Arkose Labs

New Research: The Intersection of AI, Digital Fraud and Cyber Defenses

PART 2: CURRENT STATE OF AI-BASED SOLUTIONS AND BENEFITS

November 2024

Table of Contents

Executive Summary

As a cybersecurity executive, you may not directly drive revenue, but you do hold the line in protecting revenue-driving platforms like websites and apps. Today, AI complicates this mandate, introducing new challenges in safeguarding consumer-friendly, seamless online experiences.

Part one of our inaugural research "The Intersection of AI, Digital Fraud and Cyber Defenses" revealed growing alarm over specific attack types. Enterprises continue to face frequent attacks like credential stuffing and account takeovers—roughly 3 out of 4 respondents across industries expressed serious concern about scammers gaining unauthorized access to consumer accounts. AI is the accelerant: In just 12 months, AI-powered bots (40%) have become the main source of attacks like ATO. The surge is material, with 88% of enterprises seeing a significant increase in AI-powered bot attacks since 2022. The increase was 36%. This swift escalation in the deployment of adversarial AI demands a sophisticated and thoughtful response.

> "It seems like a natural progression for fraudsters to leverage the latest AI technologies. I'm not sure if we can fully isolate that behavior yet, but it's definitely an interesting angle and a good reminder that we need the right tech to handle these evolving threats." – **Executive, Payments and Risk, Streaming Media Industry**

Part three introduces a new category to watch. These are the AI Enthusiasts—enterprises that are further down the path of leveraging defensive AI. In fact, these enterprises are 3.5X more likely to be "very well prepared" for defending against volumetric attacks compared to their peers.

Leveraging AI to defend against AI-driven attacks is now an imperative. Here, in part two of this research, we examine how forward-thinking cybersecurity executives and their teams are taking action and adopting AI-resistant solutions to fight AI with AI.

We dive into the specific actions cybersecurity leaders are taking, their AI-driven investments and the tangible gains they're experiencing. Roughly 70% of enterprises report leveraging AI to enable faster response times, predict future security threats, analyze historical data and analyze cybersecurity data in real-time.

Other key highlights:

- **21%** of cybersecurity budgets are allocated to AI-driven solutions. By 2026, this figure is expected to rise to **27%**.
- **68%** of respondents believe AI has improved their company's overall cybersecurity posture, but…
- Only **1 in 5** enterprises feels very well prepared for using AI to defend against bad actors conducting volumetric attacks.
- Given the rapidly evolving threat landscape and embrace of AI by threat actor groups, most are tapping into specialized third-party solutions – **62%** of enterprises realize more value through **buying AI-powered cybersecurity solutions** versus building in-house solutions.
- AI-powered solutions are most commonly used in **bot management, payment and CX/CRM initiatives.**
- Peace of mind is **6.5X** more commonly associated with the ability to use AI to defend against volumetric AI-powered attacks than uncertainty/fear/stress.

At Arkose Labs, we pioneered AI-resistant defenses purpose-built for global enterprises with complex infrastructures to protect their account sign-up, sign-in and other in-platform consumer touchpoints.

We would like to hear from you. Reach out to set up a knowledge-sharing conversation.

Best Regards,

Patrick Kehoe
CMO
Arkose Labs
p.kehoe@arkoselabs.com

Frank Teruel
CFO
Arkose Labs
f.teruel@arkoselabs.com

Vikas Shetty
Head of Product
Arkose Labs
v.shetty@arkoselabs.com

Actions Enterprises Are Taking

Across sectors, AI is being deployed to manage expanding risk. Survey respondents revealed that roughly 70% of enterprises have integrated AI to enhance critical aspects of their security operations, namely, accelerating response times, forecasting potential threats and conducting historical and real-time data analysis. These actions underscore a growing reliance on AI to manage the increasing velocity and complexity of cyber threats, such as fraudsters using AI-powered bots to register hundreds of millions of fake accounts, suggesting that many enterprises now see defensive AI not as an optional enhancement but as a foundational tool in their security strategy.

However, the intensity of AI adoption varies across sectors: financial services and technology stand out for implementing AI-driven security measures at a rate exceeding the cross-industry average. This distinction likely reflects the higher stakes within these sectors, where the volume of PII data and the consequences of breaches are particularly pronounced.

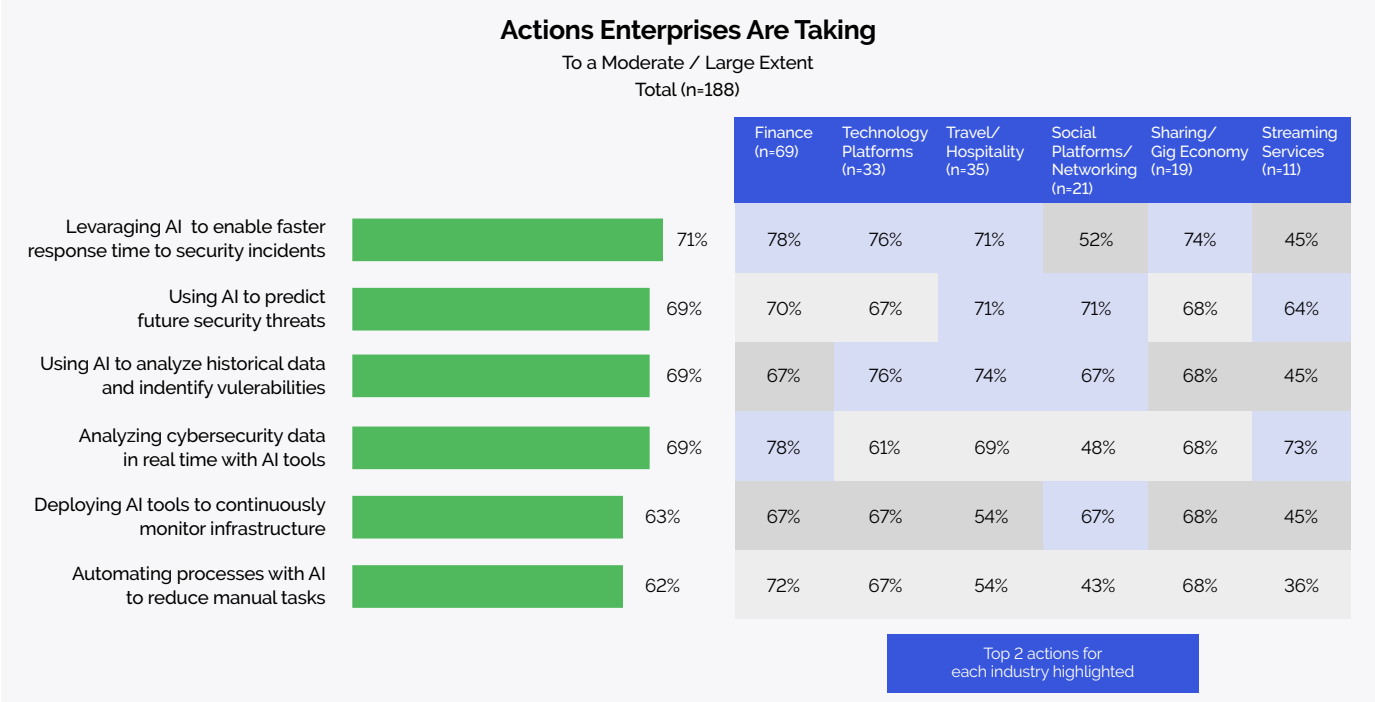


Chart 1 and Table 1 Q: To what extent is your company taking the following actions...? (RANDOMIZE; RATE EACH ROW)

Analysis of the data revealed 79% of banks report that AI is enabling faster response times to security incidents, while 85% of fintechs use AI to analyze cybersecurity data in real time. The ability to predict future security threats and analyze vast amounts of data instantaneously is a game changer for these industries, where time is money, and every second of delay in responding to a cyber threat can lead to significant financial losses.

In the airline industry, 86% of respondents use AI to identify vulnerabilities and predict threats—an essential strategy in a sector that operates on razor-thin margins. With brand trust and customer loyalty at stake, a single breach can cause lasting damage like flyers never flying with them again. Notably, in part one of the report, 86% of airlines also cited brand reputation loss as the top negative consequence from threats such as account takeovers, loyalty point theft, bonus abuse and inventory hoarding they've experienced over the past two years. The airlines also reported that due to the negative consequences, their losses reached up to $500 million over the past two years. These findings underscore the industry's high-stakes environment, where AI is contributing as a critical tool for preemptive threat management.

It's worth noting that 74% of sharing/gig economy companies, 75% of hotels and 76% of technology companies also leverage AI to speed up their response times, reflecting a broad recognition of AI's role in enhancing operational resilience that ultimately protects their consumers' digital accounts.

For the full breakdown of industry-specific data, see the Appendix.

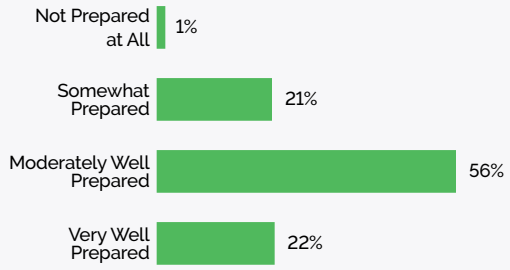
The consensus is clear: Enterprises are seeing real-time benefits in their ability to anticipate and react to threats more effectively, which is priceless as cyberattacks grow more complex and automated.

Are Enterprises Ready to Use AI to Defend Against AI-Powered Attacks?

As seen on the previous page, many companies are using AI in their cybersecurity function. But how prepared are they to defend against bad actors who are launching volumetric attacks with AI automation? The answer is concerning: Only a few—approximately 1 out of 5—enterprises are "very well prepared." AI's great contribution is efficiency and productivity. As part one reveals, AI-powered bots are becoming the tool of choice for scammers so that they can launch hard-to-detect ATO, MFA compromise, SMS toll fraud, etc. Over the past two years, a large majority of companies has seen AI-powered bots as a source for attacks increase by 36%.

Level of Preparedness for Using AI to Defend Against Bad Actors Conducting Volumetric AI-Powered Attacks

Total (n=188)



	Finance (n=69)	Technology Platforms (n=33)	Travel/ Hospitality (n=35)	Social Platforms /Networking (n=21)	Sharing/ Gig Economy (n=19)	Streaming Services (n=11)
Not Prepared at All	0%	0%	3%	0%	0%	0%
Somewhat Prepared	19%	15%	34%	14%	16%	36%
Moderately Well Prepared	54%	55%	46%	76%	68%	55%
Very Well Prepared	28%	30%	17%	10%	16%	9%

Chart 2 and Table 2 Q: And how prepared would you rate your company in terms of using AI to defend against bad actors using volumetric attacks using AI-powered bots? (SELECT ONE)

Most enterprises feel moderately well-prepared to counter AI-powered attacks with AI defenses, but maturity levels vary across industries. For example, respondents from the airline sector expressed the lowest confidence, with some even indicating they are "not prepared at all" (14%) to use AI in defending against AI-powered attacks.

This gap in readiness is a red flag for industries that are prime targets for adversaries. As AI-powered attacks become more sophisticated, enterprises need to be more than just "moderately" prepared—they need to achieve a higher level of AI maturity to stay ahead of adversarial tactics.

For the full breakdown of industry-specific data, see the Appendix.

> "The commercialization of phishing is driven by demand, and the value of these services rise as more consumers fall victim to their effectiveness. PHaaS developers who sell their wares to underlying attackers and scammers have adapted their business models to focus on product-market fit, offering highly efficient tools to compromise MFA. Enterprises are searching for answers, looking to understand the real economic drivers and technical mechanics behind this surge to effectively stop it at the point when the consumer starts to login into their account or sign-up for an account." **Arkose Labs CFO Frank Teruel**

AI's Impact: The Benefits Are Already Clear

AI-powered solutions are delivering some tangible results for cybersecurity teams. The top benefit already realized across industry is improved threat intelligence gathering (46%).

In the financial services sector, 49% of banks and fintechs report improved threat intelligence, while 48% say they are better equipped to defend against generative AI-powered attacks. This is especially significant as the financial services sector is often the primary target of cybercriminals who test new attack methods on less secure industries before deploying them on banks and fintechs.

Benefits of AI-Powered Bot Management and Account Security Solutions

Already Realized Benefits

Total (n=188)

	Finance (n=69)	Technology Platforms (n=33)	Travel/ Hospitality (n=35)	Social Platforms/ Networking (n=21)	Sharing/ Gig Economy (n=19)	Streaming Services (n=11)
Improve threat intelligence gathering	49%	64%	31%	33%	47%	45%
Better defend against basic bot attacks	35%	61%	46%	52%	47%	45%
Improve threat detection and response	39%	42%	34%	52%	47%	36%
Better defend against AI-powered bot attacks	42%	24%	40%	48%	37%	73%
Better defend against human fraud farm attacks	35%	42%	43%	57%	32%	45%
Better defend against generative AI-powered attacks	48%	39%	31%	29%	32%	36%
Reduce overall cost of securing my business	36%	30%	49%	43%	32%	45%

Top 3 realized benefits for each industry highlighted

Chart 3 and Table 3 Q: What benefits have you realized (or expect to realize in the near future) from AI-powered bot management and account security solutions? (RANDOMIZE; RATE EACH ROW)

Airlines and hotels are also reaping the benefits. 43% of airlines and 50% of hotels have seen a reduction in the overall cost of securing their operations thanks to AI. More notably, 57% of airlines report enhanced defenses against human fraud farm attacks—an area of concern particularly in industries with high levels of customer loyalty programs, which are often prime targets for fraudsters.

The streaming services industry stands out. Respondents reported they have upped their game by using AI-powered solutions to defend against AI-powered bot attacks (73%).

These benefits underscore AI's ability to address immediate and long-term cybersecurity challenges. Enterprises are not only seeing improvements in threat detection and mitigation, but they are also realizing cost efficiencies, which is critical as cybersecurity budgets grow but need to be justified.

For the full breakdown of industry-specific data, see the Appendix.

Future Benefits of AI in Cybersecurity: What to Expect

Looking ahead, cybersecurity professionals are bullish on AI's ability to deliver even more substantial benefits. 46% of respondents expect AI to drive down overall security costs during the next two years. Another interesting finding is that 45% of the total respondents are eager for AI to help them address attacks deployed by human fraud farms. These are account takeovers, MFA compromise, SMS toll fraud, etc. that can be manual and low-and-slow compared to volumetric AI-powered bot attacks but equally dangerous.

Benefits of AI-Powered Bot Management and Account Security Solutions

Expected Benefits

Total (n=188)

	Finance (n=69)	Technology Platforms (n=33)	Travel/ Hospitality (n=35)	Social Platforms/ Networking (n=21)	Sharing/ Gig Economy (n=19)	Streaming Services (n=11)
Reduce overall cost of securing my business	49%	61%	37%	29%	42%	45%
Better defend against human fraud farm attacks	55%	39%	46%	29%	58%	9%
Better defend against AI-powered bot attacks	41%	64%	54%	33%	37%	18%
Improve theat detection and response	43%	39%	49%	38%	47%	45%
Better defend against generative AI-powered attacks	43%	30%	51%	48%	26%	64%
Improve threat intelligence gathering	39%	24%	54%	43%	42%	45%
Better defend against basic bot attacks	45%	33%	40%	33%	53%	27%

Top 3 expected benefits for each industry highlighted

Chart 4 and Table 4 Q: What benefits have you realized (or expect to realize in the near future) from AI-powered bot management and account security solutions? (RANDOMIZE; RATE EACH ROW)

The industry-specific breakout reveals: 52% of banks and 59% of fintechs expect AI to help reduce human fraud farm attacks, while 64% of technology respondents anticipate improved defenses against AI-powered bot attacks. And 64% of streaming services companies expect AI-powered bot management and account security solutions to help defend against generative AI attacks. Airlines and hotels expect to see improved threat intelligence gathering and defense against AI-powered bot attacks, which makes sense. The travel and hospitality industry has done a great job of driving credit card fraud to near zero. The fraudsters pivoted and are investing in automated tools, like bots, to deliver account takeovers.

"The AI we're using today is the worst AI there ever will be." That bold assertion from Deutsche Bank Research Analyst Adrian Cox captures the moment: AI capabilities—and our mastery of them—will only advance from here. Yet, as AI improves, so will the sophistication of those who exploit it for fraud.

The optimism around AI's future impact reflects a growing belief that as AI matures, it will become more adept at addressing the nuances of different types of attacks, from fraud farms to sophisticated AI-driven threats like deepfakes and GPT prompt compromises. Financial services, in particular, are investing heavily in AI to defend against these generative AI-powered attacks, as these industries have the most to lose if their defenses fail.

For the full breakdown of industry-specific data, see the Appendix.

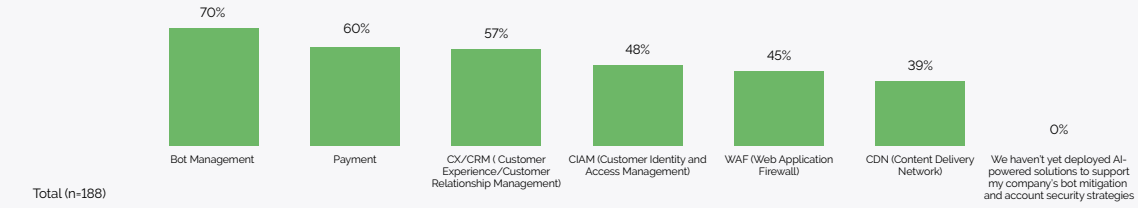
Key Areas of AI Utilization in Bot Mitigation and Account Security

AI-powered solutions are increasingly central to cybersecurity strategies in B2C environments. Currently, AI is most prominently used for bot management (70%), payment security (60%) and customer experience management (57%)—each a cornerstone of the digital consumer journey. For financial services, social media and technology, AI is invaluable in managing vast transaction volumes and safeguarding sensitive data. Nearly half of surveyed enterprises have implemented AI-driven customer identity and access management (CIAM), an area ripe for expansion as adversarial AI reshapes digital identity.

A new challenge facing cybersecurity leaders is redefining digital identity for an era where voice and video can be convincingly deepfaked. In a recent experiment, a financial services CISO used a deepfake of himself alongside his real video, tasking his global and executive teams with identifying the fake. Most participants, including seasoned cybersecurity professionals, misidentified the videos, underscoring the urgent need for sophisticated tools that are resistant to all forms of adversarial AI. For cybersecurity executives, this highlights how difficult it already is in distinguishing authentic from bot and synthetic identities.

The striking takeaway here is that none of the companies surveyed reported a lack of AI deployment for bot mitigation or account security, suggesting that AI has transitioned from a "nice-to-have" to a fundamental tool against cyber threats. But AI's utility isn't just in today's fight—it's about preparing for the future. As cybercriminals increasingly leverage AI to automate and scale their attacks, enterprises must stay ahead by continually evolving the maturity of their AI defenses.

Areas Utilizing AI-Powered Solutions to Support Bot Mitigation and Account Security Strategies



	Total (n=188)	Bot Management	Payment	CX/CRM (Customer Experience/Customer Relationship Management)	CIAM (Customer Identity and Access Management)	WAF (Web Application Firewall)	CDN (Content Delivery Network)	We haven't yet deployed AI-powered solutions to support my company's bot mitigation and account security strategies
Finance (n=69)		80%	67%	46%	42%	43%	35%	0%
Technology Platforms (n=33)		70%	61%	55%	42%	52%	39%	0%
Travel/ Hospitality (n=35)		57%	54%	74%	51%	34%	34%	0%
Social Platforms/ Networking (n=21)		76%	52%	57%	57%	48%	48%	0%
Sharing/ Gig Economy (n=19)		42%	53%	68%	68%	47%	53%	0%
Streaming Services (n=11)		82%	64%	55%	45%	64%	36%	0%

Chart 5 and Table 5 Q: And where exactly are you utilizing AI-powered solutions to support your company's bot mitigation and account security strategies? (RANDOMIZE LIST, SELECT ALL THAT APPLY)

"Customer identity or CIAM has risen to top-of-mind for financial institution (FI) business leaders and CISOs," shared **John Horn, cybersecurity practice director at Datos Insights**. "As FIs enter 2025, our research highlights the urgent business needs for a new breed of CIAM solutions, which include robust bot management and threat intelligence, to reduce account takeovers, improve fraud detection rates and increase cyber resilience."

Budgeting for AI: Investments Are on the Rise

A September 2024 survey by Datos Insights found that 55% of financial services CISOs are very concerned about AI as a risk factor for 2025—up sharply from 26% a year ago. This heightened awareness perhaps is driving the corresponding increase in AI-focused cybersecurity investments.

Spending on AI in cybersecurity is set to surge. Currently, 21% of cybersecurity budgets are allocated to AI-driven solutions. By 2026, this figure is expected to rise to 27%, reflecting growing confidence in AI's ability to combat evolving threats. While this increase may seem incremental, it signifies a strategic shift toward AI as a long-term investment rather than a quick fix.

Approximate % of cybersecurity budget spent on security solutions leveraging AI **21%**

Approximate % of cybersecurity budget expected to be spent on security solutions leveraging AI two years from now **27%**

Q: Approximately what percentage of your overall cybersecurity budget is spent on security solutions leveraging AI? An approximation is fine for this response.

Q: And approximately what percentage of your overall cybersecurity budget do you estimate will be spent on security solutions leveraging AI 2 years from now? An approximation is fine for this response.

Enterprises are clearly recognizing AI's potential, and the projected budget growth indicates a fundamental change in how businesses perceive risk. As attackers become more sophisticated, executives are realizing that traditional security methods are no longer enough. AI is increasingly seen as a critical differentiator in an enterprise's ability to outpace adversaries, not just react to them.

Industry-Specific Challenges: Not All AI Adoption Is Equal

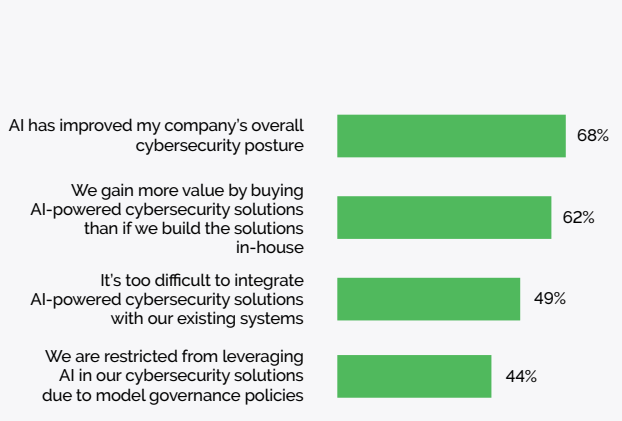
We wanted to get a sense of the current thinking around defensive AI adoption and how it's going so far. Here's what we found: 68% of respondents agree that AI has improved their company's overall cybersecurity posture, and 62% agree that they gain more value through buying AI-powered cybersecurity solutions than building in-house solutions. This finding is extremely important.

Adversaries have at least a two-year jump on using AI-powered tools to perpetrate attack types such as ATO, MFA compromise through reverse-proxy phishing, SMS toll fraud, etc. Enterprises can accelerate their use of defensive AI by partnering with innovative solution providers that already have battle-tested AI-resistant products in the marketplace. Also, solutions that are low or no-code enable enterprises to integrate faster foregoing the need to schedule and wait for engineering resources to become available for their project.

Agreement With AI-Related Cybersecurity Statements

(Agree/Completely Agree)

Total (n=188)



	Finance (n=69)	Technology Platforms (n=33)	Travel/ Hospitality (n=35)	Social Platforms/ Networking (n=21)	Sharing/ Gig Economy (n=19)	Streaming Services (n=11)
AI has improved my company's overall cybersecurity posture	74%	67%	66%	62%	63%	55%
We gain more value by buying AI-powered cybersecurity solutions than if we build the solutions in-house	61%	70%	63%	57%	53%	73%
It's too difficult to integrate AI-powered cybersecurity solutions with our existing systems	46%	39%	54%	67%	47%	45%
We are restricted from leveraging AI in our cybersecurity solutions due to model governance policies	42%	39%	40%	57%	53%	36%

Chart 6 and Table 6 Q: And how much do you agree with each of the following AI-related cybersecurity statements… (RANDOMIZE; RATE EACH)

Despite AI's growing importance, its adoption is not without hurdles, particularly in highly regulated industries like banking. Of bank respondents, 45% reported restrictions on using AI in cybersecurity models due to strict model governance requirements. This challenge highlights a tension between innovation and compliance. Banks are usually not early adopters of security technology, because regulatory frameworks designed to ensure safety in some cases inhibit rapid AI deployment.

Interestingly, 43% of airlines and 57% of hotels indicated difficulty in integrating AI into their existing infrastructure—a testament to the operational complexity and legacy systems prevalent in those industries. It should be noted that 73% of streaming services, 71% of airlines and 61% of hotels said that they gain more value from buying AI solutions than building them in-house. Hotel and airline industry expert Chris Staab, founder of the Loyalty Security Alliance, offered his opinion on this finding:

> "The problem with building in-house AI security solutions is, if I'm an airline, my job is carrying people from point A to point B and in airline-speak, it's 'butts on seats.' So if I'm building AI cyber and fraud tools, I'm not focusing on butts on seats. And then I have to maintain this technology if I decide to build it. And then am I going to pay enough versus a technology company to keep the staff to keep AI technologies on the cutting edge? Probably not."

These findings emphasize that while AI is seen as essential, a one-size-fits-all approach isn't the answer. Different industries face unique challenges in deploying and integrating AI, and this needs to be factored into their cybersecurity strategies. Forward-thinking cybersecurity executives will need to navigate the regulatory and operational roadblocks to unlock AI's full potential.

For the full breakdown of industry-specific data, see the Appendix.

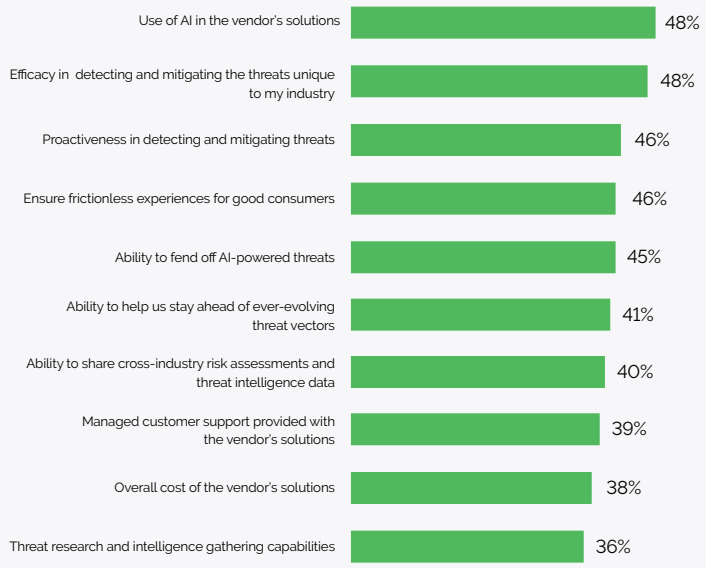
Enterprises' Expectations of Vendors Are Shifting

As enterprises ramp up their AI use, they are also raising the bar for their cybersecurity vendors. 51% of financial services expect vendors to fend off AI-powered threats, 67% of technology companies prioritize vendors that use AI to ensure frictionless consumer experiences and 57% of social media/networking companies expect their vendors to add value through hunting, analyzing and sharing threat intelligence. Across all sectors, there's a clear demand for vendors who can proactively detect and mitigate threats, proving that AI's integration into vendor solutions is no longer optional—it's expected.

For cybersecurity leaders, it's not just about choosing a partner with the best technology; it's about finding one that with domain as well as industry experience can anticipate industry-specific threats and deliver AI-powered solutions tailored to enterprises' unique challenges.

Important Characteristics for Vendors

Total (n=188)



	Finance (n=69)	Technology Platforms (n=33)	Travel/ Hospitality (n=35)	Social Platforms/ Networking (n=21)	Sharing/ Gig Economy (n=19)	Streaming Services (n=11)
Use of AI in the vendor's solutions	51%	45%	51%	43%	63%	18%
Efficacy in detecting and mitigating the threats unique to my industry	46%	64%	46%	52%	37%	27%
Proactiveness in detecting and mitigating threats	45%	45%	46%	43%	47%	64%
Ensure frictionless experiences for good consumers	43%	67%	37%	24%	58%	45%
Ability to fend off AI-powered threats	54%	52%	37%	29%	53%	18%
Ability to help us stay ahead of ever-evolving threat vectors	46%	45%	37%	38%	26%	36%
Ability to share cross-industry risk assessments and threat intelligence data	36%	42%	49%	38%	37%	45%
Managed customer support provided with the vendor's solutions	35%	42%	51%	38%	32%	27%
Overall cost of the vendor's solutions	45%	39%	26%	48%	16%	45%
Threat research and intelligence gathering capabilities	33%	45%	29%	57%	21%	27%

Top 3 important characteristics for each industry highlighted

Chart 7 and Table 7 Q: When considering a vendor to support your bot management and account security needs, how important are each of the following characteristics... (RANDOMIZE, RATE EACH)

As we look toward the future, AI will continue to be a double-edged sword in cybersecurity: a powerful tool for defenders and attackers. The key to staying ahead is achieving AI maturity—being able to deploy AI solutions and fully integrate them into an enterprise's broader security ecosystem. Enterprises that invest wisely in AI now will be better equipped to fend off the next generation of cyber threats, ensuring they stay secure, agile and resilient in an increasingly hostile digital world.

Conclusion

As AI continues to reshape the cybersecurity landscape, enterprises find themselves in a pivotal moment. The adoption of AI-powered solutions is no longer a future initiative—it's a present necessity. Across industries, enterprises are already experiencing the benefits of AI in bot mitigation, threat intelligence and incident response. Financial services, technology and travel sectors are leveraging AI to not only defend against today's attacks but to anticipate the threats of tomorrow.

However, the path to full AI maturity remains challenging. While budgets for AI are increasing, enterprises still face hurdles in integration, compliance and skills gaps. These challenges highlight the need for greater investment in AI solutions and more strategic planning to ensure that AI can be fully leveraged to defend against increasingly sophisticated attacks.

Enterprises that prioritize AI adoption and prepare their defenses now will be best positioned to navigate this rapidly evolving threat landscape. As cybercriminals continue to scale their AI-powered operations, the race to achieve AI maturity is more critical than ever. Enterprises that invest in AI today will not only strengthen their current defenses but also future-proof their cybersecurity strategies.

Best Practices for Bolstering Your Defenses Against AI-Powered Attacks, by Use Case

Implementing preemptive defenses at the consumer level is crucial for enhancing security, enabling your business to proactively detect and mitigate risk. Below are best practices for consideration and conversation.

Use Case	Best Practice 1	Best Practice 2
Account takeover/ credential stuffing	Use a blend of real-time, dynamic, previously unseen challenges—both visible and non-visible—to validate user authenticity and enable good user throughput.	Leverage AI-resistant challenges that cannot be detected by adversarial AI tools.
MFA compromise	Enable real-time identification of reverse-proxy phishing sites during consumer login.	Activate real-time alerts to enable immediate fraud mitigation as incidents occur.
Generative AI threats	Ensure robust detection and mitigation are in place around bad bots and all types of scrapers.	Identify reverse-proxy phishing sites that attempt to bypass geographical restrictions and impersonate legitimate users.
SMS toll fraud	Leverage detection that can quickly flag registration abandonment.	Establish baseline benchmarks for normal SMS spending and rapidly measure and analyze these metrics.

Recommendations

1. Focus first on the top threats that are putting enterprises most at risk: ATO/credential stuffing, fake account creation and generative AI. Stop potential fraud at the beginning of the consumer experience: sign-up and sign-in.
2. Challenge any workflows that bypass security measures, as they can create vulnerabilities, and incorporate dynamic elements to prevent AI models from adapting or learning from them. Regularly revisit these processes to ensure they align with your security protocols.
3. Prioritize and leverage solution providers who provide cross-industry risk signals that you can leverage to tune your internal cyber risk and fraud AI models.
4. Enhance your approach to accounts that are linked (e.g., linked bank accounts, linked loyalty accounts) by implementing rigorous verification processes. When linking accounts, always challenge the originating account to mitigate risks of fraud, particularly from new or unverified accounts, with a blend of dynamic, visible and non-visible challenges to foil adversarial AI.
5. Conduct due diligence to ensure your partners have the necessary skills to combat emerging threats and keep you well informed on emerging attack shifts by providing risk signals and threat intelligence that cover the fastest growing attack sources, AI-powered bots and human fraud farms.
6. Reduce AI risks and downstream costs by partnering with a vendor that has successful deployments of AI–resistant solutions at enterprises you consider your peers.
7. Touch base with your team regularly to understand the stress levels they are experiencing due to the rise in AI threats on your company.
8. Prioritize the use of third–party solutions over homegrown solutions, given most organizations will most likely not be able to build solutions that are able to surpass the two-year+ head start most bad actors already have and stay at the cutting edge of generative AI-powered attacks.

> "We are at the forefront of an AI-empowered world, but we must work together to outmatch our adversaries."
> **Tom Burt, Corporate Vice President, Customer Security & Trust, Microsoft**

Methodology

The new research "The Intersection of AI, Online Fraud and Cyber Defenses" assesses market awareness and strategic deployment of AI in defensive and offensive applications. It focuses on key sectors such as financial services (banks and fintechs), social media, streaming services, sharing/gig economy, travel and hospitality (airlines and hotels) and large technology platforms. The research examines how enterprises are using AI to enhance security protocols and counter emerging threats, as well as how they are experiencing bad actors deploying AI, including bots and fraud farms, to carry out cyberattacks and online fraud.

Survey Design and Execution

A 15-minute, close-ended online survey was conducted from September 3 to 23, 2024, targeting 188 U.S.-based cybersecurity professionals. The sample pool focused on enterprise-sized companies, with 80% of respondents working at firms where annual revenue ranged between $500 million to $10 billion or more. Participants included 54% executives (C-suite and VP-level) and 46% directors/managers, ensuring a mix of strategic and operational insights.

The primary goals of this research are to:

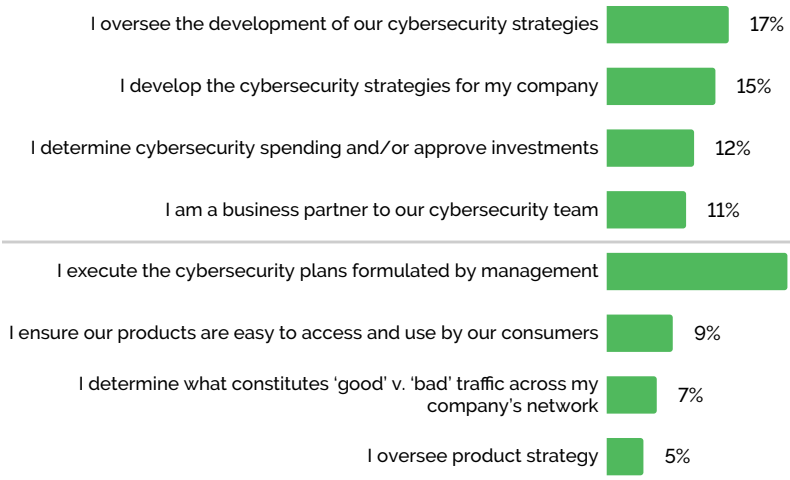
- Provide data-driven insights to assess the maturity of AI adoption in defensive cybersecurity measures.
- Gauge awareness of threats posed by malicious actors.
- Identify gaps and opportunities in enterprises' AI maturity.
- Identify best practices and actions companies are using today.
- Recommend mitigants to AI-powered risks and threats.

Demographics

Details of the professionals who participated in the research project.

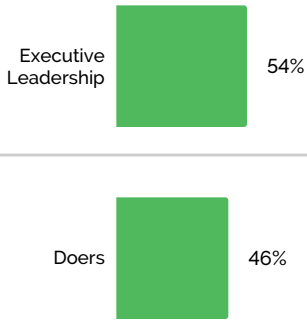
Responsibility for Cybersecurity-Based Activity

Total (n=188)



Leadership Category

Total (n=188)

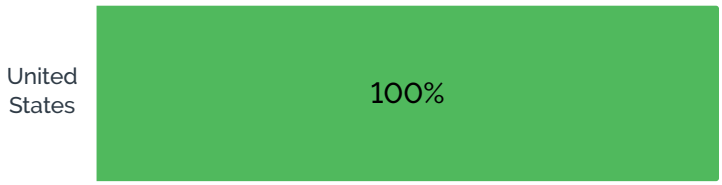


Firmographics

Details of the enterprises that participated in the research project.

Country

Total (n=188)



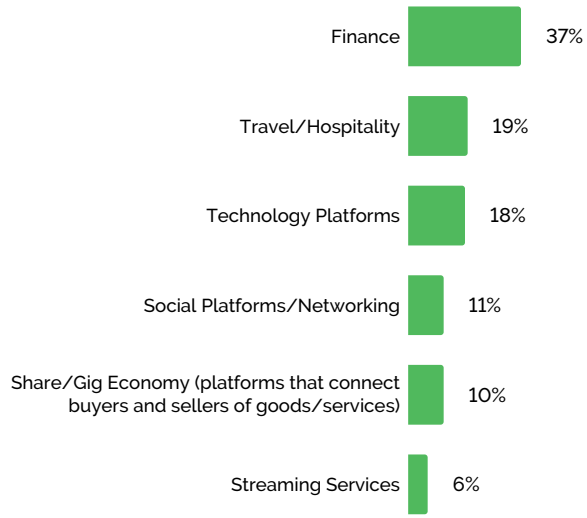
Average Percentage of Consumer vs. Business Customers

Total (n=188)

Consumer customers	72%
Business customers	28%

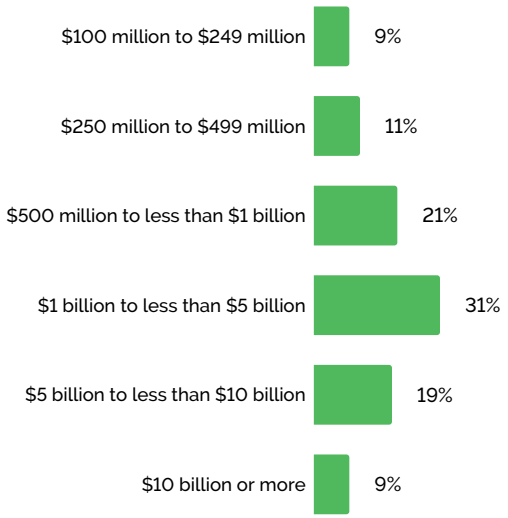
Industry

Total (n=188)



Revenue

Total (n=188)



Contact

Patrick Kehoe
CMO
Arkose Labs
p.kehoe@arkoselabs.com

Frank Teruel
CFO
Arkose Labs
f.teruel@arkoselabs.com

Vikas Shetty
Head of Product
Arkose Labs
v.shetty@arkoselabs.com

Arkose Labs' Locations

USA

400 Concar Dr, Fl 4
San Mateo CA. 94403

Australia

T.C. Beirne Building, 315
Brunswick Street (level 4),
Fortitude Valley, Brisbane
QLD 4006

United Kingdom

167-169 Great Portland
Street, 5th Floor, London,
W1W 5PF

Costa Rica

WeWork c/o Alina Mora
Calle 118B San Rafael
San José, SJ 1020

India

Redbrick Offices,
Tower B 2nd Floor,
Panchshil Business Park
Balewadi High Street, Off,
Baner – Balewadi Rd,
Pune, Maharashtra 411045

Argentina

Avenida Corrientes 800,
Buenos Aires,
Buenos Aires C1008

BOOK YOUR DEMO

Arkoselabs.com

Appendix

Industry Data Tables

This appendix presents essential tables that provide detailed industry insights into the survey data discussed throughout part two.

Table 8 is an expansion of Chart 1 and Table 1 and expands on the specific actions enterprises are taking to leverage AI in their cybersecurity strategies.

	Total	Sector							
	Total	Banks	Fintechs	Social Media/ Networking	Technology Platforms	Airlines	Hotels	Sharing/Gig Economy	Streaming Services
Total	188	42	27	21	33	7	28	19	11
Using AI to analyze historical data and identify vulnerabilities	69%	69%	63%	67%	76%	86%	71%	68%	45%
Using AI to predict future security threats	69%	67%	74%	71%	67%	86%	68%	68%	64%
Automating processes with AI to reduce manual tasks	62%	69%	78%	43%	67%	71%	50%	68%	36%
Leveraging AI to enable faster response time to security incidents	71%	79%	78%	52%	76%	57%	75%	74%	45%
Deploying AI tools to continuously monitor infrastructure	63%	67%	67%	67%	67%	57%	54%	68%	45%
Analyzing cybersecurity data in real time with AI tools	69%	74%	85%	48%	61%	71%	68%	68%	73%

Table 9 is an expansion of Chart 2 and Table 2 and expands on the preparedness of companies using AI to defend against volumetric, AI-powered attacks.

	Total	Sector							
	Total	Banks	Fintechs	Social Media/ Networking	Technology Platforms	Airlines	Hotels	Sharing/Gig Economy	Streaming Services
Total	188	42	27	21	33	7	28	19	11
Not prepared at all	1%	0%	0%	0%	0%	14%	0%	0%	0%
Somewhat prepared	21%	17%	22%	14%	15%	0%	43%	16%	36%
Moderately well prepared	56%	57%	48%	76%	55%	71%	39%	68%	55%
Very well prepared	22%	26%	30%	10%	30%	14%	18%	16%	9%

Table 10 is an expansion of Chart 3 and Table 3 and expands on industry breakdown of the benefits that enterprises have already experienced deploying defensive AI.

Already Realized Benefits	Total	Sector							
	Total	Banks	Fintechs	Social Media/ Networking	Technology Platforms	Airlines	Hotels	Sharing/Gig Economy	Streaming Services
Total	188	42	27	21	33	7	28	19	11
Improve threat detection and response	41%	36%	44%	52%	42%	14%	39%	47%	36%
Improve threat intelligence gathering	46%	45%	56%	33%	64%	29%	32%	47%	45%
Reduce overall cost of securing my business	38%	38%	33%	43%	30%	43%	50%	32%	45%
Better defend against basic bot attacks	45%	36%	33%	52%	61%	43%	46%	47%	45%
Better defend against AI-powered bot attacks	40%	43%	41%	48%	24%	43%	39%	37%	73%
Better defend against generative AI-powered attacks	39%	48%	48%	29%	39%	29%	32%	32%	36%
Better defend against human fraud farm attacks	40%	38%	30%	57%	42%	57%	39%	32%	45%

Table 11 is an expansion of Chart 4 and Table 4 and reveals the industry breakdown of the expected benefits that enterprises anticipate realizing in the future by deploying defensive AI.

Expected Benefits	Total	Sector							
	Total	Banks	Fintechs	Social Media/ Networking	Technology Platforms	Airlines	Hotels	Sharing/Gig Economy	Streaming Services
Total	188	42	27	21	33	7	28	19	11
Improve threat detection and response	44%	50%	33%	38%	39%	71%	43%	47%	45%
Improve threat intelligence gathering	40%	40%	37%	43%	24%	71%	50%	42%	45%
Reduce overall cost of securing my business	46%	50%	48%	29%	61%	29%	39%	42%	45%
Better defend against basic bot attacks	40%	43%	48%	33%	33%	43%	39%	53%	27%
Better defend against AI-powered bot attacks	45%	40%	41%	33%	64%	57%	54%	37%	18%
Better defend against generative AI-powered attacks	43%	40%	48%	48%	30%	71%	46%	26%	64%
Better defend against human fraud farm attacks	45%	52%	59%	29%	39%	29%	50%	58%	9%

Table 12 is an expansion of Chart 6 and Table 6 and reveals the industry breakdown of the opportunities and struggles enterprises face when embracing AI.

Top 2 boxes ("Agree/Completely agree")	Total	Sector							
	Total	Banks	Fintechs	Social Media/ Networking	Technology Platforms	Airlines	Hotels	Sharing/Gig Economy	Streaming Services
Total	188	42	27	21	33	7	28	19	11
AI has improved my company's overall cybersecurity posture	68%	79%	67%	62%	67%	86%	61%	63%	55%
We are restricted from leveraging AI in our cybersecurity solutions due to model governance policies	44%	45%	37%	57%	39%	29%	43%	53%	36%
It's too difficult to integrate AI-powered cybersecurity solutions with our exisiting systems	49%	50%	41%	67%	39%	43%	57%	47%	45%
We gain more value by buying AI-powered cybersecurity solutions than if we build the solutions in-house	62%	62%	59%	57%	70%	71%	61%	53%	73%