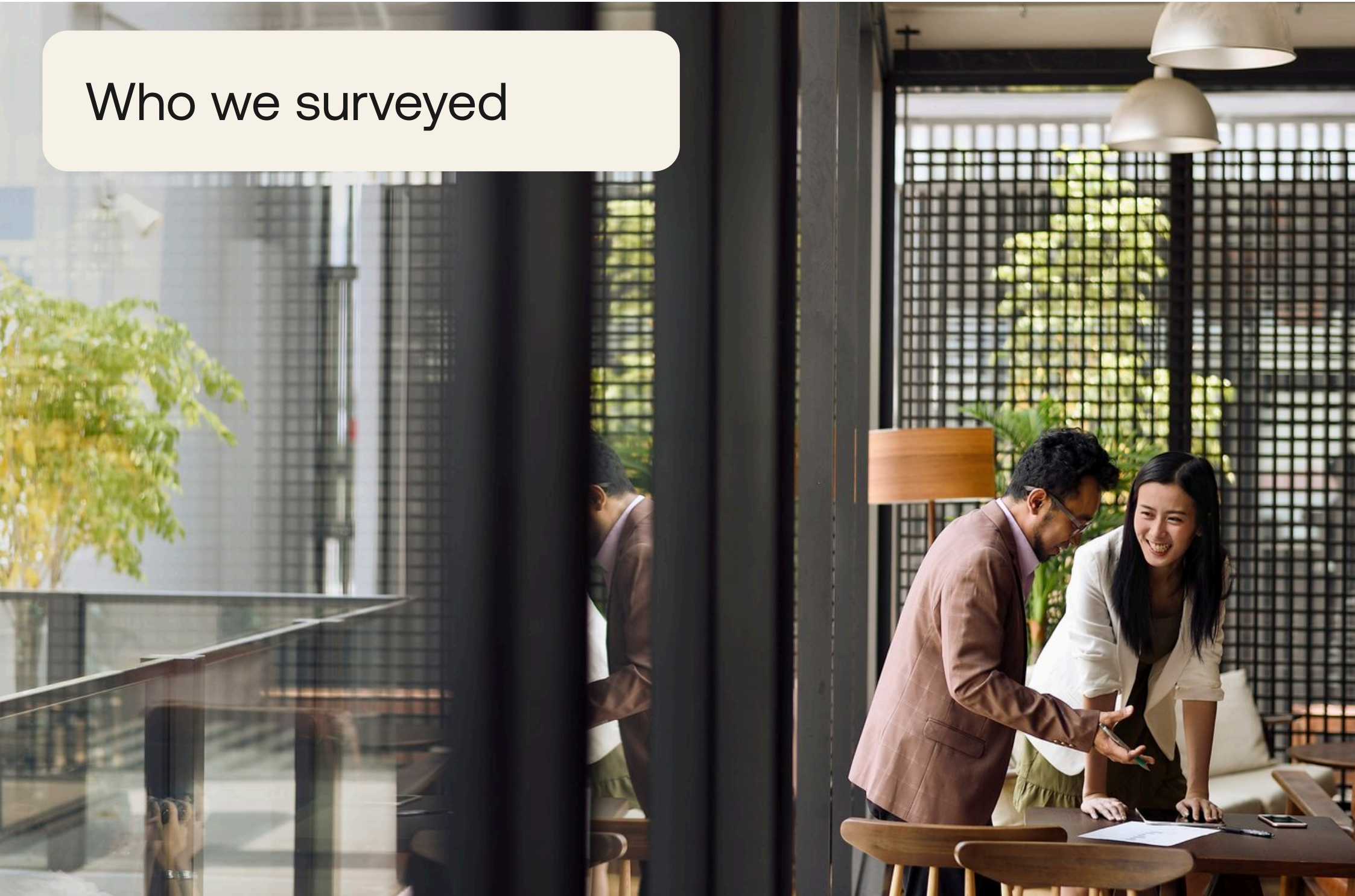
Data privacy is a concern

Respondents say **data privacy**, followed by **security risks**, are top AI concerns.

Identity is more important than ever

79% of executives view Identity and Access Management (IAM) as either **important** (33%) or **very important** (46%) when bringing AI capabilities to their organization.

Who we surveyed



WHO WE SURVEYED

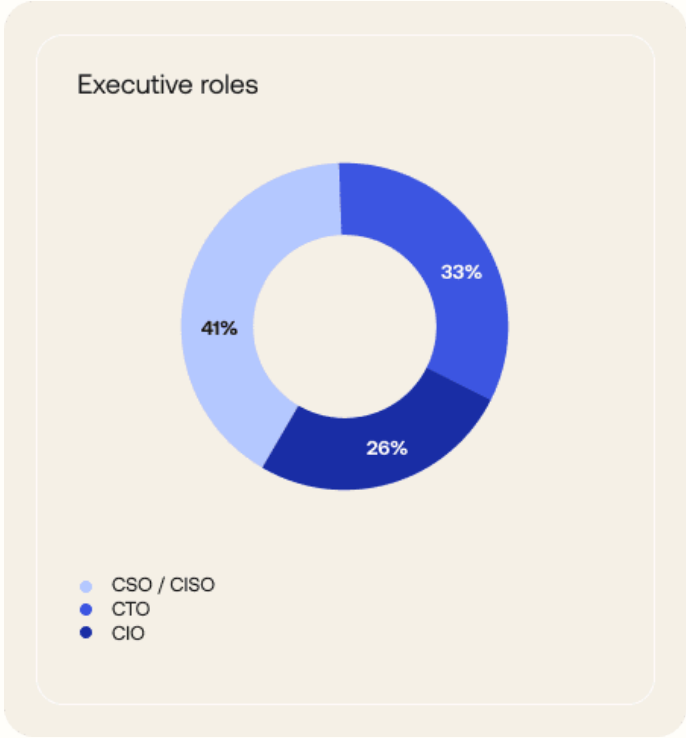
Demographics and strategic priorities

With a company's success closely tied to its ability to spark innovation, expand security, and drive efficiency, we focused our survey on the three executive roles most closely associated with those initiatives:

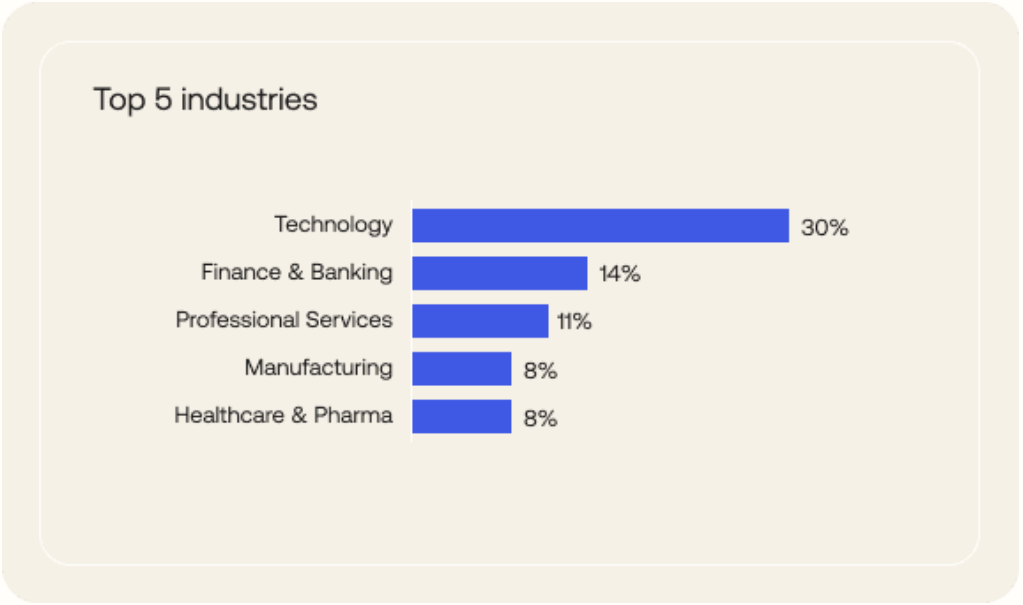
- CSOs/CISOs (security)
- CTOs (innovation)
- CIOs (operational efficiency)

Here's an overview of who we surveyed and their top strategic priorities.

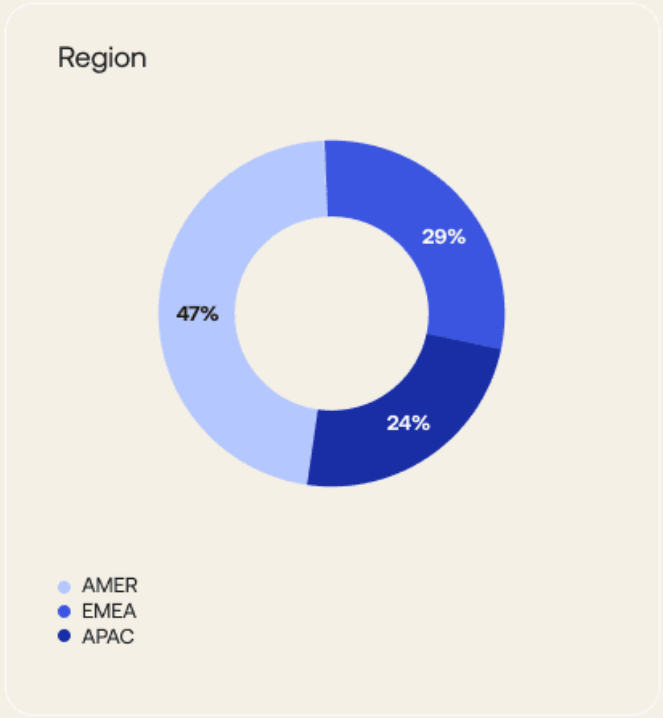
Demographics: Executives span roles, industries, and regions



We surveyed 125 global executives, including 41% with a **CSO** or **CISO** role, 33% with a **CTO** role, and 26% with a **CIO** role.

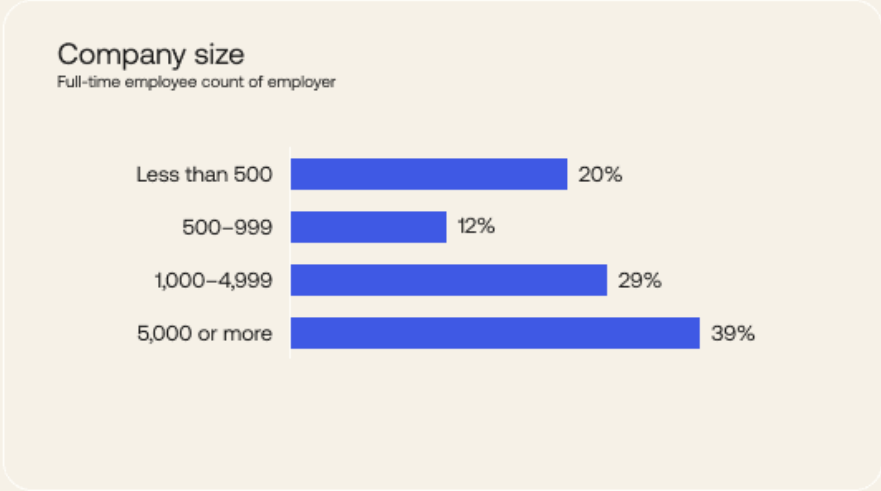


Surveyed executives represent companies in more than 20 industries, led by **technology** (30%), **finance and banking** (14%), and **professional services** (11%).



We sought a global perspective for our survey, focusing on three regions: 47% of respondents work for organizations headquartered in the **Americas (AMER)**; 29% work at businesses headquartered in **Europe, the Middle East, and Africa (EMEA)**; and 24% work at companies headquartered in **Asia-Pacific (APAC)**.

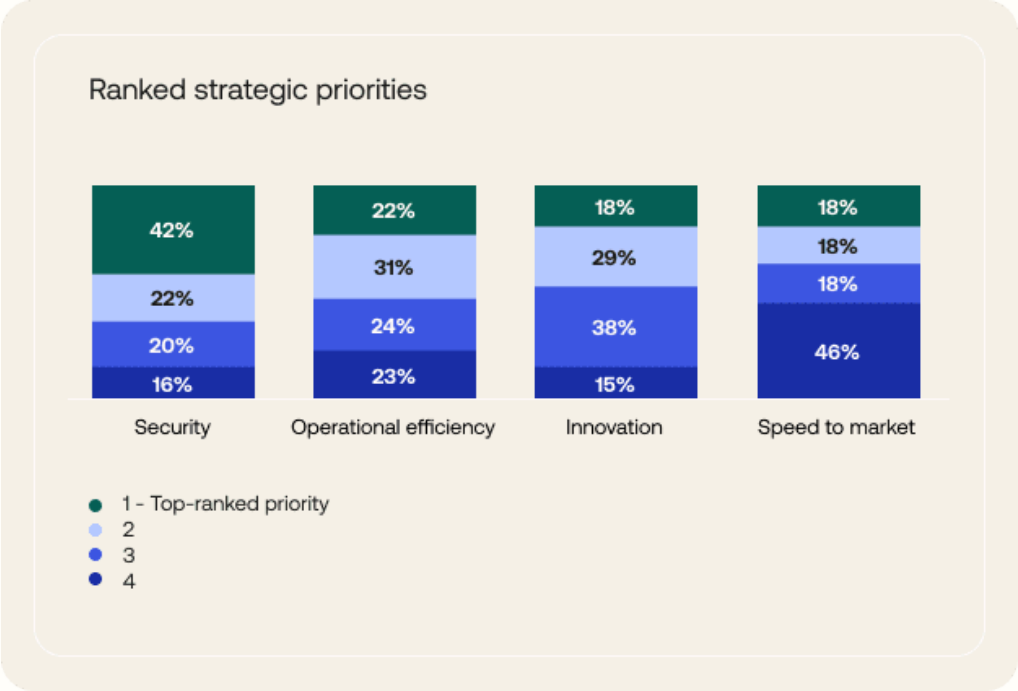
Among the executives, 68% work at companies with **more than 1,000 employees**. The remaining 32% are employed at businesses with **fewer than 999 workers**.



Strategic priorities: Security takes top slot

To understand the executive outlook in the AI era, we focused on the strategic priorities that drive their work. We were curious: Would respondents gravitate toward one strategic priority?

We asked executives to rank, from most to least important, the following strategic priorities: **security**, **operational efficiency**, **innovation**, and **speed to market**.



Across the board, respondents coalesce around **security**. Forty-two percent of all executives surveyed tap **security** as their top strategic priority, followed by **operational efficiency** at 22%.

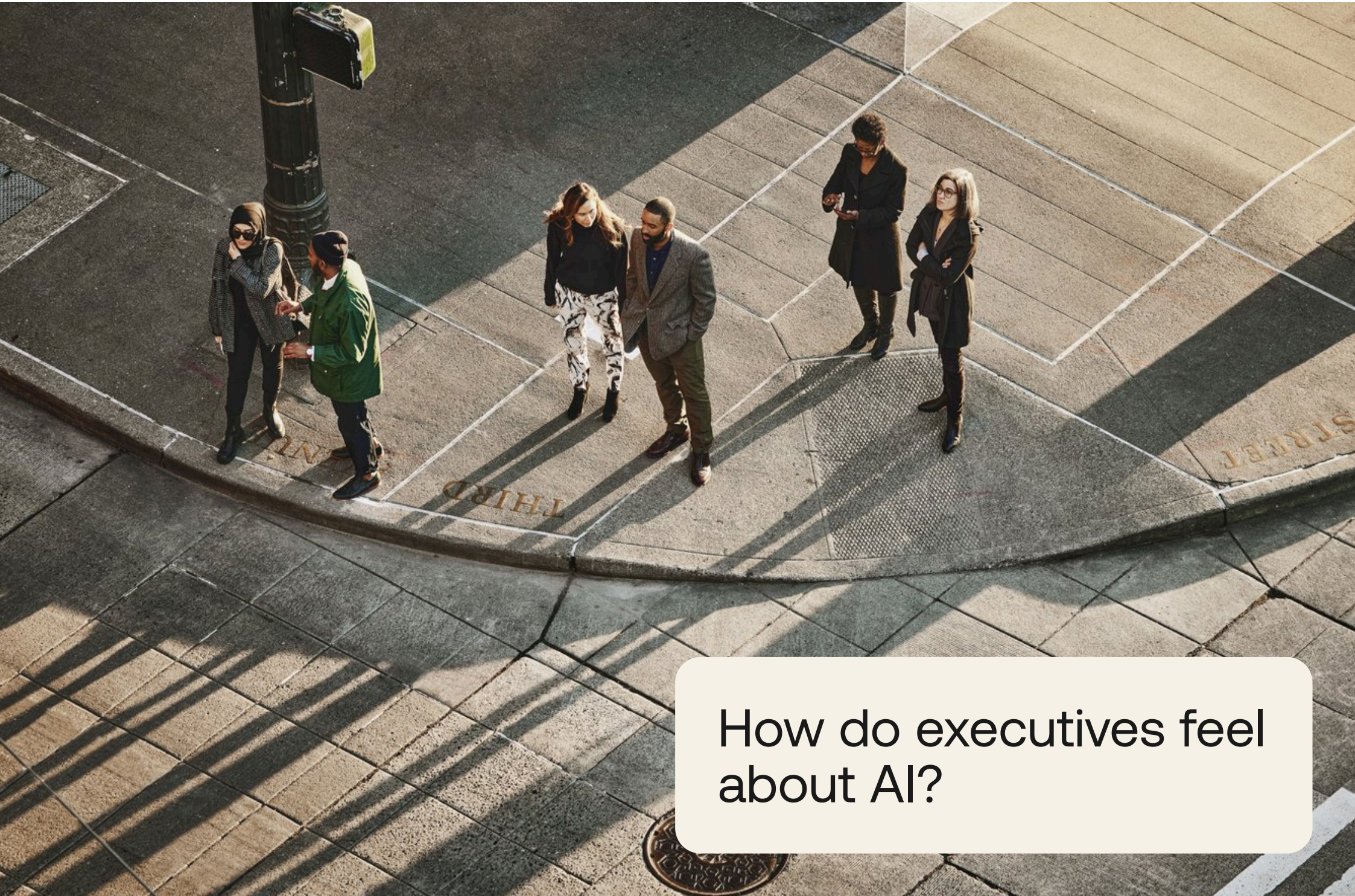
When broken down by role, however, the survey reveals that executive groups show a preference for different strategic priorities: **security** for CSOs/CISOs, **speed to market** for CTOs, and **operational efficiency** for CIOs.

Leaders at larger companies tend to rank **security** as their most important strategic priority. That priority shifts slightly for smaller companies: Executives at businesses with fewer than 500 employees distribute their priorities more evenly among **operational efficiency**, **innovation**, and **speed to market**, with **security** being less of a focus.

Respondents from the technology industry tend to rank **security** as their most important strategic priority, followed by those in finance and banking and professional services.

Security is the top priority for executives in EMEA and AMER, while **innovation** takes the top slot for respondents in APAC.

okta
The World's Identity Company



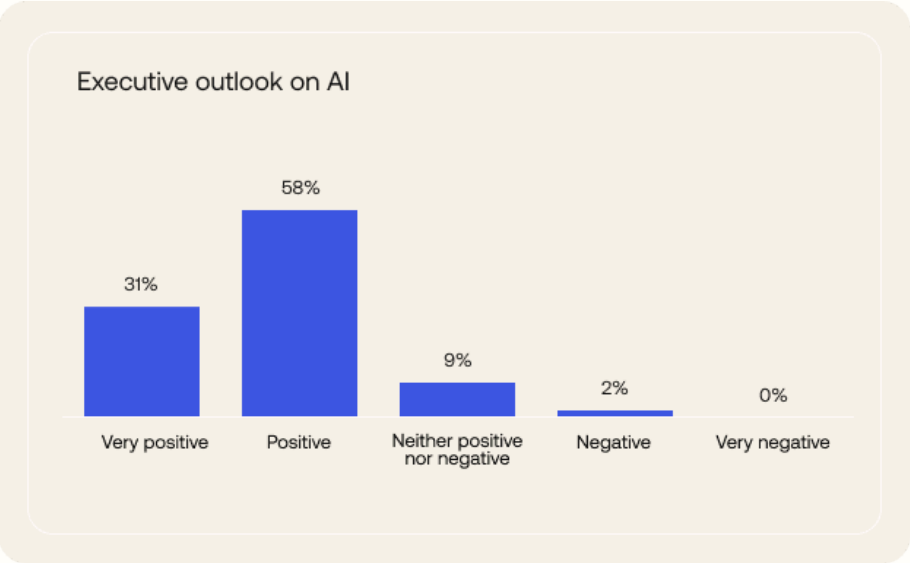
How do executives feel about AI?

EXECUTIVE AI SENTIMENT

The AI present and future looks bright

Despite the very real risks associated with AI, particularly its impact on the threat landscape, executives express optimism about the technology.

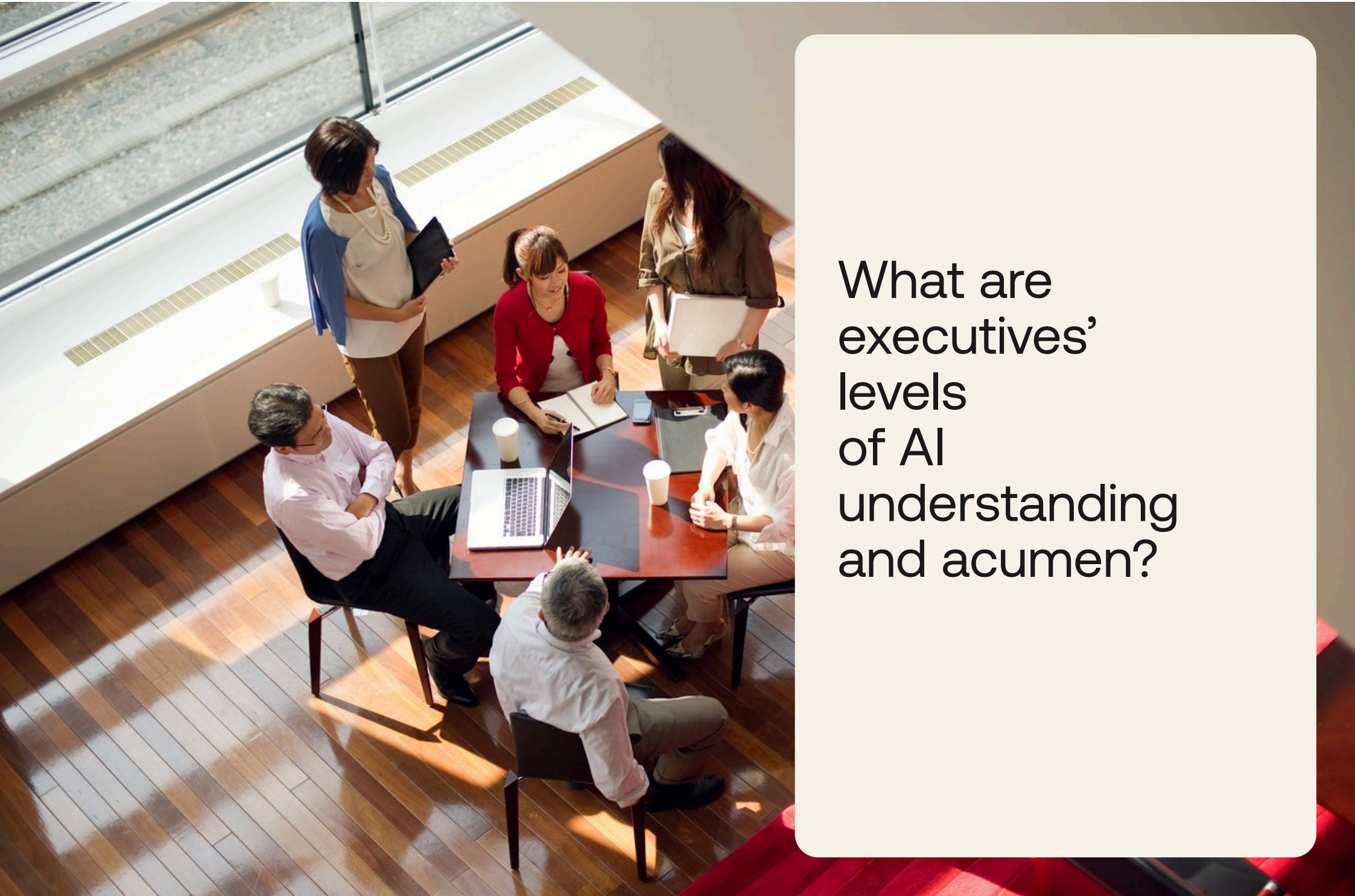
When asked to indicate their outlook on AI on a five-point scale ranging from **very positive** to **very negative**, executives report viewing AI as much more of a positive force in the world than a negative one.



That optimism is most pronounced in EMEA, where 39% of executives say they have a **very positive** outlook on AI's impact on the world. They're followed by 29% of AMER respondents and 27% of APAC executives.

When it comes to AI becoming a bigger part of daily life, 46% of executives say they feel equal parts concern and excitement.

This suggests respondents recognize AI's potential benefits and risks. When combined with the 44% of executives whose excitement outweighs their concern, the data indicates many executives see some benefit from AI's increased prevalence.



What are executives' levels of AI understanding and acumen?

AI UNDERSTANDING AND ACUMEN

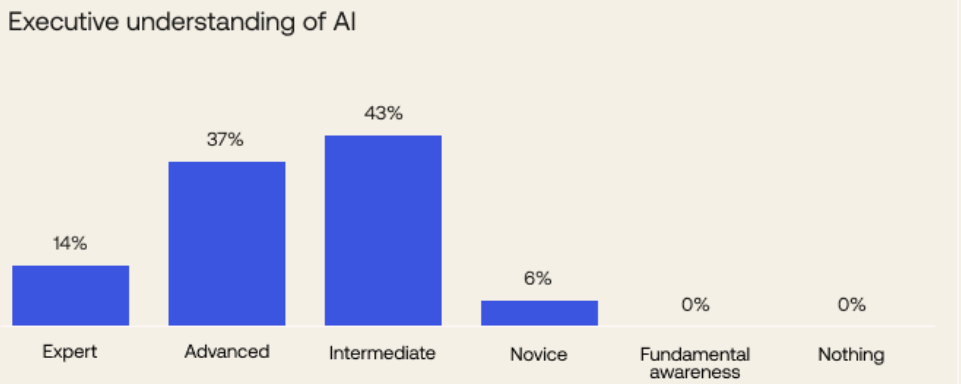
Executives show healthy AI understanding, confidence levels

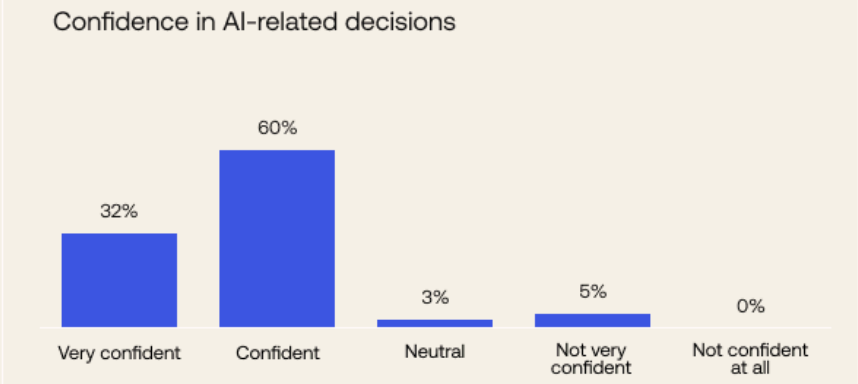
They aren't called "decision-makers" for nothing. Each day, executives are inundated with decisions big and small, with more and more of those calls likely connected to AI.

Knowledge influences decision-making, so establishing respondents' familiarity with AI was key to better understanding their priorities, concerns, and decision-making confidence.

Which statement best describes your level of understanding about artificial intelligence?

- **Expert**: I hold a graduate degree in Computer Science, and I have research experience in AI R&D.
- **Advanced**: I have experience implementing AI models from scratch. I am technically fluent in one or more subdomains of AI, such as Machine Learning, Data Mining, or Reinforcement Learning.
- **Intermediate**: I am familiar with the technical aspects of one or more subdomains of AI. I may have implemented an AI system using API calls.
- **Novice**: I have used AI systems, and I have a non-technical understanding of their functioning, such as what they can do, their biases, safety, or limitations.
- **Fundamental Awareness**: I am aware when a software uses AI, but I am not familiar with any technical or non-technical aspects of it, such as biases, safety, or limitations.

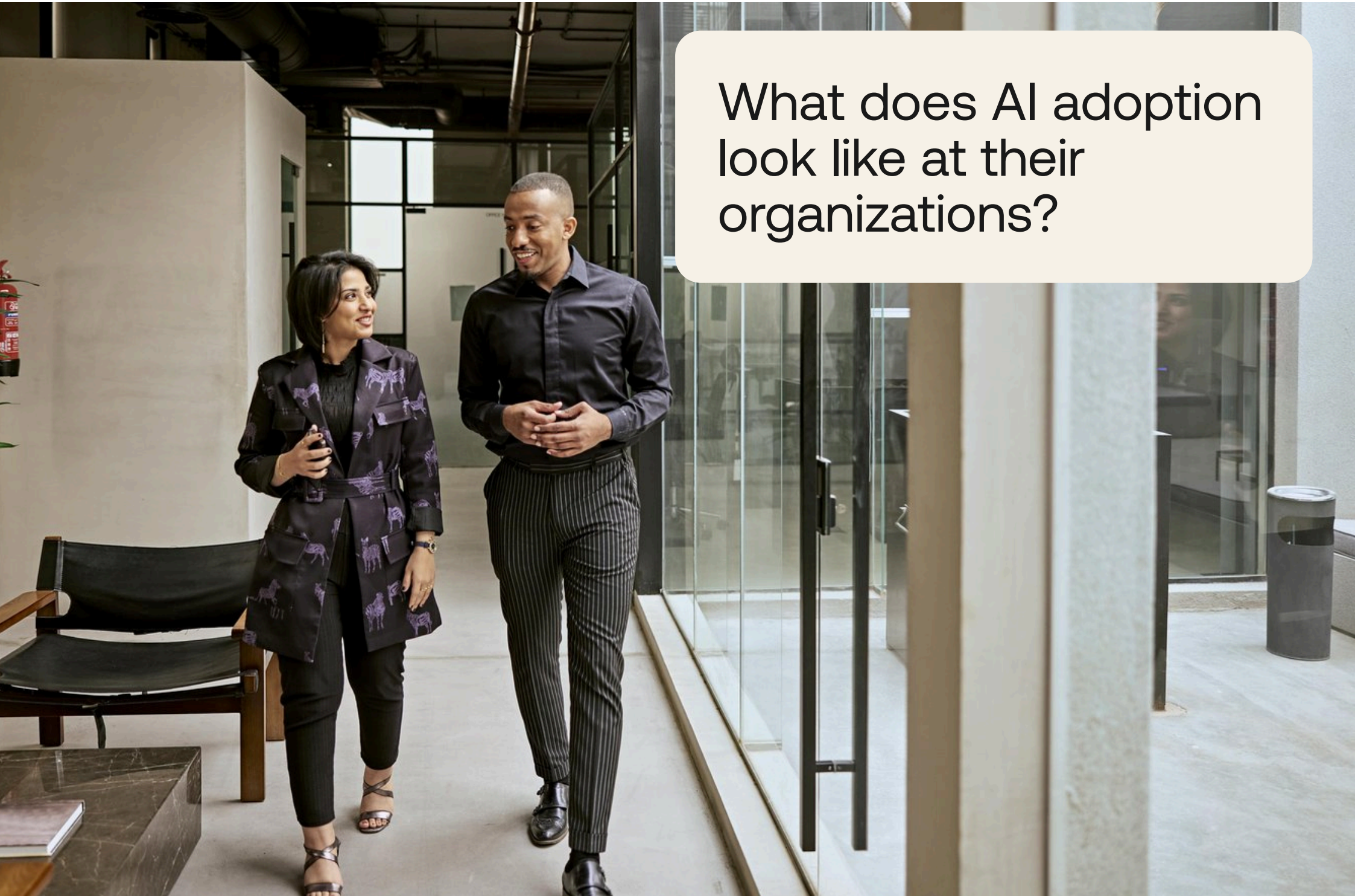




Most respondents (43%) assess their understanding of AI as **intermediate**, and another 37% self-assess as **advanced**. Only 14% of executives report having an **expert** understanding of AI. A small percentage of respondents, 6%, consider themselves AI **novices**.

More CTOs self-assess their level of understanding about AI to be **expert** (22% of their group), followed by CIOs (18% of their group) and CISOs (4% of their group).

When asked about their confidence when making decisions related to AI, 92% of surveyed executives report being **confident** or **very confident**. When broken down by role, nearly half of CTOs (51%) say they are **very confident** in their decisions, followed by CIOs at 27% and CISOs at 20%.



What does AI adoption look like at their organizations?

AI ADOPTION AND INTEGRATION

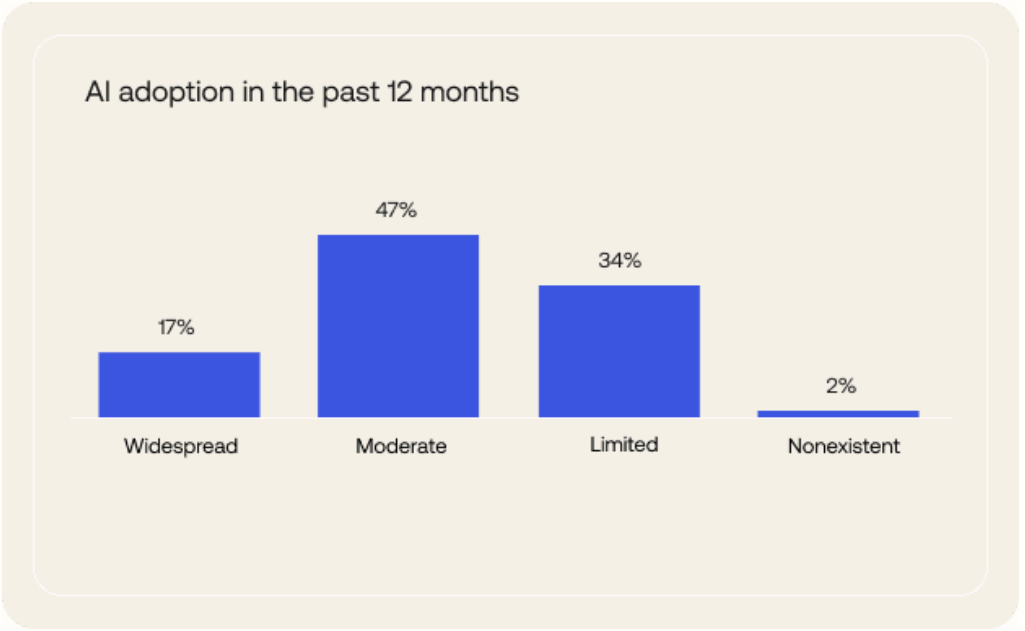
Businesses welcome AI to the team

For many, there are two distinct eras of generative AI: before ChatGPT and after ChatGPT.

Adoption of the tool after its November 2022 release to the public set records. Overnight, it seemed the entire world — or close to it — was using generative AI in one way or another. But how closely does that impression match with reality? We asked executives to walk us through AI adoption in their organizations.

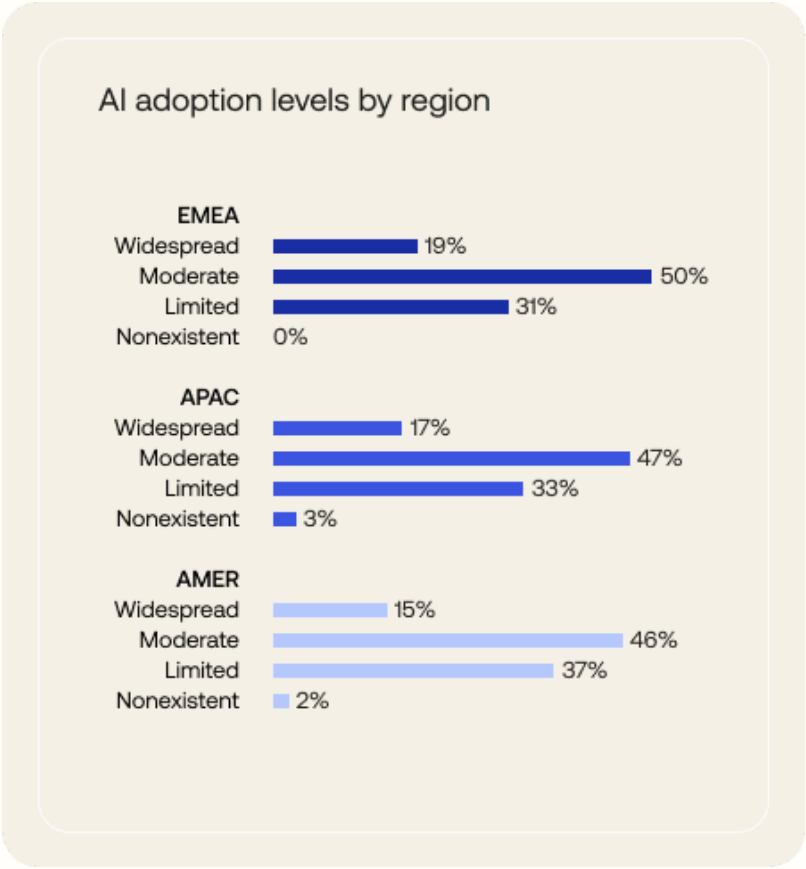
Almost all organizations have had some level of adoption of AI in the past 12 months: 64% of executives say their organizations have seen **moderate** to **widespread** adoption of AI, followed by 34% of executives who say AI adoption is limited. Only 2% of executives describe AI adoption as **nonexistent.**

This level of adoption is happening despite signals of possible friction. Executives rate the ease of integrating AI technology at their organizations as **6.4** on a scale of 0 (not difficult) to 10 (extremely difficult), suggesting the effort is a **moderately difficult** undertaking.



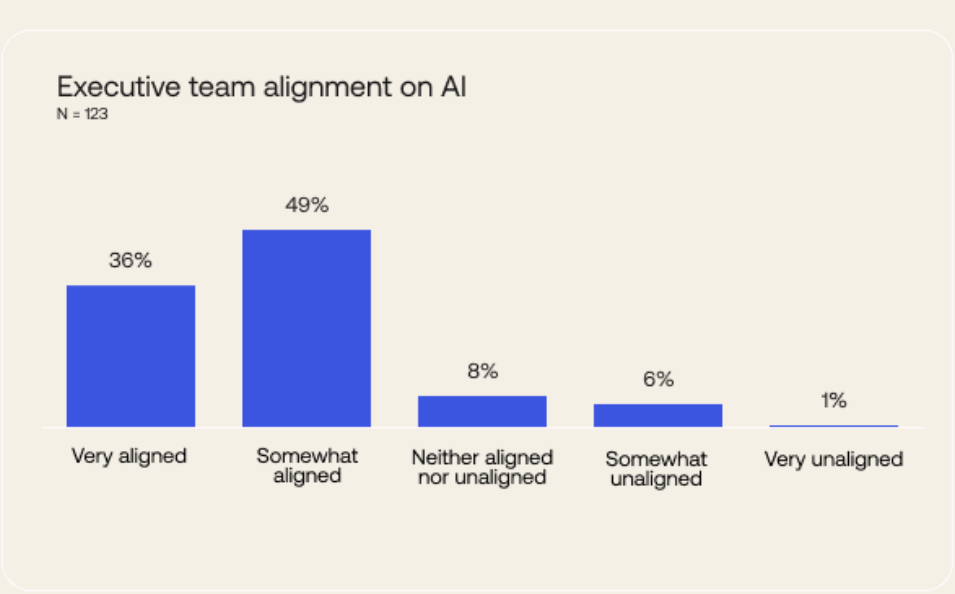
Levels of adoption

Widespread: Nearly all teams use at least some AI.
Moderate: Many teams use AI.
Limited: A few teams use AI.
Nonexistent: No teams use AI.



Executives in EMEA report slightly more **widespread** (19%) and **moderate** (50%) levels of AI adoption when compared with APAC and AMER.

Most executives who see their organizations having moderate to widespread adoption of AI are from the **technology industry**, followed by **finance and banking** and **professional services**.



A strong majority of executive teams, consistently across regions, are either **somewhat** or **very aligned** on AI adoption and integration. The level of alignment among leaders could impact how widespread AI adoption is within an organization.

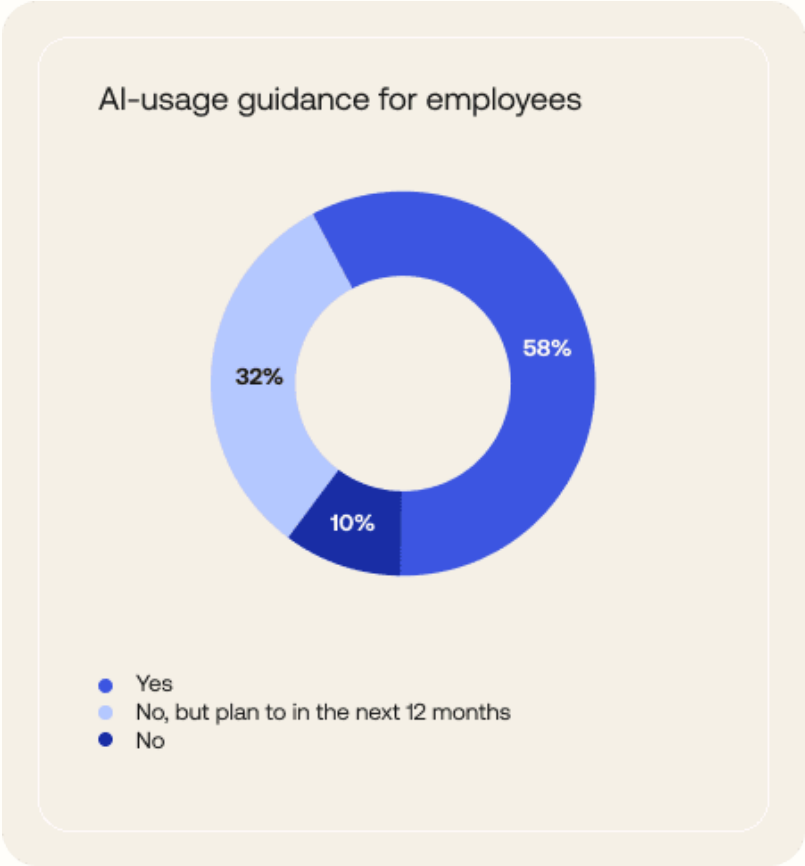
Out of the respondents who report **widespread** AI adoption, 81% characterize their executive teams as **very aligned** on AI. While this data doesn't establish causation, it suggests a shared vision — clearly and effectively communicated from the leadership team to employees — could be a boon to organizations as they seek to bring more AI capabilities into the fold successfully.

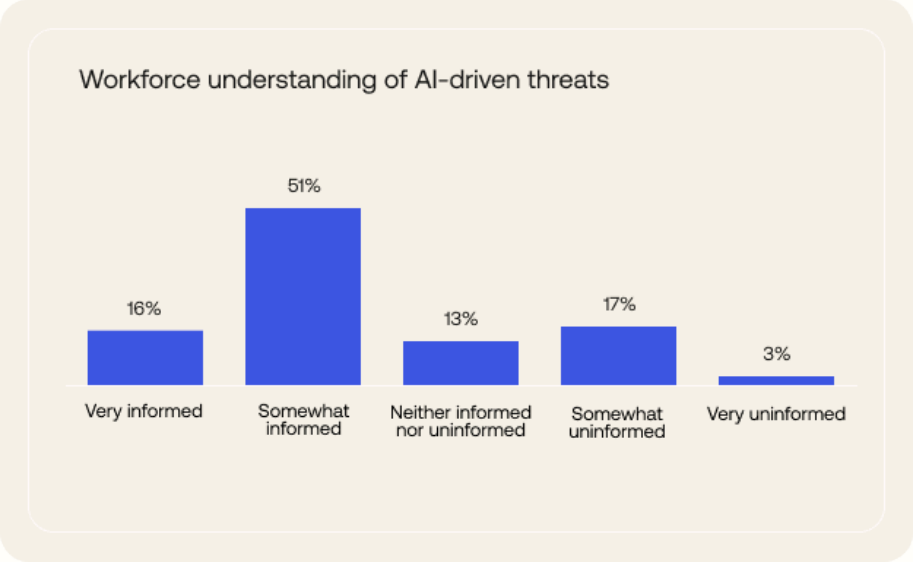
An integral component of AI adoption is creating guidance for employees that establishes and communicates the appropriate use of AI tools.

Fifty-eight percent of executives — led by those in EMEA at 67% — report having **developed guidance** for employees on AI usage. Another 32% say they plan to do so in the next 12 months. The remaining 10% say they have not developed any guidance.

Employee guidance is another area where a unified executive team could make an impact. Respondents with aligned executive teams are more likely to say their companies have created AI-usage guidance for employees.

Even the degree of alignment could have an influence: 77% of respondents who report having a **very aligned** executive team say their organizations have developed guidance, compared with 54% of respondents who characterize their executive team as **somewhat aligned**.





When asked how informed their respective organization's workforce is about AI-driven threats, more than two-thirds of survey respondents (67%) suggest their workforces are either **very informed** or **somewhat informed** about AI-driven threats, with the highest levels seen in EMEA organizations.

Executive takeaways: What it takes to successfully adopt and integrate AI

Respondents shared their views on what elements are critical to an organization successfully adopting and integrating AI.

"A focus on risk identification, mitigation, and management is needed to ensure that **AI adoption works within the boundaries of acceptable risk**. Secondly, a realistic set of expectations and appropriate metrics for measuring progress and performance are needed." (CIO, Healthcare & Pharmaceuticals, APAC)

"Proceeding with caution and level-setting expectations early on. **New tech can be dangerous if not adopted appropriately**, and company secrets, drift, and hallucinations need to be high on the list of concerns." (CSO/CISO, Technology, AMER)

"Having a deep understanding of the SWOT matrix for the AI applications in the target segment is key. You need to know what you are getting into and **weigh the risk-versus-reward ratio**." (CTO, Energy, Mining, Oil & Gas, APAC)

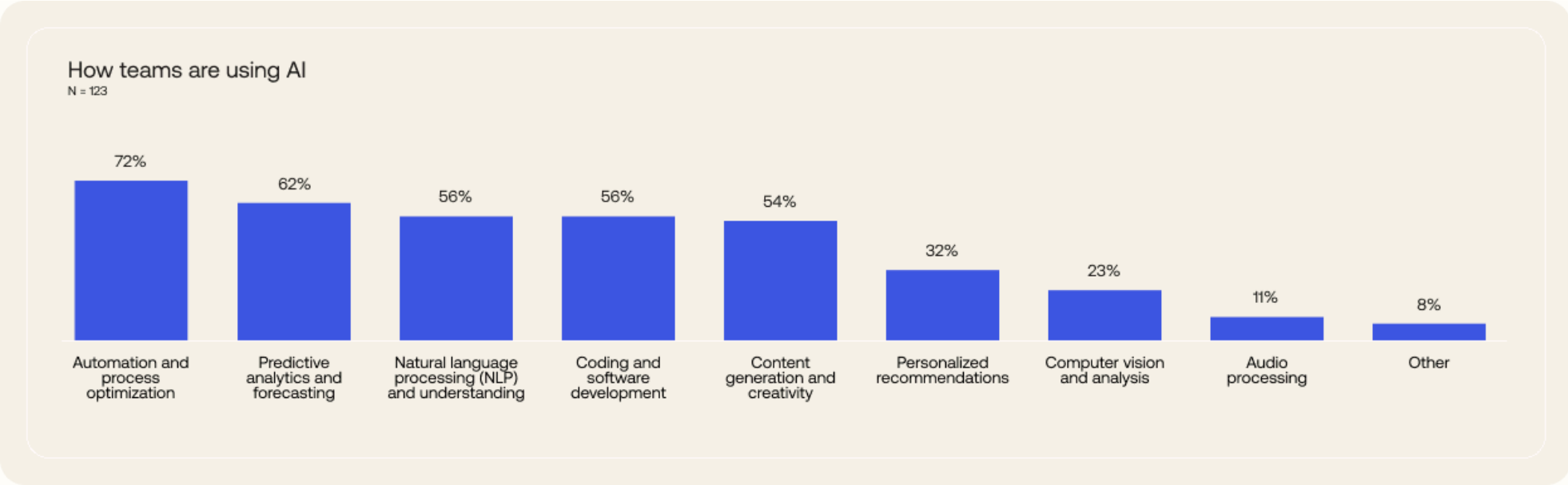
AI adoption, a closer look

As the AI landscape evolves, so does organizations' use of the technology, from bolstering security measures to enhancing customer experiences. We asked executives about the extent to which AI is being used (if at all) for security purposes, in customer-facing products, and by internal teams.

Across the business

AI is being used to some degree for security purposes at 71% of surveyed executives' companies, with more than half (59%) of executives characterizing the use as **moderate, with specific projects or initiatives**.

AI is also making its way into customer-facing products, services, and features: 85% of respondents say they use AI in consumer-facing offerings. Of that group, 72% of executives report **moderate** (58%) or **extensive** (14%) integration.



At the workforce level

When asked how their teams are currently using AI, executives report the most common use case is **automation and process optimization** (72%), followed by **predictive analytics and forecasting** (62%).

In EMEA and APAC, the top AI use case is **automation and process optimization**. In AMER, it's **natural language processing (NLP) and understanding**.

Overall, CIOs report fewer unique use cases at their organizations than CTOs and CISOs, notably focusing their efforts on **coding and software development**, **personalized recommendations**, and **computer vision and analysis**.

How do executives' companies stack up against the competition?

AI AND THE COMPETITION

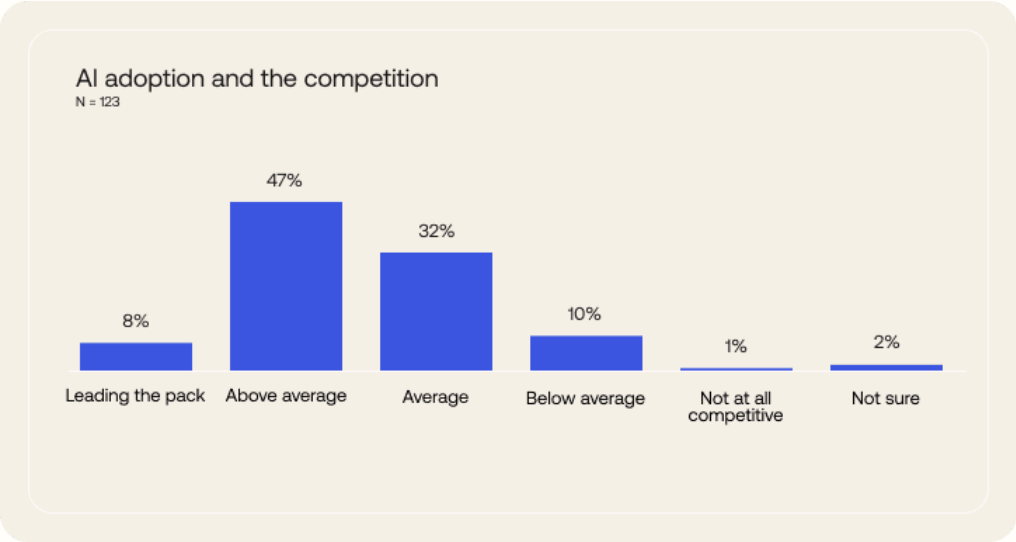
Peer perspective: Comparing AI adoption strengths and weakness

“Know the competition” is a basic business tenet.

After digging into their companies’ approaches to AI, executives shifted their focus to comparing their strategies with those of industry competitors.

More than half of survey respondents (55%) believe they're **ahead of competitors** in their ability to adopt AI technology. That sentiment is strongest among those in APAC (62%) and executives who are CTOs (55%) and CISOs (64%).

And what about the 11% of respondents who characterize their companies as **below average** or **not at all competitive**? That group provided insight into why they think their organizations are behind competitors in adopting and leveraging AI. Their most commonly cited reasons were **lack of AI skills** and **insufficient data infrastructure**.



Executive takeaways: Mind the competitive gap

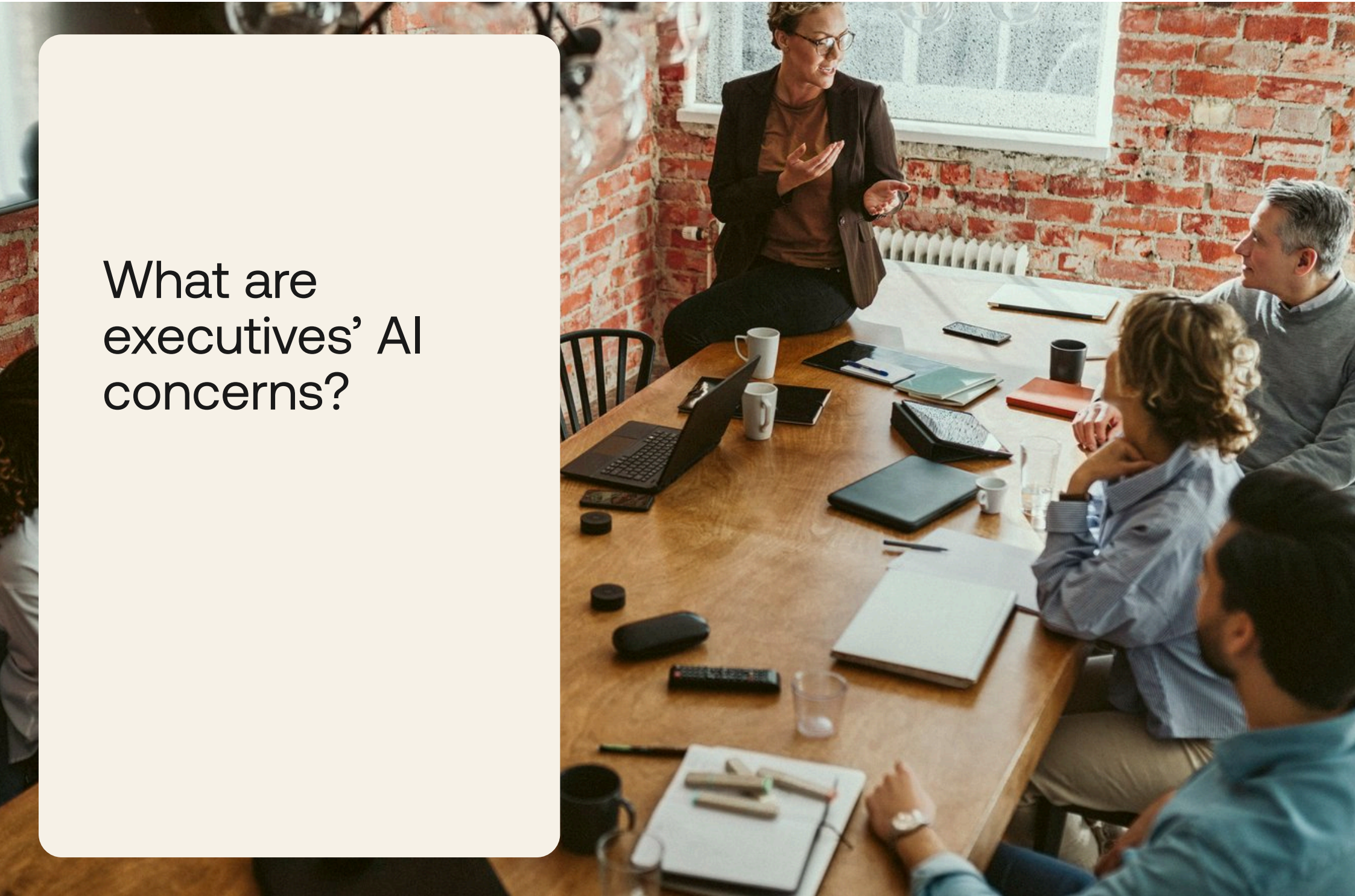
Respondents reflect on why their companies could be falling behind in adopting AI.

“Education [industry] is **slow to adopt and change**. We usually need to see others doing it first.” (CSO / CISO, Education, AMER)

“We're mostly on-prem and running legacy systems. **Integration is a problem**.” (CSO / CISO, Media & Communications, EMEA)

“We are a large organization in healthcare with a very visible parent company. Our ability to move fast and innovate is heavily limited by reputation, cost, and impact. We **cannot move as fast or adapt as quickly as our competitors**.” (CTO, Healthcare & Pharmaceuticals, APAC)

What are executives' AI concerns?



AI CONCERNS

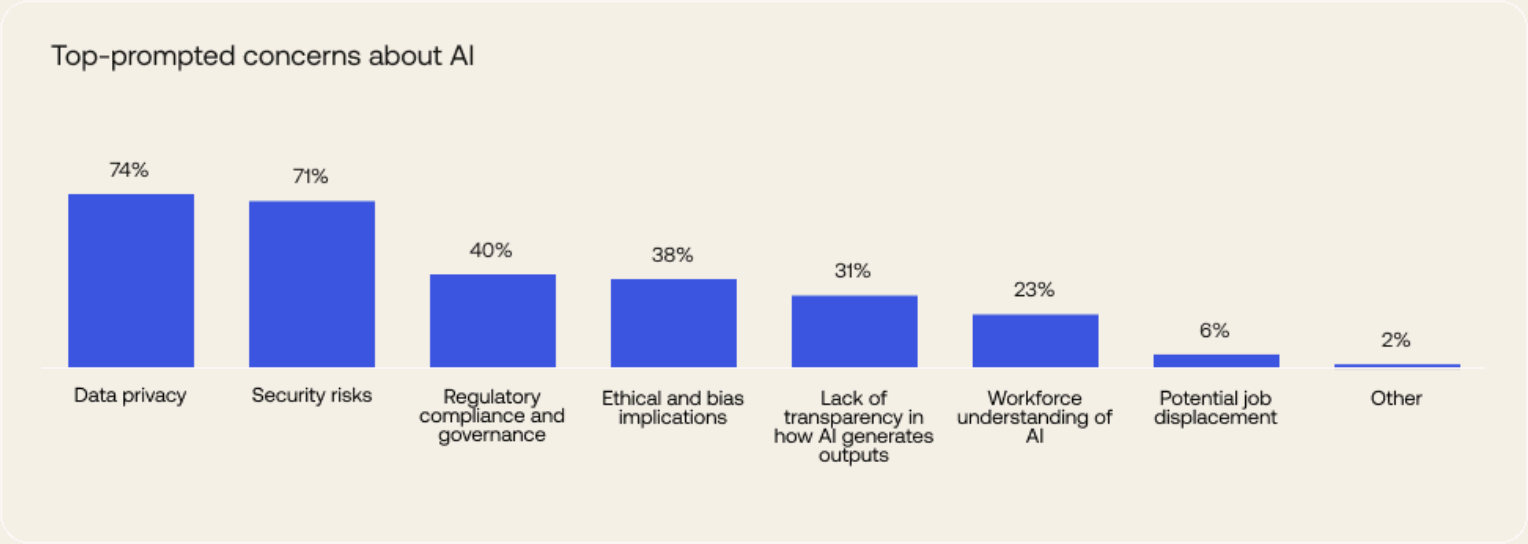
Assessing executive worries and company readiness

“AI will almost certainly increase the volume and heighten the impact of cyber attacks over the next two years,” according to a report published by the UK’s National Cyber Security Centre in January 2024.

As the world braces for a surge in AI-assisted attacks, business leaders must anticipate and then avoid risks. We wanted to know more about their primary security-related AI concerns and how prepared they are to guard against attacks.

Executives selected **data privacy** (74%) as their top prompted concern, followed closely by **security risks** (71%).

These concerns are generally consistent across roles, with a few exceptions: **CISOs** are more concerned about **regulatory compliance,** and **CIOs** are more concerned about **the workforce's understanding of AI**. Although respondents united around two primary worries, they report mixed levels of concern about AI's impact on security at their organizations: 34% say they're **slightly concerned**, 28% suggest they're **moderately concerned**, and 11% report they're **extremely concerned**. Only 3% report being **not at all concerned**, meaning that for the majority of executives, concern is a constant, regardless of how acutely it's felt.



So, how ready are companies to defend against AI-fueled security threats when they come knocking?

More than half (54%) of the surveyed executives say their organizations are **somewhat prepared** to defend against AI-driven attacks. Seventeen percent of respondents characterize their organizations as either **somewhat unprepared** or **very unprepared**.

EMEA has a slight lead in perceived preparedness, with 67% of respondents from that region saying their companies are **very prepared** or **somewhat prepared** to defend against AI-driven threats. For perspective, 50% of APAC executives and 58% of AMER respondents describe their companies as **very prepared** or **somewhat prepared**.

Executive takeaways: What worries them about AI

Executives shared what concerns them the most regarding AI's impact on security. Although the list was expansive, one specific worry took the lead: ***Generative AI tools are helping make phishing attacks more effective****. Here are some more of their reflections:*

"**People are always your biggest threat in security**. AI is becoming more and more lifelike as time progresses, and hackers are becoming faster, adaptable, and innovative. Without educating our internal team sufficiently on the threats of AI, I believe we are opening ourselves up to greater risk of a human-enabled security threat." (CTO, Healthcare & Pharmaceuticals, APAC)

"Rogue actors using AI to **gain access to protected data**." (CIO, Finance & Banking, AMER)

"As always, **it's the unknown**: How are threat actors deviously planning to leverage AI against us? It is a very powerful tool for good as well as for bad." (CSO / CISO, Technology, AMER)

What are executives' AI-related priorities over the next year?

AI PRIORITIES

Safeguarding their business' future

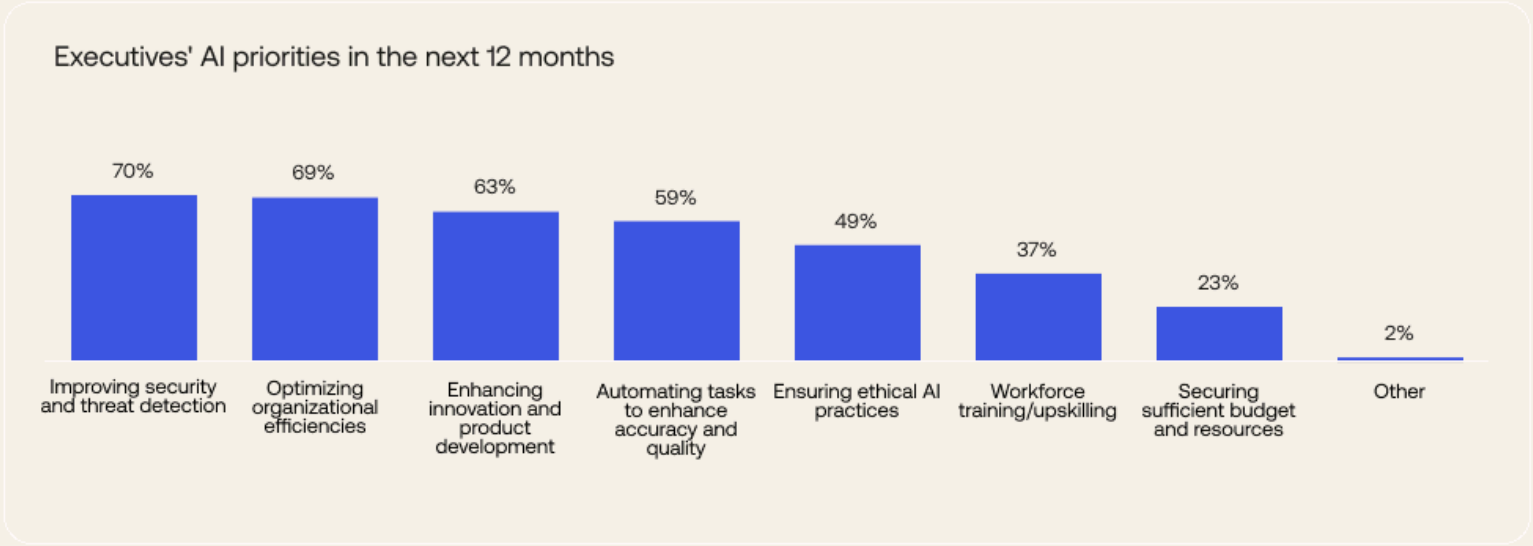
AI outlook, concerns — and now priorities. Executives offered insight into what they are focusing on in the near term. With rapid developments in both the technology and its application, respondents focused on the 12-month window following their taking the survey.

Executives forecast AI will impact all the prompted core strategic priorities — **innovation**, **security**, **speed to market**, and **operational efficiency** — with relatively similar magnitude, indicating the continued pervasiveness of the technology across the business world.

Looking ahead to the next 12 months, respondents selected **improving security and threat detection** as a top priority for AI, followed closely by **optimizing organizational efficiencies**.

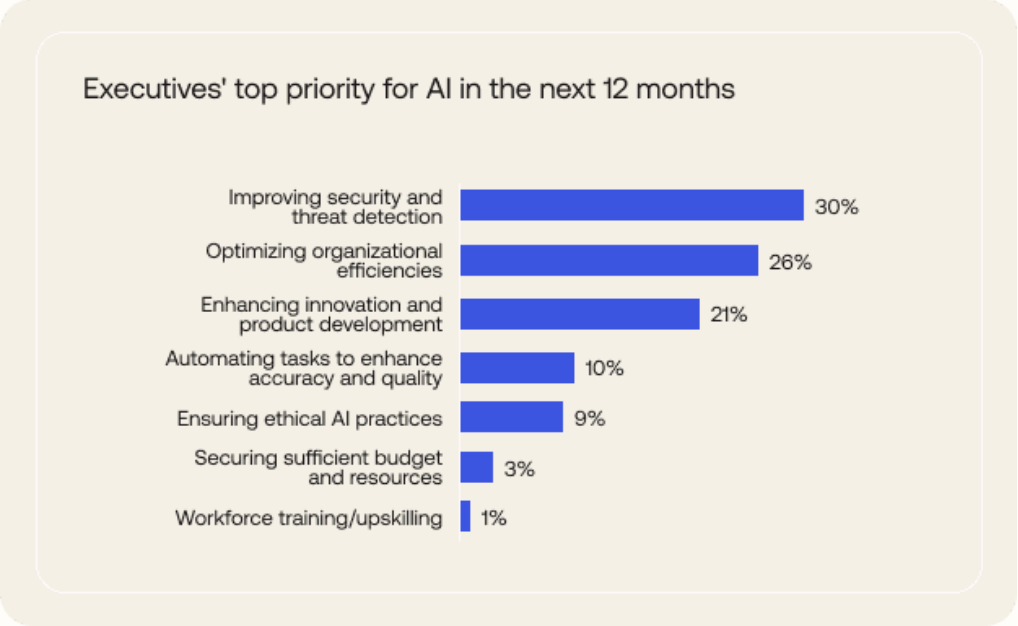
Improving security and threat detection is the top-prompted AI priority in APAC and the Americas. **Optimizing organizational efficiency** is the top-prompted AI priority in EMEA.

CISOs' priorities largely involve **improving security and threat detection,** whereas CIOs are most focused on **optimizing organizational efficiencies**. Meanwhile, CTOs show a preference for **enhancing innovation and product development**.



When we asked executives to identify their top priority for AI in the next 12 months among prompted alternatives, **improving security and threat detection** was the most common, selected by 30%, followed by **optimizing organizational efficiencies** (26%) and **enhancing innovation and product development** (21%).

Resource-wise, executives appear to feel supported in these efforts: 59% of respondents are either **satisfied** or **very satisfied** with their organization's current level of investment in their top priority.



okta
The World's Identity Company

The Identity connection

IAM AND AI

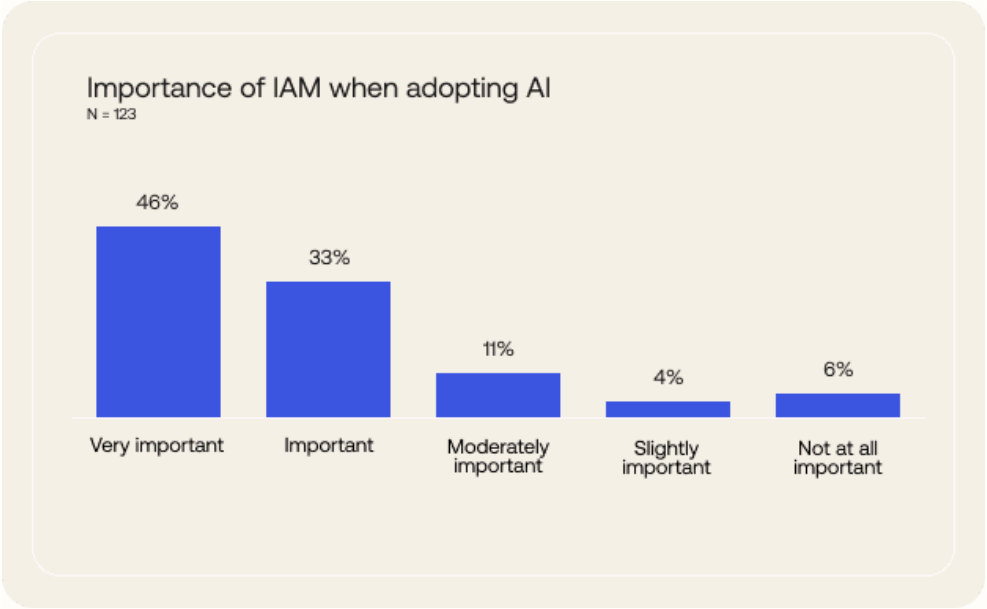
The importance of Identity in the AI era

As AI adoption increases globally, Identity is key to helping businesses embrace the technology's undeniable power without sacrificing security.

We asked executives to rate how important **Identity and Access Management (IAM)** — ensuring the right people have access to the right resources at the right times — is to adopting and integrating AI at organizations.

More than three-quarters (79%) of executives suggest IAM is **important** or **very important** when adopting and integrating AI. The **very important** cohort is led by those in APAC and in a CIO role.

When responding to an open-ended question regarding the importance of IAM in AI adoption, the most common response related to **ensuring only authorized users are accessing permitted tools**.



Executive takeaways: IAM in focus

Here's what respondents had to say about the role IAM plays in AI adoption.

"**IAM is a key pillar in security**. It should be at the root of all you do. Managing who has access to the proper data and systems is critical." (CSO / CISO, Education, Americas)

[IAM] is the only technical control we have to manage who has access to this new technology. We are **slowly opening the gates for specific justified needs** — not being afraid of AI but by embracing it slowly and methodically. (CSO / CISO, Technology, Americas

"We need to implement ethical AI, and this comes with the **right level of segregation of duties and authorizations**." (CSO / CISO, Technology, EMEA)

Conclusion and methodology

Conclusion and methodology

Spanning regions, industries, and headcounts, our survey offers a view into how executives are approaching AI and all its dynamic considerations. And while the degree to which businesses have adopted AI varies, one thing is clear: Inaction is not an option.

Conclusion

Leaders must make critical decisions about when, how, and to what degree to use AI — even as the technology itself is rapidly changing. Determining what's next can be difficult, especially considering AI's many unknowns. Based on respondents' answers, here are some paths organizations — regardless of their level of AI maturity — can consider:

Enhance security

Move swiftly and intentionally to strengthen security infrastructure to mitigate AI-related threats and risks.

Foster collaboration

Work with industry peers, regulatory bodies, and internal and external experts to develop and share insights and best practices for responsible AI collaboration.

Expand education

Prioritize educating employees on those best practices while offering them the space for learning and experimentation with generative AI tools.

Methodology

Commissioned by Okta, AlphaSights recruited 125 C-suite executives to take an online double-blinded survey on their sentiments, concerns, and business priorities regarding AI. In total, 51 CSOs/CISOs, 41 CTOs, and 33 CIOs were surveyed. These experts were engaged via an initial phone conversation with AlphaSights associates to determine whether or not they had relevant experience; those with applicable experience received the survey. AlphaSights fielded the survey in January 2024, recruited the panel, and put together an initial analysis of the key findings. An Okta team of marketers and data analysts delved into the results to produce the full report.

About Okta

Okta is The World's Identity Company. As the leading independent Identity partner, we free everyone to safely use any technology—anywhere, on any device or app. The most trusted brands trust Okta to enable secure access, authentication, and automation. With flexibility and neutrality at core of our Okta Workforce Identity and Customer Identity Clouds, business leaders and developers can focus on innovation and accelerate digital transformation, thanks to customizable solutions and more than 7,000 pre-built integrations. We're building a world where Identity belongs to you. Learn more at okta.com.