DARKTRACE

The State of AI Cybersecurity

2025 Report

Global perspectives on the growing role of AI in cybersecurity

Contents

Executive Summary

As a field, cybersecurity has always been fast-changing and intricately complex. This constant shape-shifting is what keeps things interesting for practitioners, who are consistently being challenged to learn something new. Over the last couple of years, however this already rapid pace of transformation has accelerated even further, with groundbreaking advancements in Artificial Intelligence (AI) rewriting the terms of contest between attackers and defenders. Today's security leaders must build strategies to stay ahead of the curve so that defenses can evolve along with the sophistication of attacks.

Harnessing the Power of AI in Cybersecurity: The Time Is Now

We recently surveyed over 1,500 cybersecurity and IT professionals around the world to understand their attitudes about AI in cybersecurity. We asked how AI is impacting the threats they face, how they are responding, and what role they see AI playing in present-day and future prevention, threat detection, incident response, and recovery workflows.

This is the second year that we've conducted this research. We found that a growing number of CISOs now agree that the impacts of AI-powered threats on their organizations are significant. A very large majority (89%) believe that these threats will continue to bedevil their organizations well into the future. Hands-on practitioners are especially worried, with SecOps team members expressing higher levels of concern about the long-term impacts of AI than CISOs.

Key Takeaways from our Research

AI cyber threats are a reality, and the time to act is now.

78% of CISOs believe AI is having an impact on cyber threats today and are moving quickly to protect themselves. Cyber professionals feel significantly *more* prepared for AI cyber threats than they did 12 months ago, but **45%** still feel they are not ready for this reality.

Defensive AI is becoming an integral part of the SOC, augmenting understaffed teams.

Despite 'insufficient personnel' being considered the greatest inhibitor to defending AI-powered threats, increasing cyber security staff is at the bottom of the priority list for survey participants, with **only 11%** planning to increase cybersecurity staff in 2025—less than in 2024.

CISOs are calling for proactive, platform-based solutions that keep their data in-house.

CISOs have expressed a preference for broader platforms over point products (**89%**) and solutions that don't require their data to be shared externally (**82%**). The vast majority have confidence in AI's ability to help them become more proactive.

Although cybersecurity stakeholders feel better prepared for this new reality than they did last year, nearly half (45%) of those surveyed still lack confidence in the preparedness of their organization to face AI-powered threats. There's strong desire to improve cyber readiness, and a great deal of talk about risk reduction steps like implementing an organization-wide AI security policy. However, more organizations have discussed formal policies for the safe and secure use of AI than have actually implemented them.

AI education is on the rise, and stakeholder understanding of AI (in all its forms) is growing, but there's still a long way to go. More than half (56%) of the participants in this year's survey admitted that they did not know exactly which types of AI were being used in the cybersecurity solutions that their organizations were using. A tendency we observed last year—to overestimate the role that generative AI (gen AI) plays in cyber defense—persists, too.

Education and training will be key for empowering practitioners to maximize the value they gain from AI technologies. But leaders, too, must understand the differences between the various types of AI, how they are applied in cybersecurity solutions, and how they can augment human analyst capabilities to empower SecOps teams to achieve more with the same resources.

As organizations embrace these tools, benefiting from their ability to streamline workflows, reduce false positives, and enable the detection of never-before-seen threats, the need for AI education will only become more urgent. Threat actors are racing to take advantage of the transformative potential of AI, and leading SecOps programs are doing the same. Attackers always look for the softest targets. Increasingly, these will be organizations that have not implemented effective AI-driven solutions that help enhance visibility, reduce complexity, and boost productivity. We hope that this research will cast light on these growing risks to help organizations avoid them.

In the report that follows, you will learn more about our findings. We'll also share some recommendations for addressing today's top challenges.

88%

of security teams are already experiencing significant time savings through the use of AI.

84%

of survey participants prefer AI solutions that do not require their data be shared externally for model training or other purposes.

95%

of those surveyed believe AI can improve the speed and efficiency of cyber defense.

88%

of respondents agree that the use of AI within the security stack is critical for freeing up time so that security teams can be more proactive.

63%

of participants believe their cybersecurity tools use only or mostly gen AI, though this isn't likely the case.

The AI Revolution Is Underway

Enterprise AI adoption has progressed since the start of 2024, but breach numbers and losses to cybercrime have not declined in tandem. This suggests that attackers are adopting AI at least as quickly as defenders.

With the cybersecurity industry rushing to integrate AI into workflows across prevention, detection, response, and recovery, technologies are evolving much more quickly than skillsets. Hiring enough new talent to solve perennial problems in security operations, such as burnout, short job tenures, and excessive turnover, is all but impossible in the current climate.

The good news is that there's growing awareness among stakeholders that AI, when applied in the right places, can help organizations overcome these challenges. There's also greater awareness that the time to take these steps is now, before threat actors significantly advance their ability to make use of this technology.

Already there are signs that a shift is taking place. Since the release of ChatGPT a little over two years ago, threat researchers have seen more novel social engineering campaigns. Analysis of malicious emails reveals that these threats are becoming increasingly capable of circumventing conventional email security tools. They are also becoming much more targeted, evidence that threat actors are leveraging gen AI to create bespoke messages for select organizations or even individuals.[1]

The bad news is that many of the challenges we observed last year continued to persist. Rapid adoption of AI-driven technologies is placing new demands upon defenders. Decision-makers need to understand how products and features work so that they can make smart choices about what to implement. Security analysts, incident responders, and architects need to learn how to work with this new technology on a hands-on basis. Yet misunderstandings about AI remain prevalent.

We are heartened to see significant progress among the leaders in AI and cybersecurity maturity, but there remains a gap between these trailblazers and the rest of the pack. Because AI-powered threats are both pressing and rapidly evolving, there's an urgent need for all organizations to keep pace.

[1] Darktrace, First 6: Half-Year Threat Report 2024, Available at: https://cdn.prod.website-files.com/626ff4d25aca2edf4325ff97/66b11449115ff7537adb646b_First6_Half_Year_Threat_Report_2024-compressed.pdf

Ongoing Evolution: The Impact of AI on the Cyber Threat Landscape

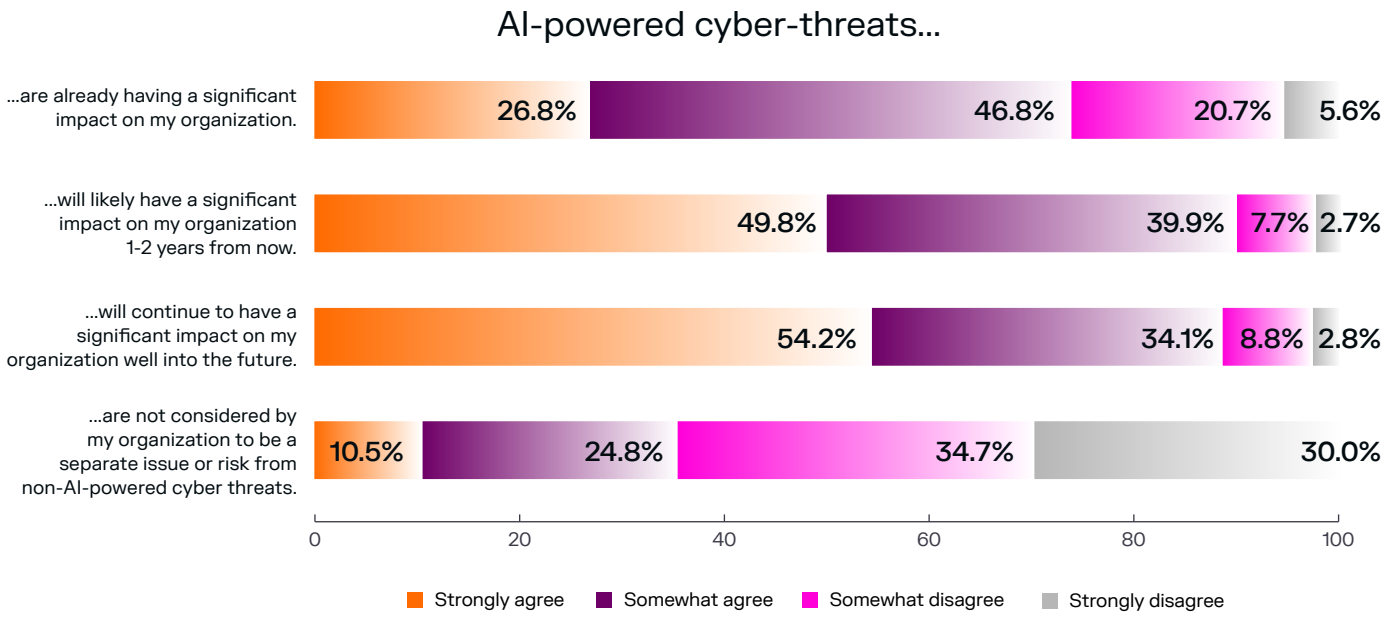
There's an expanding body of evidence that AI is being harnessed more and more effectively by threat actors.[2] Our threat researchers, for instance, observed a 135% increase in novel social engineering attacks targeting Darktrace / EMAIL customers over the course of 2023, the same period when ChatGPT saw popular adoption.[3]

The areas where there is greatest concern about the malicious use of AI include:

Novel social engineering attacks powered by AI are harder to detect and more readily bypass traditional defenses.

More advanced attacks at speed and scale delivered by less capable threat actors due to easy access to AI.

Attacks targeting AI systems by attackers who are going after machine learning models, training data, and the APIs and interfaces through which they are accessed.



Participants are aware of the major impact that AI is having on the threat landscape. Nearly three-quarters (74%) agree that AI-powered threats now pose a significant challenge for their organization. Nine in ten (90%) of survey participants agree that AI-powered threats will continue to have a significant impact on their organization for the next one to two years, slightly more than last year.

[2] Ibid.
[3] Darktrace, Generative AI: Impact on Email Cyber Attacks, Available at: https://darktrace.com/resources/generative-ai-impact-on-email-cyber-attacks

Industries impacted by AI-powered cyber threats:

most

Retail

80% are already seeing a significant impact from AI.

Technology

79% are already seeing a significant impact from AI.

Manufacturing

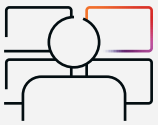
74% are already seeing a significant impact from AI.

Government

54% are already seeing a significant impact from AI.

least

% agreeing that AI-powered threats are having an impact today, by job role:



65%

SecOps practitioners

vs.

78%

CIOs or CISOs

% agreeing that AI-powered threats will continue to have an impact in the long term:

90%

SecOps practitioners

vs.

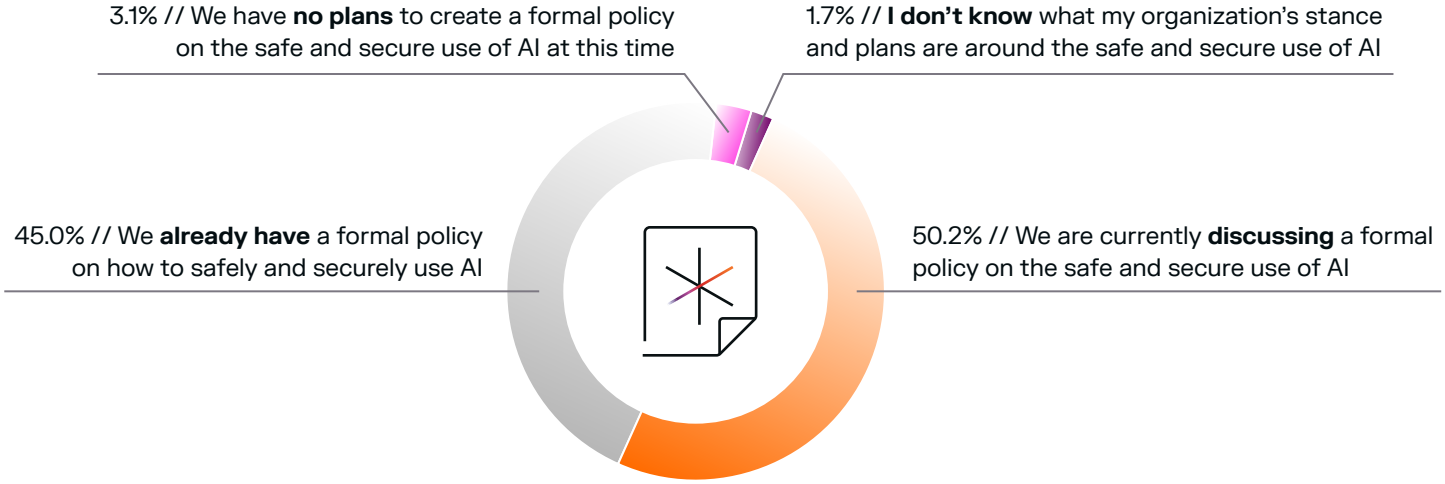
88%

CIOs or CISOs

A majority of participants (65%) indicated that their organizations consider AI-powered threats a separate issue from non-AI-powered threats. In a world where it's all but impossible to determine whether or not an attack is AI-powered, and where AI-powered threats will make up a progressively larger portion of the attacks that organizations face, this distinction may ultimately prove less and less meaningful.

Instead, organizations will need to turn their focus elsewhere—to adopting a proactive, risk-based approach to defense, one that can efficiently counter growing numbers of unique threats, arriving at ever-greater speed.

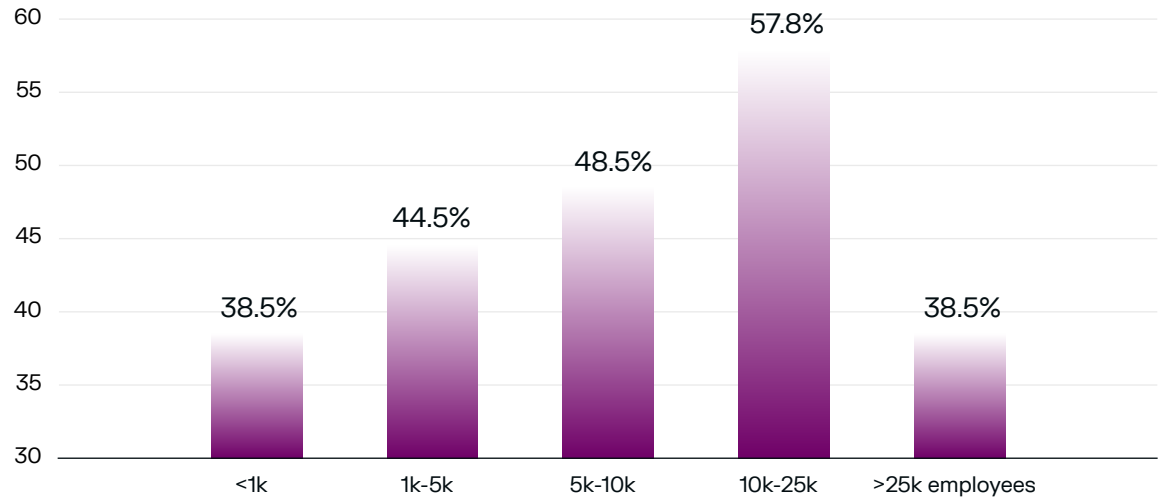
AI security policy: More talk than action



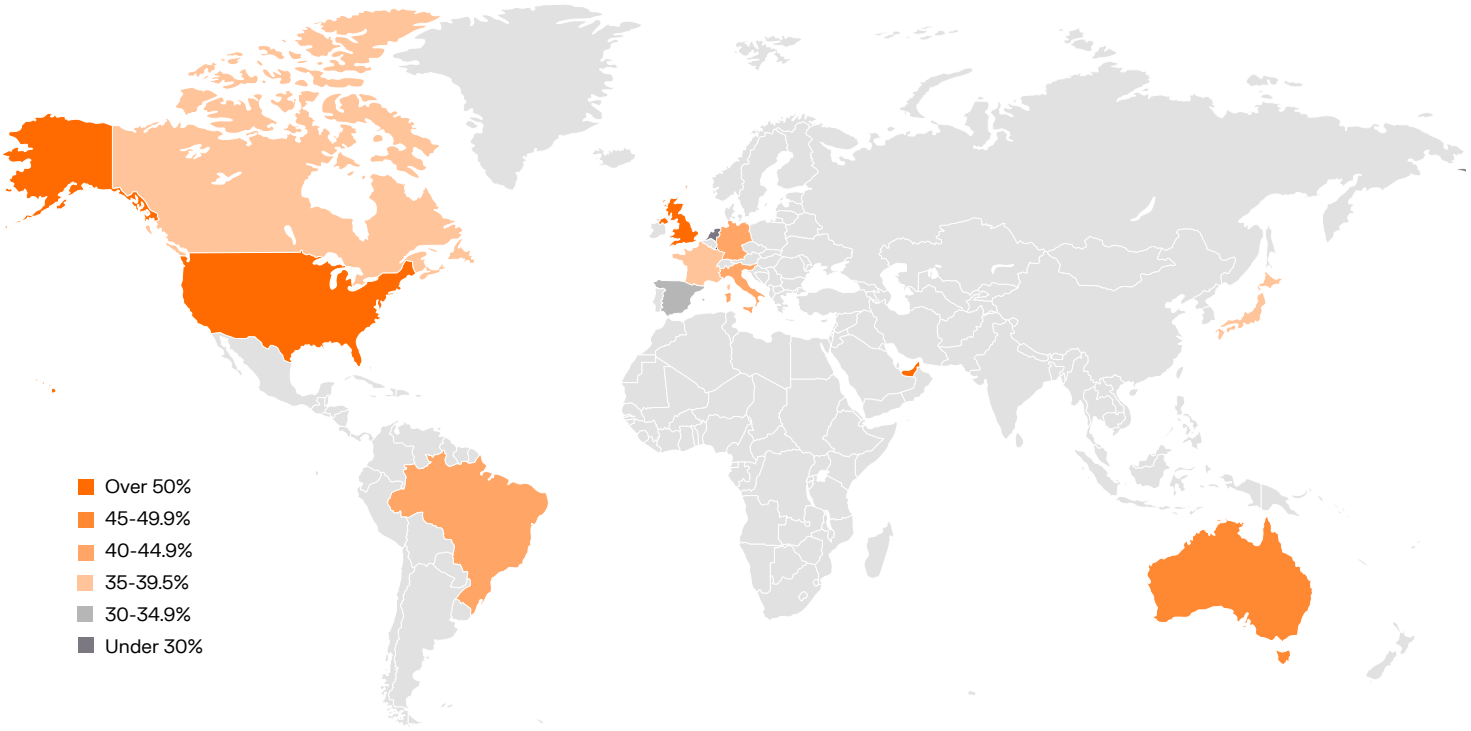
Among the 95% of participants who said their organizations were either discussing a policy on the safe and secure use of AI or had already implemented one, only a minority (45%) had already established such a policy.

The very smallest organizations (those with fewer than 1,000 employees) and the very largest (those with more than 25,000 employees) were the least likely to have AI security policies in place, with only 38% of participants in these two groups reporting that they had already implemented a policy.

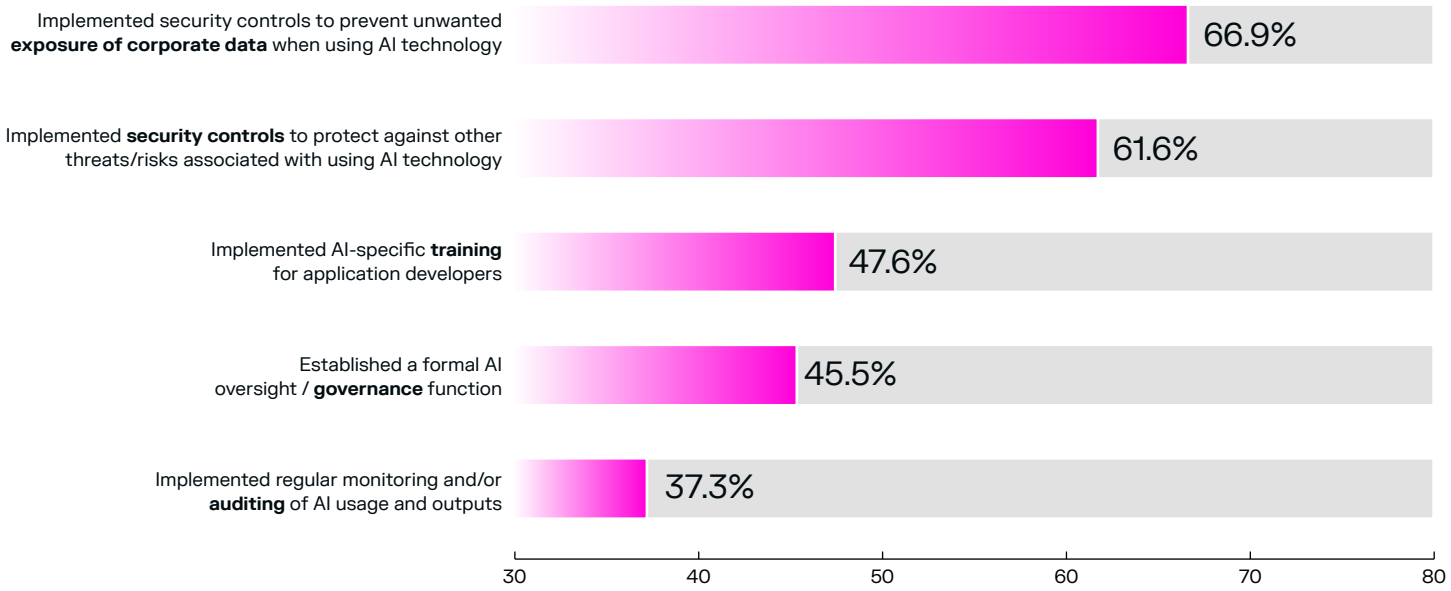
Organizations that have a formal policy on how to safely and securely use AI, by organization size



Organizations that have a formal policy on how to safely and securely use AI, by country



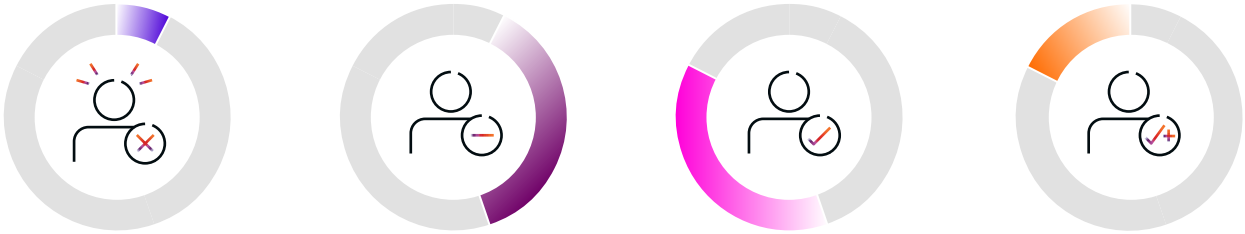
Measures taken to ensure safe and secure use of AI



More than 85% of participants in last year's survey indicated that their organizations had already taken steps to mitigate the risks associated with AI adoption. This year, we see them going even further by implementing specific controls, training, and oversight.

Organizations in the financial services and retail sectors tended to exhibit higher levels of maturity, while government agencies were lagging in this area.

Self-doubt remains prevalent: Nearly half of participants say their organizations ***aren't adequately prepared*** for AI-powered threats



7.6%
We are NOT adequately prepared for AI-powered threats

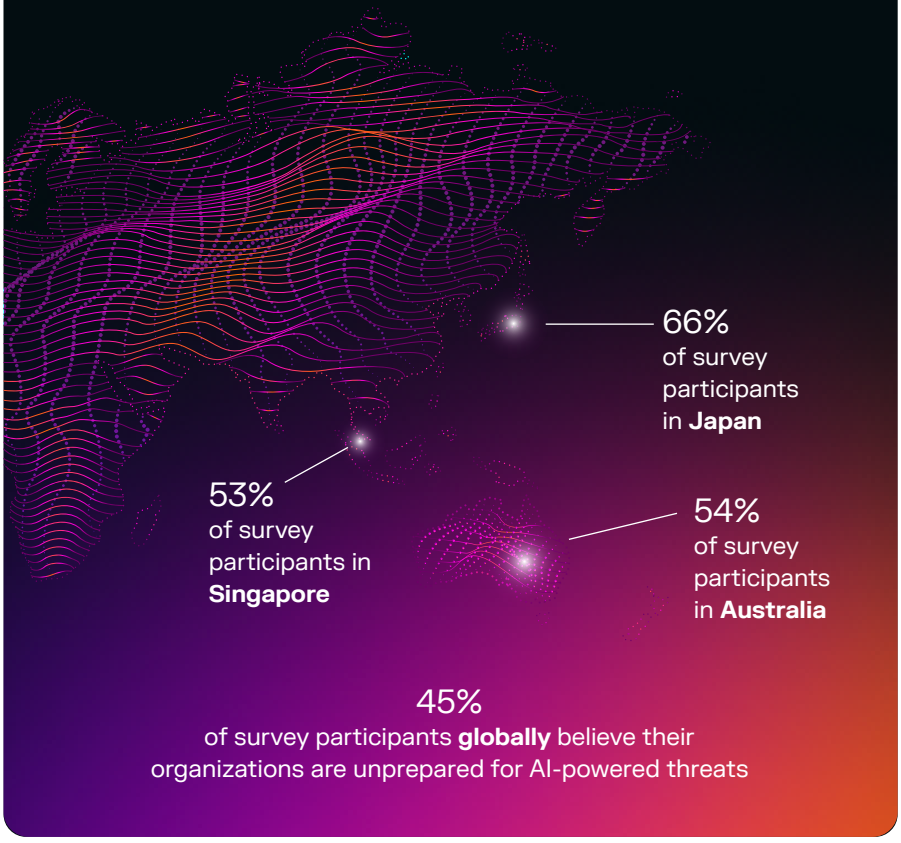
37.2%
We are somewhat prepared for AI-powered threats

37.9%
We are prepared for AI-powered threats

17.3%
We are definitely prepared for AI-powered threats

This represents an increase in confidence from last year, when a full 72% of participants agreed that their organizations were not adequately prepared. Still, less than 18% have strong confidence in their organization's readiness to defend against AI-powered threats and attacks, an increase of only 2%.

Survey participants in the Asia-Pacific region were most likely to believe their organizations are unprepared (with 58% agreeing)



45%
of survey participants **globally** believe their organizations are unprepared for AI-powered threats

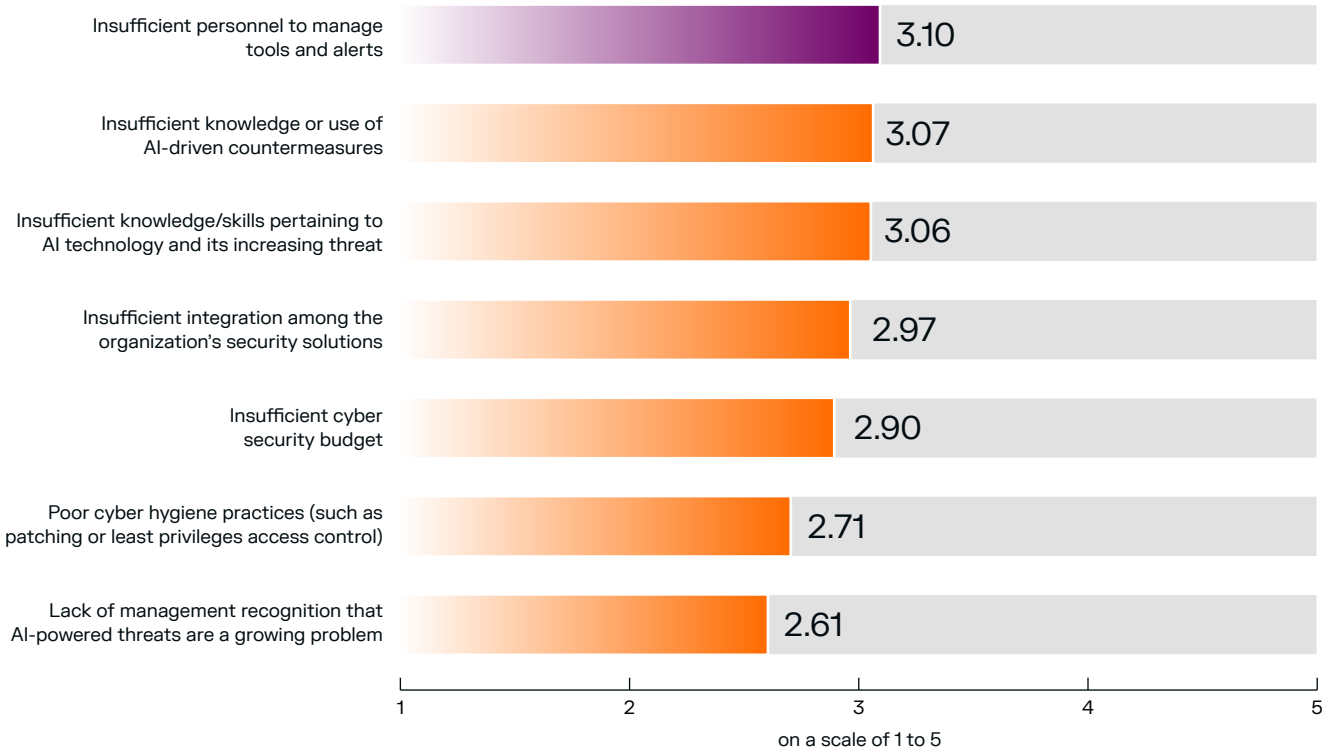
The Confidence Gap

Participants in executive roles were far more likely to agree that their organizations were prepared to face AI-driven threats (with **62%** generally in agreement) than those with hands-on experience.[4] Nearly half (**49%**) of security operations practitioners and **47%** of security architects and engineers expressed confidence in their organizations' preparedness.

These differences in confidence are evidence of a disconnect between leaders and front-line practitioners. Those who are in the trenches understand what it is like to do battle with AI-powered adversaries on a daily basis, and clearly see where present-day solutions fall short.

[4] Executive roles include CIOs, CISOs, and other IT security executives. Those with hands-on experience include roles like security analysts, operators, incident responders, admins, architects, and engineers.

Greatest inhibitors of organizations' abilities to defend against AI-powered threats



With the size of the worldwide talent gap now approaching five million, and 71% of organizations surveyed reporting that they have at least one unfilled cybersecurity position, it is no surprise that skills gaps are creating significant risks for organizations across industries. Nor is it surprising that organizations are struggling to find professionals with the skills needed to manage AI-powered defenses, since these tools are new.

Budget isn't a concern for most survey participants, which was also the case last year. Lack of management recognition of the problem fell to last place, indicating that high-level awareness also isn't the main issue.

Confidence in traditional cybersecurity tools is waning

One in every ten surveyed cybersecurity professionals has no confidence whatsoever in the ability of non-AI-based cybersecurity solutions to detect and block AI-powered threats, while fully half (50%) of participants are less than significantly confident in the capabilities of these traditional tools.

How confident are you in traditional cyber security solutions (i.e., ones not featuring AI technology) to detect and block AI-powered threats and attacks?

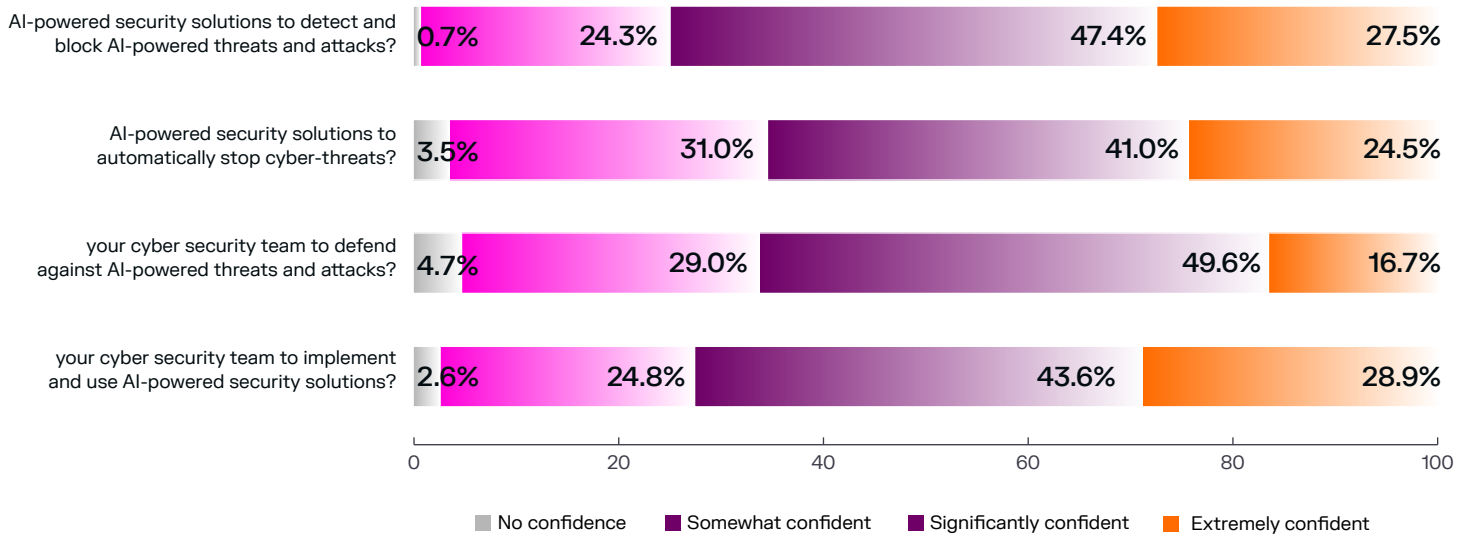
10.2%
Not confident

40.2%
Somewhat confident

35.6%
Significantly confident

13.9%
Extremely confident

Currently, how confident are you in the ability of...



While confidence in traditional cybersecurity tools is declining, security professionals have growing confidence in their ability to implement and use AI-powered solutions. This year, 73% of survey participants expressed confidence in their security team's proficiency in using AI in their tool stack, an increase from last year.

Participants from the APAC region were particularly likely to report a lack of confidence in traditional cybersecurity solutions (55% don't believe they can stop AI-powered threats), but they also don't have confidence in the defensive capabilities of their teams (45% do not believe they can defend against AI-powered threats) or their ability to implement and use AI-driven tools (40% expressed a lack of confidence here).

As leading organizations implement and optimize their use of AI, they are incorporating it into a growing number of workflows. The more familiar it becomes, the higher the confidence levels of practitioners are likely to be.

SOC analysts and administrators are slightly less confident in the ability of AI-powered tools to detect and block AI-powered threats, with 45% and 55%, respectively, expressing a lack of confidence. Stakeholders in very large organizations (those with more than 25,000 employees) also have less confidence in AI-powered security solutions than average, with 51% expressing a lack of confidence. With larger and more diverse attack surfaces to protect, larger enterprises face more complex defensive challenges—making things harder for their teams, regardless of which tools they use.

73%

of survey participants expressed confidence in their security team's proficiency in using AI in their tool stack, an increase from last year.

55%

of administrators are slightly less confident in the ability of AI-powered tools to detect and block AI-powered threats.

51%

of stakeholders in very large organizations (those with more than 25,000 employees) also have less confidence in AI-powered security solutions.

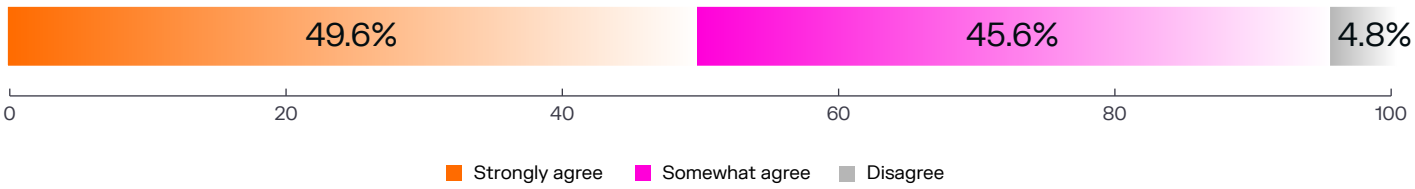
Navigating Digital Ecosystem Complexity: The Impact of AI on Cybersecurity Solutions

AI can serve as a much-needed force multiplier for Security Operations Center (SOC) teams, making it possible for organizations to scale their ability to detect, investigate, and respond to threats without adding headcount. Because AI can analyze massive amounts of data, it empowers defenders to act faster, more accurately, and more effectively. When SecOps programs use AI to automate low-level, repetitive tasks, they become able to focus their attention on higher-value work that's more strategic in nature.

However, not all AI is created equal when it comes to closing the skills gap. The organizations that are best able to understand the strengths and weaknesses of different types of AI—as well as how each can best be applied in relevant use cases—will be advantaged in building effective and efficient defenses.

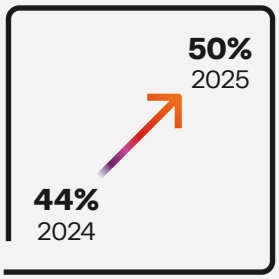
Not everyone has this understanding. Further complicating the situation is the fact that cybersecurity vendors are eager to capitalize on all the hype about AI, but vendor claims can be vague and confusing.

95% of cybersecurity professionals agree that AI-powered solutions can significantly improve the speed and efficiency of their defenses.

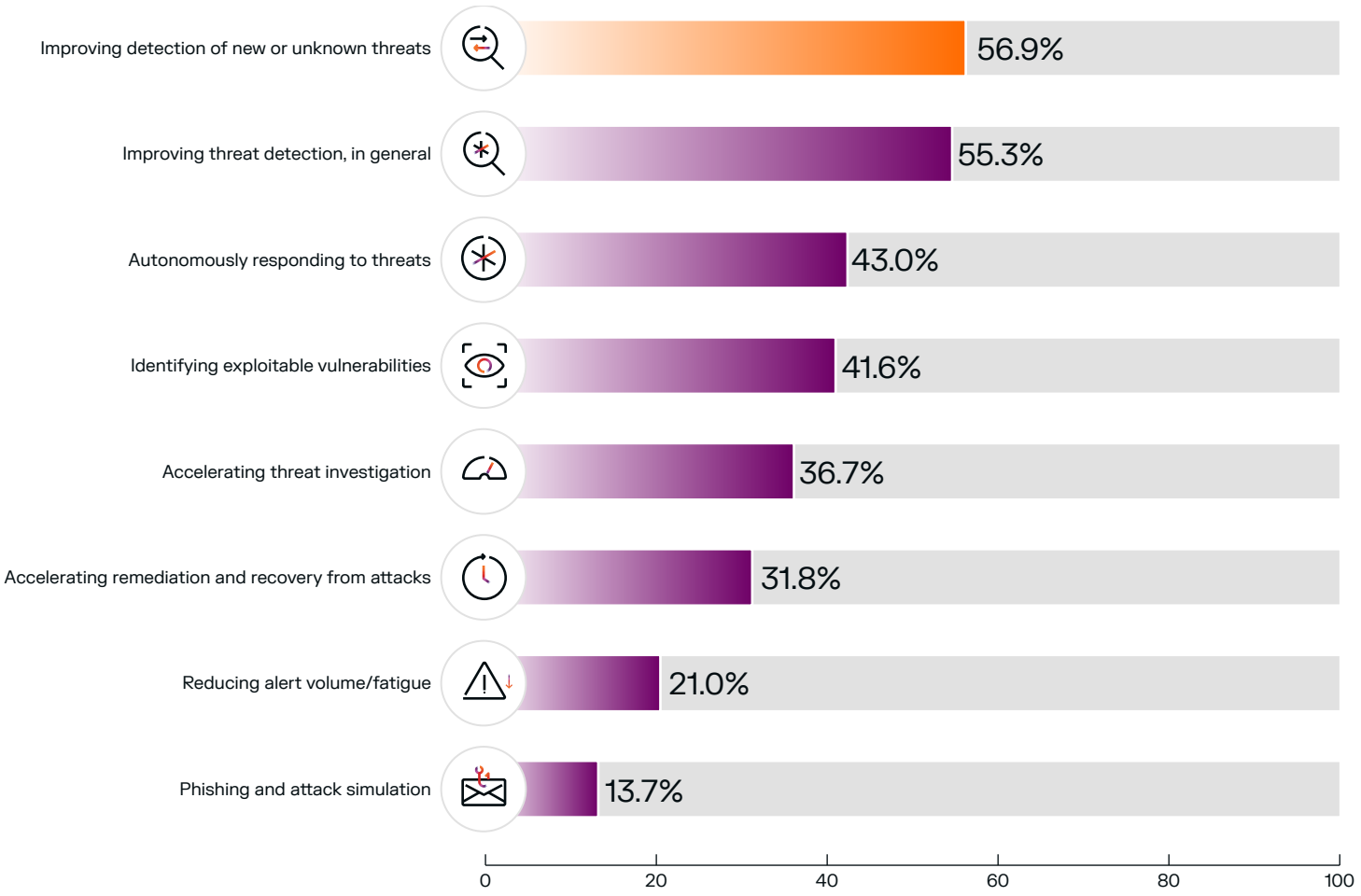


There's near universal agreement that AI-powered cybersecurity solutions will greatly improve the ability of security teams to prevent, detect, respond to, and recover from threats. In fact, 95% of participants agree with the above statement.

The percentage of cybersecurity professionals surveyed who agree that AI-powered solutions can significantly improve the speed and efficiency of their defenses increased from 2024 to 2025.



Areas/domains defensive AI is expected to impact the most

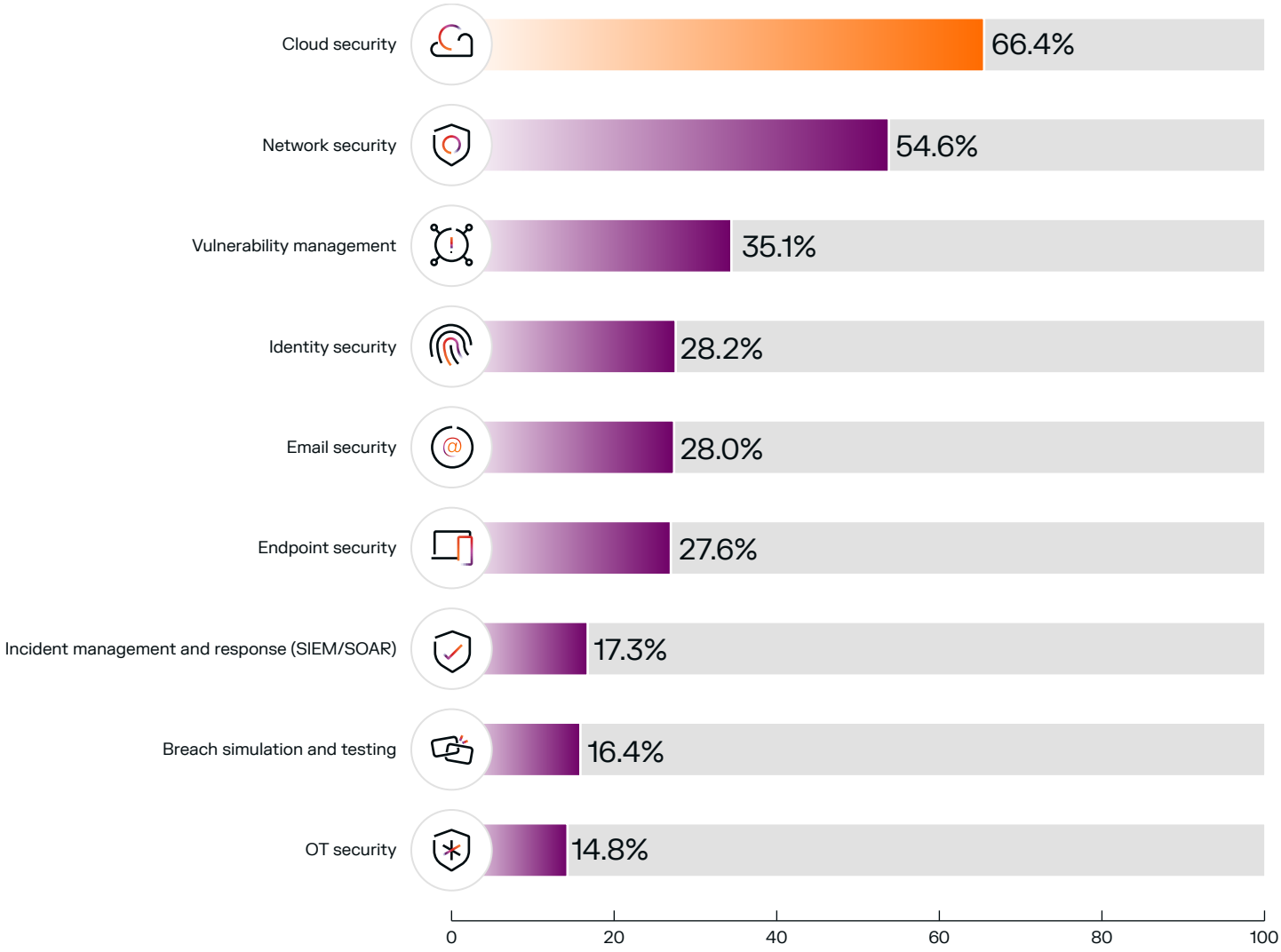


Improving the detection of new and unknown threats is the number one area within cybersecurity where AI is expected to have an impact. AI that is trained on an organization's real-time data can understand what is normal for every device, account, user, and cluster within that organization. This makes it possible to pinpoint anomalous behavior patterns and activities as soon as they occur, so that novel threats can be identified and stopped right away.

Areas that participants ranked lower (including reducing alert volume and analyst fatigue and phishing and attack simulation) are things that AI can already do well. Tools like Darktrace's Cyber AI Analyst are helping automate Level 2 SOC analysis in over 10,000 organizations, reducing alert volume from thousands of individual events to just a handful of overarching incidents. With AI already in widespread use—and delivering value—in these areas, it is likely that participants aren't expecting its biggest impact to come within the next three years for these use cases, because it is already here.

Improving the detection of new and unknown threats is the **#1** area within cybersecurity where AI is expected to have an impact.

Domains within cybersecurity where participants expect defensive AI to have the greatest impacts



Cloud security (66%) and network security (55%) are the domains within cybersecurity where defensive AI is expected to have the greatest impact.

Since last year's survey, expectations that AI will impact cloud and network security in the next few years have increased (from 61 to 66% for cloud, and from 46 to 55% for network). Vulnerability management is also seeing much more interest, with the percentage of participants selecting it having increased from 23 to 35%.

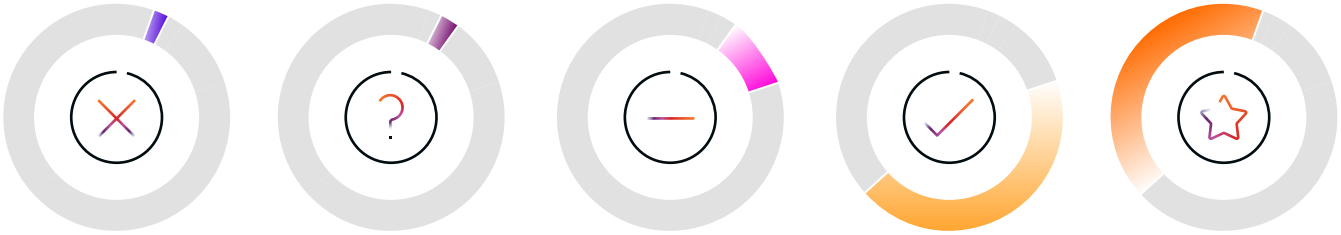
As security professionals become more familiar with AI and the kinds of value it can bring in real-world workflows, their responses may be more representative of the experiences that most early implementers are having. Security teams may, for instance, already be seeing the impact that AI can have on areas like incident response, where it can autonomously initiate an intervention to contain an in-progress attack, buying them time to conduct deeper analysis and remediation. They may be aware of its capability to improve breach and attack simulation and testing.

Yet the cloud's complexity continues to present challenges. As enterprises become more and more reliant upon SaaS applications and cloud platforms, attackers will target these environments, seeking unauthorized access to privileged accounts through account takeovers. Once they've gained initial access to cloud resources, they can move laterally across the environment in search of valuable data or opportunities for fraud and extortion.

Knowledge Is Power: Understanding AI Types and Technologies

If stakeholders are to maximize the value of AI in real-world operations, they will need a nuanced understanding of what AI is, how the different types of AI work, and where AI can deliver the most value. Not all of today's cybersecurity decision-makers and practitioners have this requisite knowledge.

Only 42% of security professionals are confident that they fully understand all the types of AI in their organization's security stack.



2.1%
Not applicable — we are not using any form of AI in our cybersecurity stack at this time

2.6%
I don't know what type(s) of AI are being used in our cybersecurity stack

9.9%
I have only a vague understanding of which type(s) of AI are being used in our cybersecurity stack

43.3%
I have a reasonable understanding of which type(s) of AI are being used in our cybersecurity stack

42.0%
I know exactly which type(s) of AI are being used in our cybersecurity stack

Executives surveyed report higher levels of understanding (60% say they know exactly which types of AI are being used) than participants in other roles. This may indicate the greater confidence that leaders are often asked to exhibit, rather than higher levels of technical proficiency. Despite having more hands-on job responsibilities, SecOps practitioners and administrators surveyed were more likely to report having a "reasonable understanding" of the types of AI in use in their organizations (42% and 55%, respectively).

Survey participants in larger organizations (>10K employees) report lower levels of understanding

26%

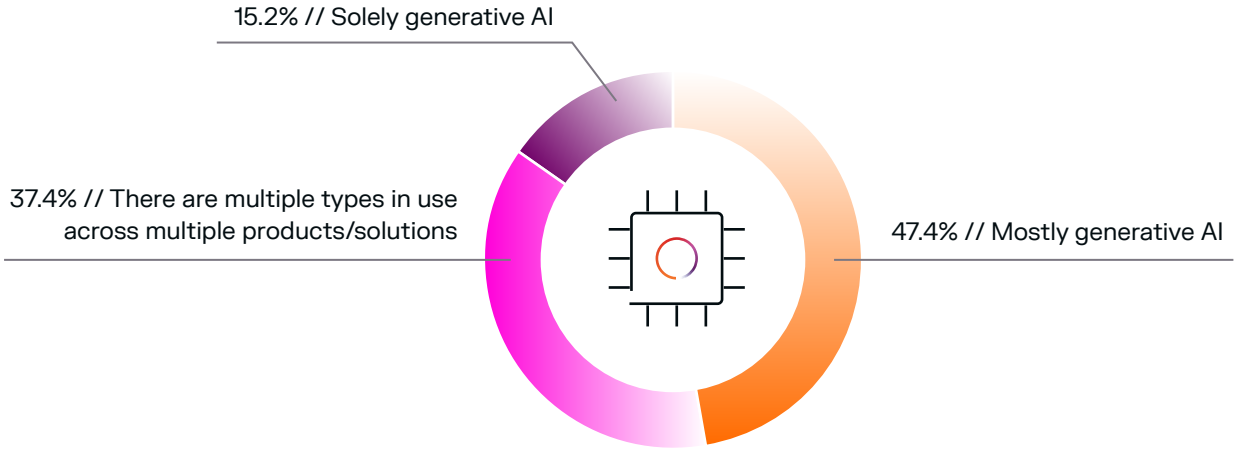
say they have only a vague or no understanding of the AI technologies being used in their organization's cybersecurity stack — twice the overall average.

17%

of participants in the APAC region admitted to having only a vague understanding of the AI their organization uses for cyber defense—or no knowledge at all.

What's clear is that vendors are introducing new AI-powered solutions and capabilities at a faster pace than employees are being trained how to use them. If organizations are going to maximize the value of AI, they will need to facilitate effective human-AI collaboration. For this, cybersecurity professionals must have training on how to leverage, understand, and work with AI systems. While implementing AI can help upskill human teams, it can do so only if security professionals are supported by providing them with access to the right resources and education.

63% of security stakeholders believe their existing cybersecurity stack solely or mostly leverages generative AI

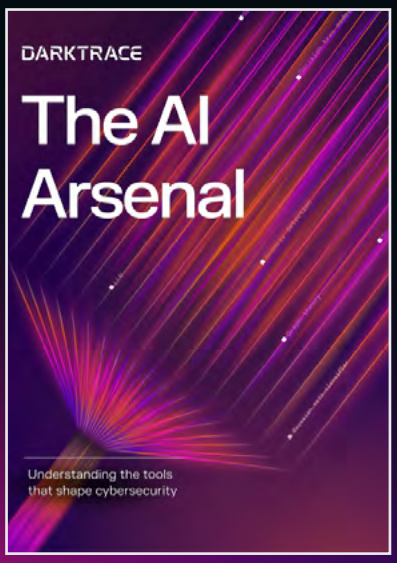


Both this year and last, participants have shown a tendency to believe that gen AI plays a much larger role in cyber defense than is actually the case. Nearly two-thirds (63%) believe that their organization's cybersecurity tools leverage solely or mostly gen AI. Participants in Latin America are especially prone to entertain this misconception, with 83% believing that their cybersecurity stack uses gen AI exclusively or primarily.

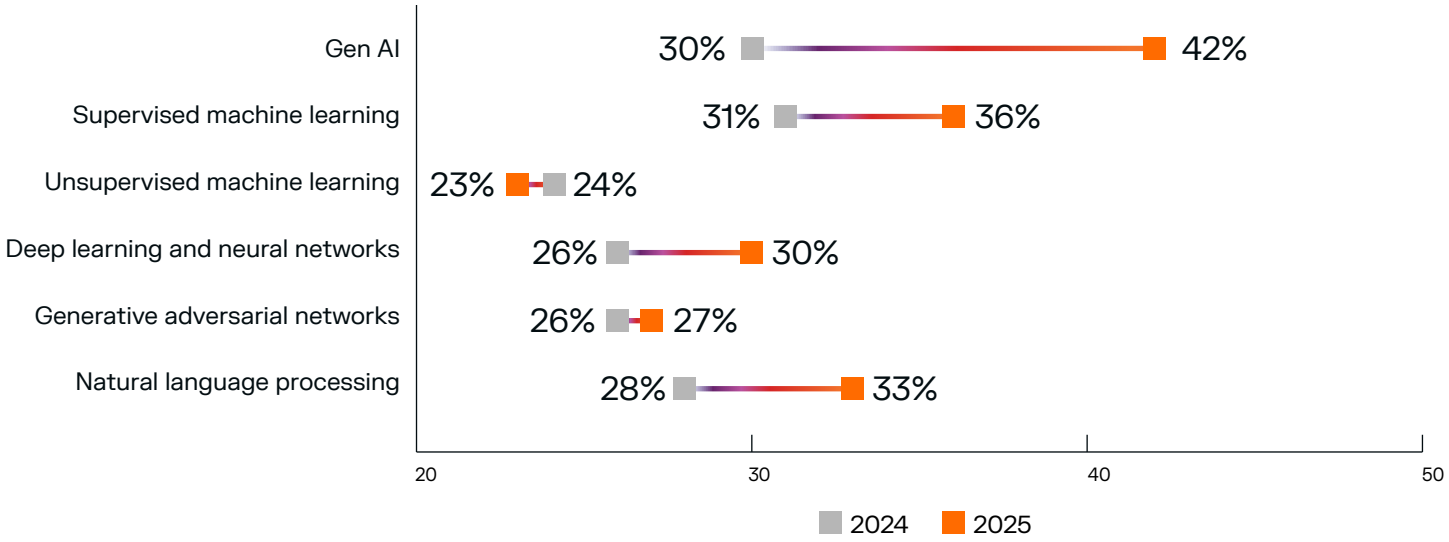
In reality, this is rarely true. Gen AI can serve only in a limited number of use cases, such as phishing simulations and enabling SecOps analyst teams to interact with threat hunting and triage workflows via a natural language interface. Other types of AI can deliver value for a much wider set of use cases, including forecasting attacker behavior, accelerating detection and remediation, and augmenting preventative workflows.

Darktrace has published a technical whitepaper that deep-dives into different AI types and techniques currently in use in cybersecurity

Read the Report →



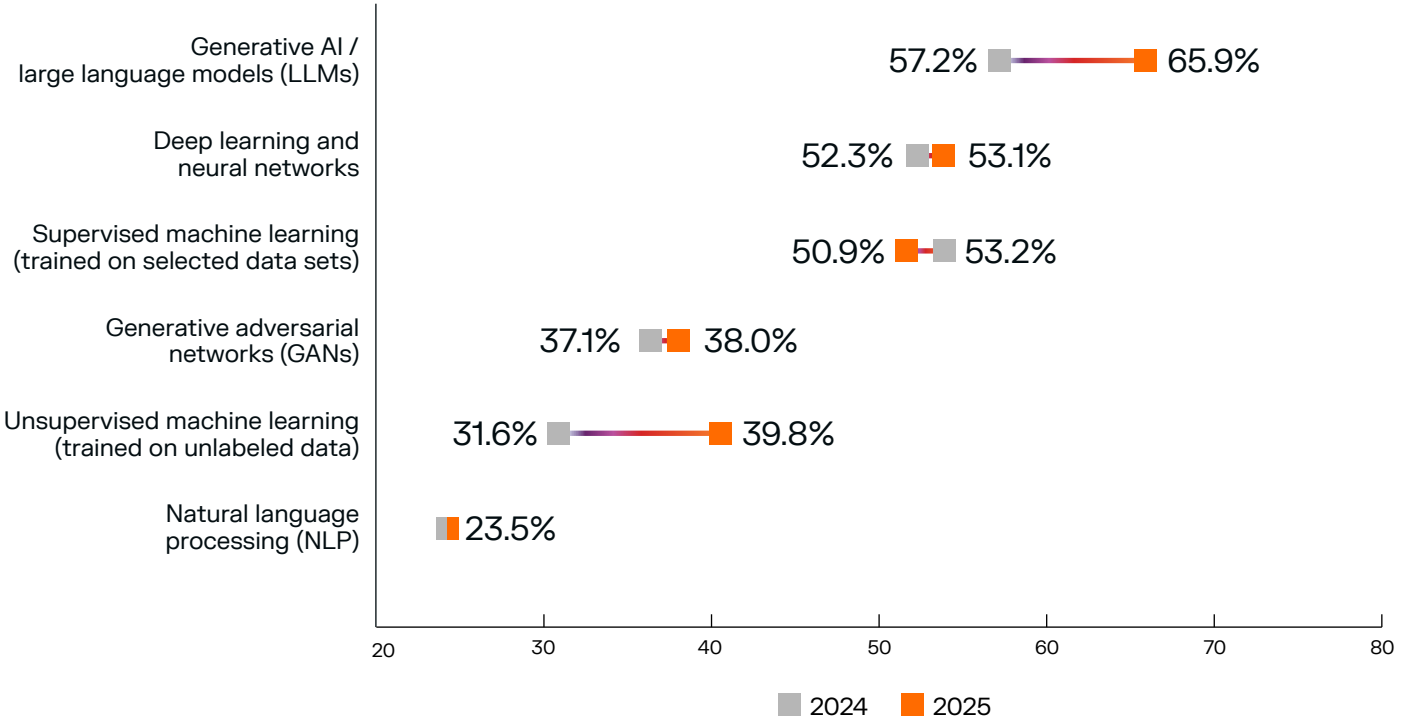
Levels of familiarity differ with different types of AI – but are growing across the board.
% of survey responders saying they are 'very familiar' with each type of AI



Executives report the highest degrees of familiarity with all the technologies they were asked about (91% familiar with gen AI, 74% familiar with GANs), which may reflect a more abstract understanding of what it means to be familiar with a technology. Those in more hands-on roles may have a more in-depth understanding of what "familiar" means, so only 61% of SecOps practitioners said they were familiar with gen AI, while 60% were familiar with supervised ML, and 30% familiar with GANs.

If organizations want to implement AI effectively across their security stacks, they'll need to invest in training stakeholders across the organization (in both technical and non-technical roles) to better understand what AI is and how it can work to level up cyber defense.

Which of the following types of AI do you expect to have the greatest impact on cyber security in the next 3 years?



In general, it seems that AI types that are more familiar (see previous question) are perceived to be more likely to impact the field.

Executives are particularly excited about the future potential of gen AI to transform SecOps, while practitioners expect deep learning, neural networks, and supervised ML to have a bigger impact than gen AI.

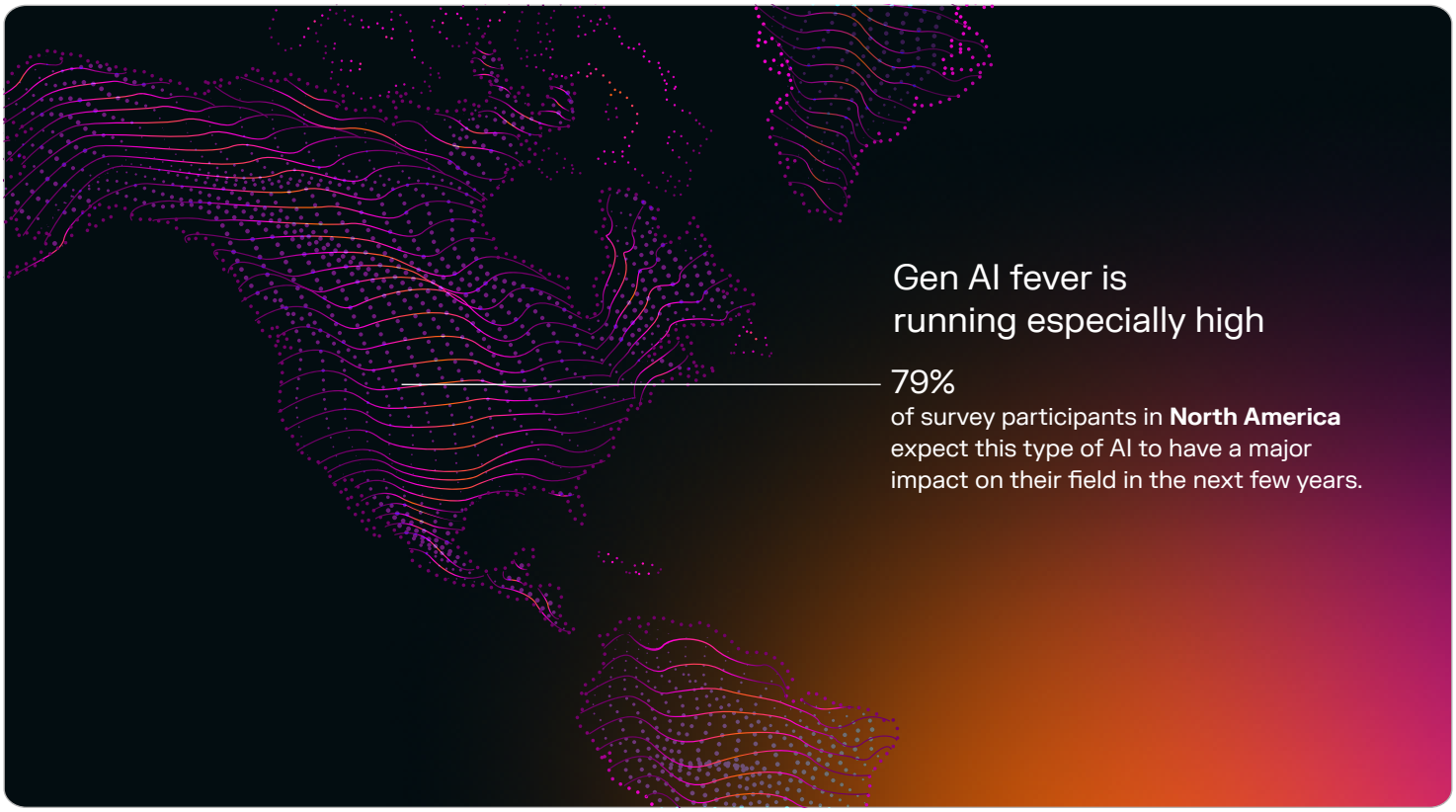
71%

of Executives expect generative AI to transform SecOps

vs.

50%

of SecOps practitioners expect generative AI to transform SecOps

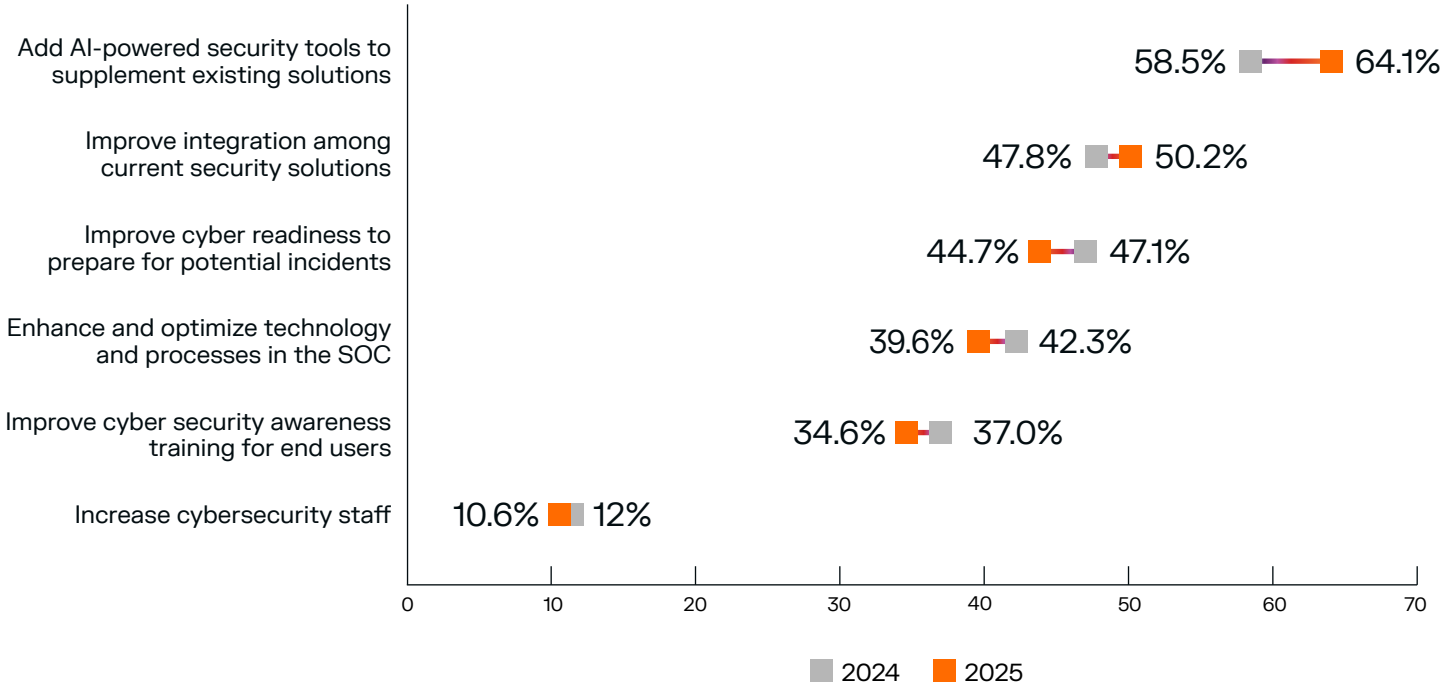


The effectiveness of hands-on practitioners is in fact more likely to be aided by technologies like unsupervised ML, which can provide insights that traditional cybersecurity tools will miss. Unsupervised ML continuously learns what is normal for an organization, making it able to detect all kinds of attacks, including unknown and novel ones. These include zero-day exploits, account takeovers, insider threats, lateral movement, and cross-domain attacks. It is already being harnessed for these purposes in solutions like the Darktrace ActiveAI Security Platform, where it delivers unprecedented visibility into never-before-seen threats. Practitioners working with such solutions are unlikely to believe that this type of AI will have a large future impact on their field, because it is instead having a massive *present-day* impact.

Future Focus: Priorities and Objectives

Security professionals know that their field is changing fast. They are aware that the rise of AI will require them to adopt new tools and learn to use them effectively. Still, they aren't always certain about how to plan for the future, or what to invest in.

The top priorities of security stakeholders for improving their defenses against AI-powered threats include augmenting their existing tool stacks with AI-powered solutions and improving integration among their security tools



As was also the case last year, security stakeholders are less interested in hiring additional staff than in adding new AI-powered tools onto their existing security stacks. This remains true even though survey participants earlier indicated (see page 11) that a lack of personnel was their biggest inhibitor to building effective defense against AI-driven threats.

With burnout pervasive, the talent deficit reaching a new peak, and growing numbers of companies unable to fill cybersecurity positions, it may be that stakeholders realize they simply cannot hire enough personnel to solve this problem, no matter how much they may want to.

In fact, interest in hiring security staff has declined since last year, even as the percentage of participants prioritizing adding AI-powered tools onto their security stacks grew from 58 to 64%. Executives are particularly enthusiastic about adding on AI-driven tools, while practitioners in SecOps are more interested in improving security awareness training and improving cybersecurity tool integration.

One conclusion we can draw from the attitudinal shifts from last year's survey to this year's: while hiring more security staff might be a nice-to-have, implementing AI-powered tools so that existing employees can work smarter is increasingly viewed as a must-have.

Priorities When Adding New Solutions

"When purchasing new security capabilities or replacing existing products, my organization prefers ones that are part of a broader platform over individual point products."

87% agree

89% among executives;
78% among security operators & analysts

These results are similar to last year's, where again, almost nine out of ten agreed that a platform-oriented security solution was more effective at stopping cyber threats than a collection of individual products.

"The use of AI within our security stack is critical to freeing up time for our security team to become more proactive (vs. reactive)."

88% agree

92% among executives;
80% among security operators & analysts

A large majority agree that the use of AI within their cybersecurity stack is already freeing up time for practitioners, allowing them to adopt a more proactive approach. AI itself can contribute to this shift from reactive to proactive security, improving risk prioritization and automating preventative strategies like Attack Surface Management (ASM) and attack path modeling. Teams can also leverage AI to build more effective security awareness training programs.

"We prefer defensive AI solutions that do NOT require our organization's data to be shared externally (e.g., to "feed" an external LLM)."

84% agree

82% among executives;
86% among security operators & analysts

This preference may reflect increasing attention to the data privacy and security risks posed by gen AI adoption. It may also reflect growing awareness of data residency requirements and other restrictions that regulators are imposing.

Different vendors have different methods of handling model training data and other AI inputs. Many move proprietary data out of the customer environment and into a centralized data lake, where it is combined with the data from hundreds of other organizations and used to train the models.

Others offer their customers the option of storing all of their data onsite or in a private cloud. Different analytic methods are also available, including non-invasive ones that protect privacy by analyzing metadata rather than content. If your organization has regulatory restrictions on how its data can be used or where it can be stored, it is vitally important to ask questions about AI governance of prospective vendors.

The Time Is Now: Achieving AI Cyber Maturity

Over the past year, threat actors have used gen AI to launch large numbers of relatively unsophisticated attacks, such as sending out large volumes of highly convincing phishing emails. They're harnessing other types of AI for more sophisticated purposes too, but this is still happening at a smaller scale. Inevitably, though, these ongoing efforts to innovate and leverage new tools will bear fruit. We expect to see more and more successful AI-driven attacks in the months and years to come.

Defenders are well aware of this evolution and understand that incorporating AI into the security stack is essential for keeping up with the progressive development of threats. But levels of understanding of the technology vary across organizations, as do degrees of adoption and implementation maturity.

The Darktrace ActiveAI Security Platform was expressly designed to help organizations fill talent gaps and uplevel their cybersecurity maturity. The platform was built to enable collaboration and reduce the learning curve—lowering the barrier to entry for junior or less-skilled analysts. Darktrace also offers expert training, 24/7 access to cybersecurity analysts, and managed services to support your team.

Darktrace has been using AI technology in cybersecurity for more than a decade. As a pioneer in the space, we have made innovation an integral part of our process.

The Darktrace ActiveAI Security Platform uses multi-layered AI that trains on your unique business data for tailored security across the enterprise. This approach ensures well-rounded and reliable coverage with models that are always on and always learning, allowing your team to stop attacks in real time. Additionally, our focus on using customer data from the entire digital estate brings advantages in data privacy, interpretability, and data transfer costs.

Darktrace promotes the responsible use of AI, using proven methods to enforce safeguards in its application and ensure that its outputs are always explainable. With our unique approach and continuous product innovation, Darktrace helps augment human teams to protect against evolving attacks in real time, including the latest and most innovative cyber threats. We facilitate positive and effective human-AI partnerships to meet individual organizations' unique needs.

Take the Next Step

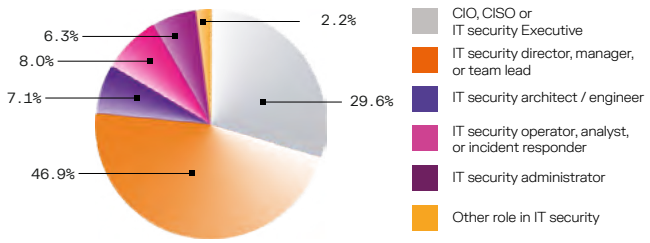
Navigate the next wave of AI disruption.

Join us at **Darktrace LIVE** — coming to a city near you — to network with your peers and see expert talks and live demos.

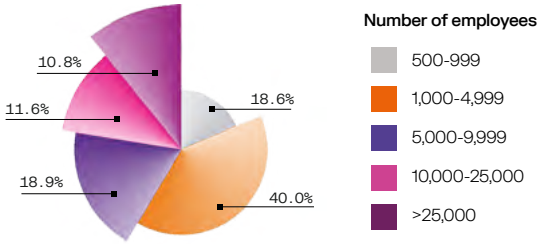
Survey Methodology

Our survey was conducted online in September 2024. Respondents held a variety of positions within information security. Roughly 30% were CIOs, CISOs, or other senior leaders. Survey participants came from 14 different countries in four different regions, including North and Latin America, Europe, and the Asia-Pacific region. Their organizations ranged in size from 500 employees to more than 25,000, with most (59%) working for organizations with more than 1,000 and less than 10,000 employees.

Survey participants by role



Survey participants by size of organization



Disclaimer:

This report is based on data derived from a survey that assessed how cybersecurity and IT professionals perceive AI in cybersecurity. The findings are based on self-reported assessments and subjective opinions of survey participants rather than objective performance measures or independently verified data.

This report is provided "as is" without any warranties or representations, either express or implied, including but not limited to any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. Darktrace, contributors, and associated organizations make no representations or warranties regarding the completeness, accuracy, or reliability of the information contained in this report, particularly in regard to the subjective nature of the survey responses.

Darktrace, contributors, and associated organizations do not accept any liability for errors, omissions, or actions taken based on the contents of this report. Readers are advised to consult additional sources and experts for the most current and comprehensive information regarding AI-powered cybersecurity and organizational preparedness.

About Darktrace

Darktrace (DARK.L), a global leader in cybersecurity artificial intelligence, is on a mission to free the world of cyber disruption. Its technology continuously learns and updates its knowledge of 'you' for an organization and applies that understanding to help transform security operations and improve cyber resilience. Breakthrough innovations from its R&D Centers have resulted in more than 200 patent applications filed. Darktrace employs 2,400 people around the world and protects over 10,000 organizations globally from known, unknown and novel cyber-threats.

North America: +1 (415) 229 9100 | Europe: +44 (0) 1223 394 100 | Asia-Pacific: +65 6804 5010 | Latin America: +55 11 4949 7696

darktrace.com | info@darktrace.com