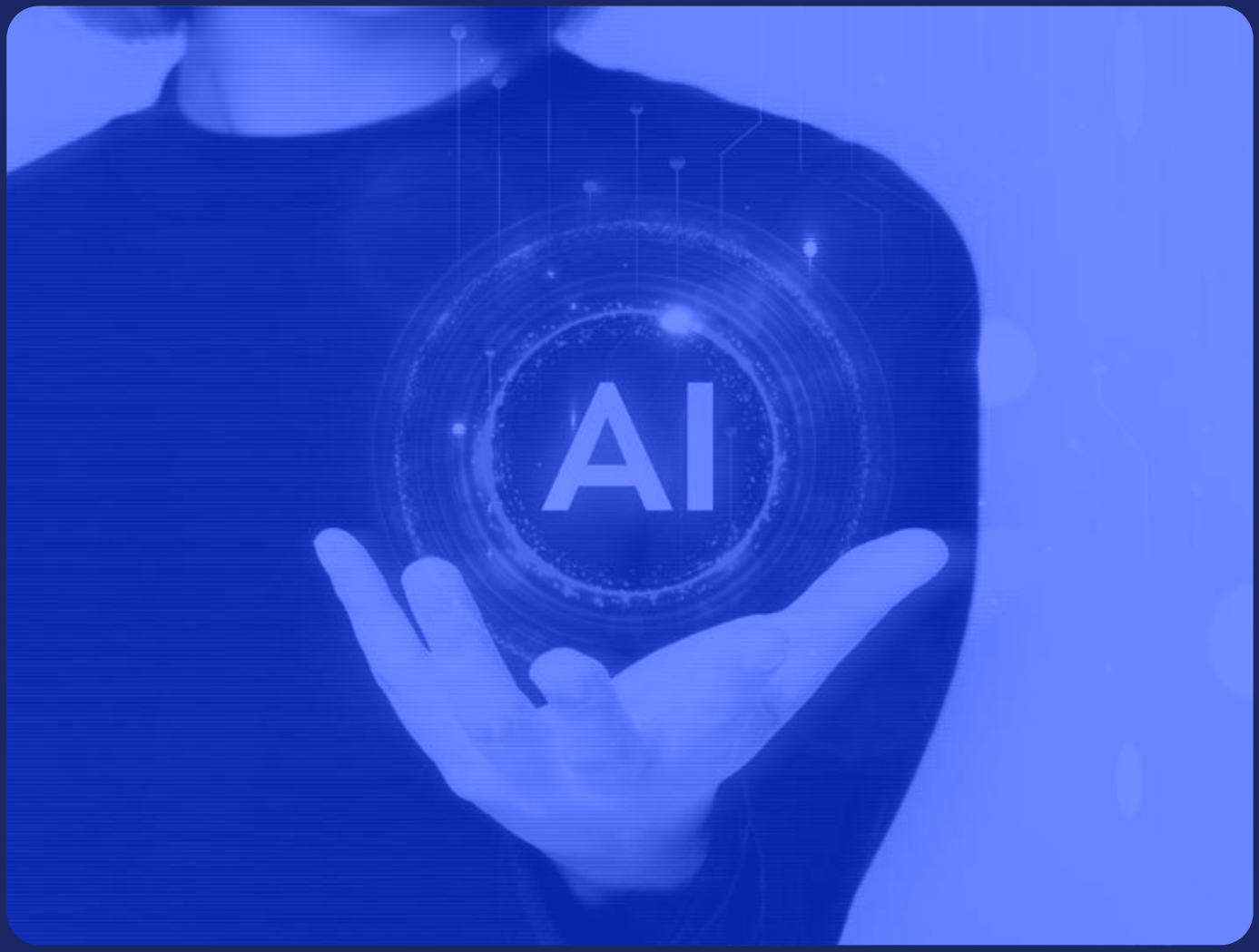
Arkose Labs

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

PART 3: AI ENTHUSIASTS: TRAILBLAZERS TAKING ACTION AGAINST ADVERSARIAL AI



November 2024

Table of Contents

Executive Summary

As cybercriminals turn to AI to orchestrate impactful attacks at scale, companies need to leverage advanced technologies to stop this onslaught of threats and online fraud. When it comes to pivoting fast, attackers often have an advantage over their targets. They can shift tactics and skill up fast, while switching strategies can take longer for some cybersecurity teams at major global corporations. It's a gulf that cybersecurity and anti-fraud executives have to close, and fast.

Part one of our inaugural research The Intersection of AI, Digital Fraud and Cyber Defenses revealed growing alarm over specific attack types like account takeovers—76% of 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 have become the main source of attacks (40%) like ATO. Enterprises are under siege at scale, with 88% of enterprises indicating a significant increase in AI-powered bot attacks since 2022. This swift escalation in the deployment of adversarial AI demands the deployment of solutions that are AI resistant, especially because a majority of enterprises report losing between $10 million and more than $500 million over the past two years.

Part two of the research exposes the specific actions cybersecurity leaders are taking, their AI-driven investments and the tangible gains they're experiencing. 71% of enterprises report leveraging AI to enable faster incident response times, predict future security threats, analyze historical data and analyze cybersecurity data in real-time. Within this environment, 67% of enterprises say they gain more value by partnering rather than trying to build in-house AI-powered defenses. This trend is perhaps driven by the fact that most enterprises do not have nearly enough talent in-house with cybersecurity plus AI skills. On average, enterprises report spending 21% of their cybersecurity budgets today on security solutions leveraging AI, and that by 2026 spend will account for 27%.

It's very early days in terms of AI maturity in cybersecurity for enterprises. Based on our threat intelligence and research, we believe bad actors have a two- to three-year headstart using AI as a main ingredient to scam at scale. And these financially motivated bad actors are aiming at high-value targets, like the biggest banks in the world, tech titans and social media companies, as well as airlines and hotels.

But within these early days, patterns point to pioneers emerging from the data. We've coined this group of trailblazing enterprises "AI Enthusiasts." 25% of respondents fall into this group, which is representative across each industry studied. These are the enterprises that have embraced AI and are already deploying multiple actions to detect and stop attacks, which are driving meaningful positive business outcomes. Why? Because they have to. The data shows that AI Enthusiasts are also the segment that are on the frontlines, facing the highest volume of sophisticated generative AI-powered attacks.

Highlights distinguishing AI Enthusiasts from the other respondents include:

- AI Enthusiasts are undertaking 3 or more **AI-based actions** to address cybersecurity concerns, especially generative AI threats.
- This elite group is focusing on and realizing the benefits of AI solutions in key areas—**improved threat intelligence (58%), buoyed threat detection and response (46%) and reduced cost of securing the business (48%).**
- They are **3.5x** more likely to be "very well prepared" to defend against volumetric attacks compared to their peers.
- AI Enthusiasts are more likely to recognize the **sophisticated (81%) and frequent (75%)** cyber threats posed by generative AI.

In this third and final part of the research we are uncovering the strategic moves that AI Enthusiasts are making, examining what we can learn from them and identifying areas for further research. The responses we received reveal the blueprint for enterprises that want to be ready to fight back against AI-equipped attackers, and prepare for tomorrow's cybersecurity challenges, today.

We're excited to share these insights to engage you in the conversation. We invite you to set up one-on-one meetings with us to discuss your experiences so far on the AI journey.

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

Defining Cybersecurity AI Enthusiasts

AI Enthusiasts are not just fans of new technology—they're warriors in the cybersecurity trenches, deploying AI as sword and shield to detect and stop online fraud and protect their business operations and consumers' digital transactions.

While many enterprises are still getting started with AI-powered cybersecurity, AI Enthusiasts are embedding it into the DNA of their cybersecurity and anti-fraud operations. Already, they are using AI to ensure consumer account integrity as well as detect and mitigate bots and human fraud farms. This select group is poised to

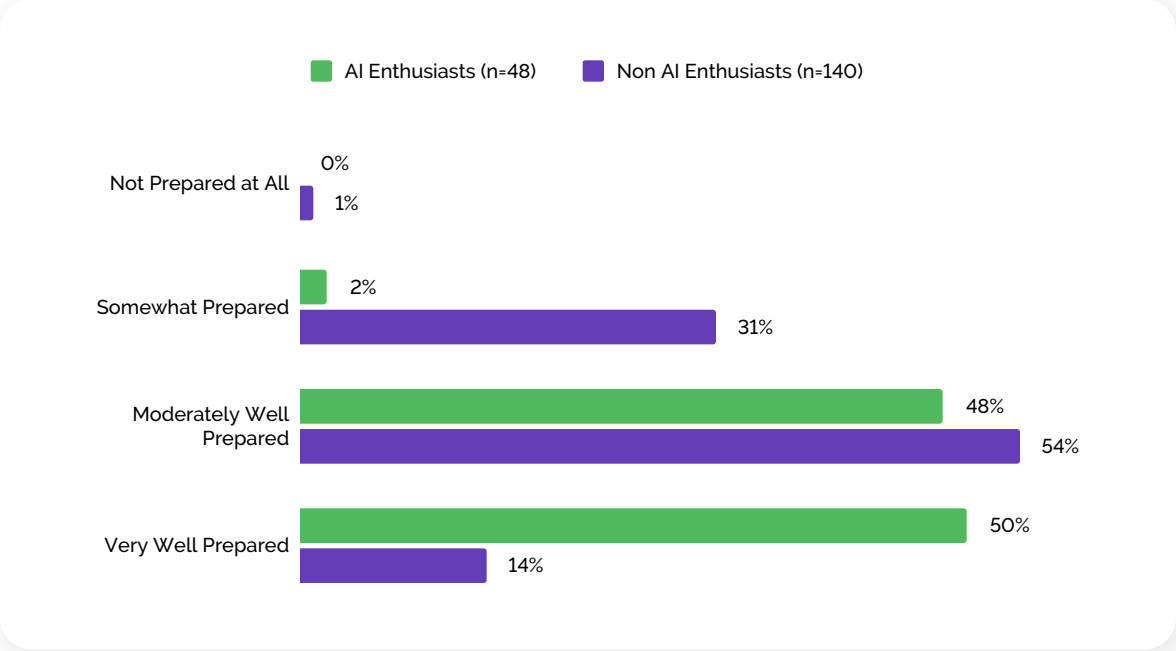
outpace adversaries, with strong threat intelligence, fast response times and efficient security operations. Put simply, AI Enthusiasts are not sitting back and watching AI unfold in the cybersecurity space. They're adopting defensive AI early, being among the first to transform their cybersecurity posture by acting on at least three of the following fronts:

- **Digging through historical data:** These enterprises use AI to analyze historical data and identify vulnerabilities.
- **Automating the mundane:** By handing over manual, repetitive tasks to AI, they free up human talent to focus on strategic defenses.
- **Setting 24/7 watchdogs:** Deploying AI tools to continuously monitor their infrastructure means they are quick to identify vulnerabilities, even when human eyes are off the clock.
- **Forecasting the next attack:** Using AI to predict new security threats ahead of time, businesses can stay steps ahead of adversaries.
- **Slashing response times:** AI helps them cut down the lag between detection and action, reducing the window for damage.
- **Crunching real-time data:** They deploy AI to chew through massive volumes of cybersecurity data at lightning speed, spotting threats instantly.

A Proactive Stance Pays Off

AI Enthusiasts are 3.5 times more likely to report that they are very well prepared to defend against AI-driven volumetric attacks, compared with their peers.

Level of Preparedness for Defending Against Bad Actors Conducting Volumetric AI-Powered Attacks



Q: How prepared would you rate your company in terms of defending against bad actors conducting volumetric attacks using AI-powered bots? (SELECT ONE)

But, hang on. We think this finding requires further research. Here's why: Most enterprises are in the early days of working with defensive AI to stop adversarial AI attacks and are still grappling with the scope and speed of the threat changes occurring all around them.

In part one on page 3, we report that a majority of cybersecurity leaders' direct reports and teams feel significant stress due to volumetric AI-powered attacks taking place today and targeting their companies. Adding to that stress is the fact that 50% of AI Enthusiasts indicate they don't have the necessary talent with dual cybersecurity plus AI experience. Institutional workflows pose another obstacle to being "very well prepared"—big banks and airlines, for example, cannot pivot fast enough because they're entrenched in traditional structures and wrapped in heavy regulations.

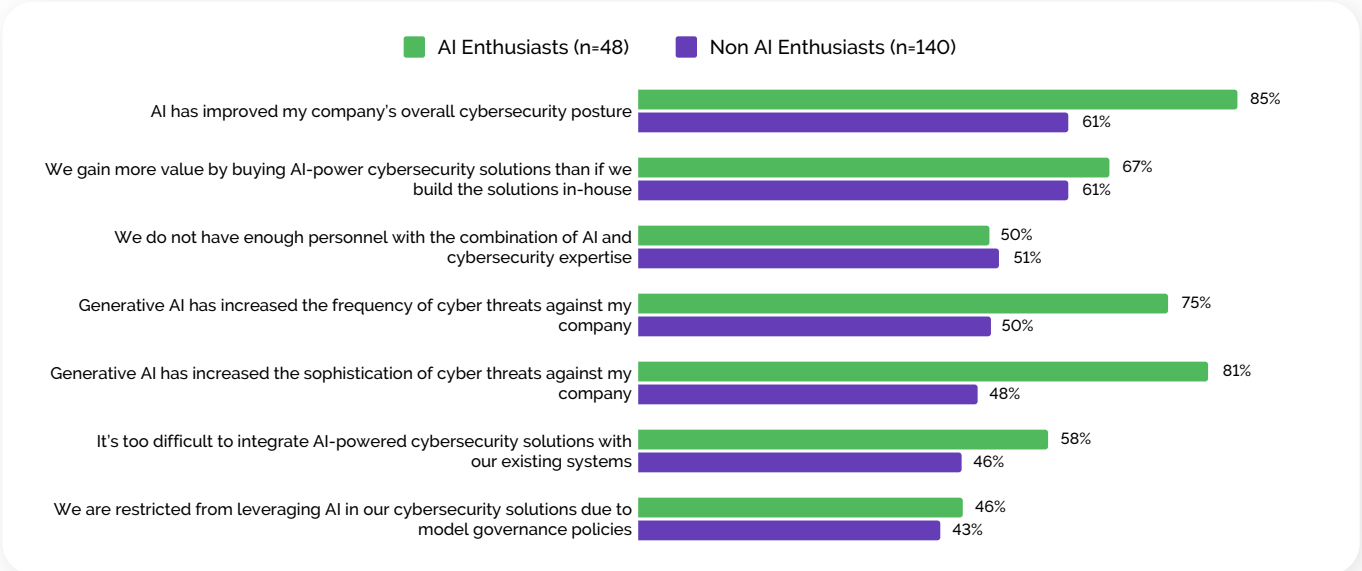
Within that context, the research finding that two-thirds of AI Enthusiasts rely on trusted partners to leverage AI in their defenses is critical. So while some enterprises believe they're protected, in reality, they're highly dependent on their supply chains and vendors. It's still early days. Enterprises that think they're 50% very well prepared are probably 100% vulnerable.

AI Enthusiasts remain a cohort that is worthy of understanding and tracking over time because they're outliers based on the number of actions they are taking and the results they are experiencing. They are a rare breed. Only 26% of the enterprises we surveyed fall into the AI Enthusiasts category. The rest? They're playing catch-up in a game that waits for no one.

AI: The Posture Enhancer

Of AI Enthusiasts, 85% say their overall cybersecurity posture has been significantly boosted by AI, compared to 61% of non-AI Enthusiasts. This gap shows a clear and meaningful advantage to getting on board with AI-powered defenses now. It also reflects the efficiency with which AI Enthusiasts are leveraging defensive AI.

Agreement with AI-Related Cybersecurity Statements (Agree/completely agree)



Today's attacks, like account takeovers, fake account creation, MFA compromise, etc. aren't just growing in number, but in innovation and advancement too. Interestingly, generative AI has significantly lowered barriers for malicious actors, enabling them to execute complex attacks by enhancing traditional techniques such as scraping and phishing with advanced AI tools. The progression towards Large Action Models (LAM) and the increasing integration of AI-powered workflows, such as Chat Assistants, have expanded the landscape for potential cyber threats. As enterprises continue migrating core operations to AI-driven platforms, these systems are becoming high-priority targets for sophisticated cyberattacks.

Given that context, 81% of AI Enthusiasts acknowledge that generative AI has increased the sophistication of threats against their enterprises, underscoring their acute awareness of emerging risks. They're also aware that the same tech is powering their adversaries. In fact, AI Enthusiasts (75%) are much more likely to report that generative AI has ratcheted up the frequency of the threats against them. It's a result that points to increased awareness, more so than the other respondents in the research, about the breadth of attacks deployed by fraudsters today, and a heightened vigilance when it comes to stopping them in their tracks. Their ability to defend against sophisticated threats stems partly from leveraging their third-party solution providers (67%) for detection and defense, an approach that likely helps them sidestep internal restrictions and manage resource limitations effectively.

AI Enthusiasts and Revenue Spend

For this analysis we wanted to explore spend as a percentage of revenue for AI Enthusiasts. As we dug into the data, we found that there are not too many differences between the revenue categories and the percent of budget, perhaps indicating that enterprises cannot or don't have to spend their way to better outcomes and that there are other factors at play.

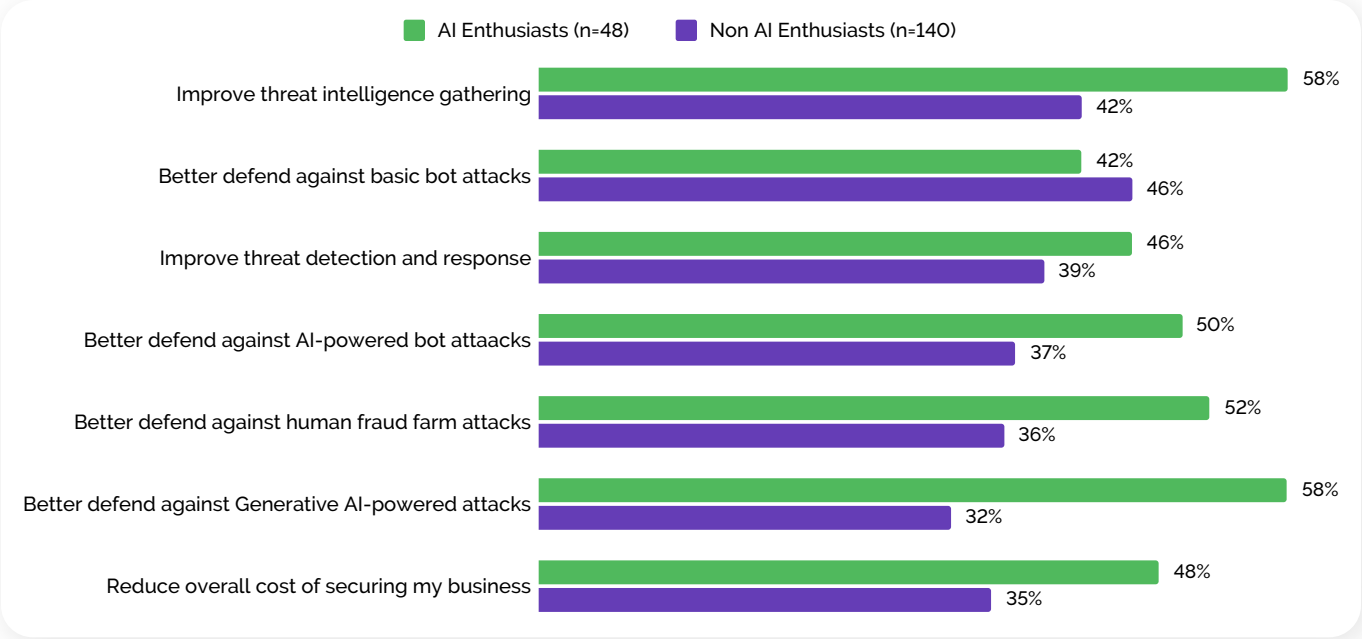
AI Enthusiast Spending on Security Solutions Leveraging AI

Company's Annual Revenue	Percent of overall cybersecurity budget dedicated to security solutions leveraging AI
$100 million to $249 million	28%
$250 million to $499 million	18%
$500 million to less than $1 billion	17%
$1 billion to less than $5 billion	22%
$5 billion to less than $10 billion	17%
$10 billion or more	22%

Benefits AI Enthusiasts Already Are Experiencing

Honing a world class cybersecurity strategy takes investment and resources, but it would be a mistake to assume that the shift toward defensive AI is going to mean increased costs across the board. The AI Enthusiasts are among the companies demonstrating how to cost-effectively battle adversarial AI. AI Enthusiasts are doubling down on improving threat intelligence (58%), which has knock-on effects, like improving threat detection and response (46%). This group was also more likely than peers to report a reduced overall cost of securing their business. The data suggests that AI Enthusiasts are hyper efficient, using defensive AI to streamline processes to reduce the cost of security. This cohort is achieving a goal that most enterprises are striving toward with their AI adoption strategies.

Chart 3: Benefits of AI-Powered Bot Management and Account Security Solutions (Already Realized Benefits)



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 actions they are taking are working. Interestingly, 58% of AI Enthusiasts report that they are better able to defend against generative AI-based attacks, compared to just 32% of their peers. With better defense against AI-powered bot attacks (50%) and human fraud farm attacks (52%) alike, AI Enthusiasts are armed to deal with the most damaging attack sources, distinguishing them from other businesses.

It's a posture that can benefit team members across a cybersecurity department. For a VP of CIAM, for example, the findings underscore the importance of integrating AI into identity management. Throughout 2024, identity has become a crucial factor in improving fraud detection rates.

> "Looking ahead to this coming year, we're witnessing a significant shift in the industry with the rise of generative AI. The majority of online content is increasingly being generated by AI, and that's only going to grow. With this change, the threats we face are becoming more prevalent, and it's our responsibility to protect our clients." **– Technology Lead, Trust and Safety, Tech Industry**

But this isn't traditional identity verification—it's identity reinforced by risk assessments that stem from advanced bot detection and mitigation combined with threat intelligence analytics. With the rise of AI-powered attacks, particularly from sophisticated malicious bots, leveraging this modern, dynamic identity data is essential for robust defense of customer accounts and access points,

Investment in AI can alleviate the burden on team members, enabling them to focus on high-priority threats and strategic initiatives. For a VP of Cybersecurity Engineering, deploying AI will ensure their team is prepared for increasingly sophisticated threats that leverage AI for scale and complexity. And for a VP of Cyber Fraud Fusion, adopting AI tools will enable teams to effectively combat fraud tactics, such as AI-generated synthetic identities that are used to create voluminous fake accounts and automated fraud schemes.

Lessons from AI Enthusiasts

Here's the bottom line: AI Enthusiasts are setting the standard for cybersecurity and digital fraud defenses in the age of AI, and they're not looking back. They are showing that early and strategic AI adoption doesn't just help you keep up—it puts you leagues ahead of bad actors. AI Enthusiasts are already reaping the rewards of superior preparedness, cost efficiency and intelligence-driven defense. For those hesitating to go all-in in deploying AI in their cybersecurity strategies, the gap will only become harder to close. Many enterprises are still on the sidelines or in very early stages, but now is the time to act.

For now, a select number of AI Enthusiasts is writing the playbook on how to defeat today's evolving cybercrime threats. The question is, how many companies will catch up?

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. Prioritized 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

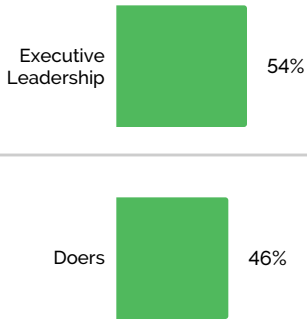
Details of the professionals who participated in the research project.

Responsibility for Cybersecurity-Based Activity

Total (n=188)

Leadership Category

Total (n=188)

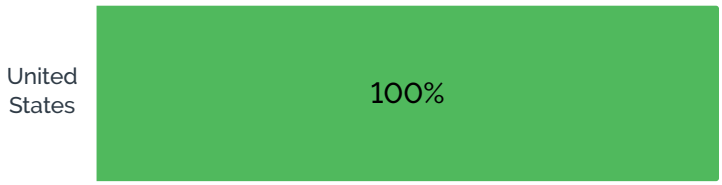


Firmographics

Details of the enterprises that participated in the research project.

Country

Total (n=188)



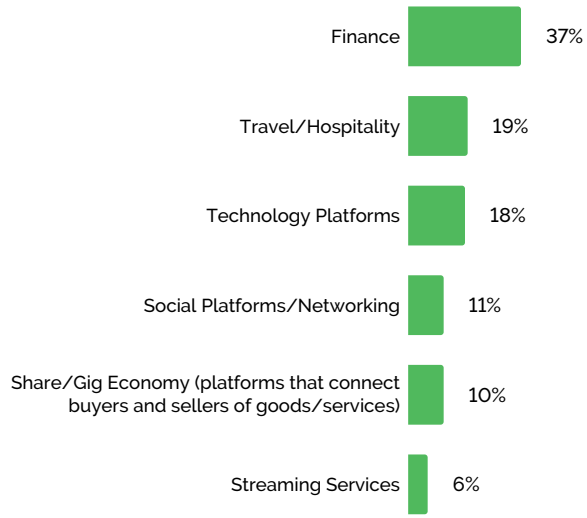
Average Percentage of Consumer vs. Business Customers

Total (n=188)

Consumer customers	72%
Business customers	28%

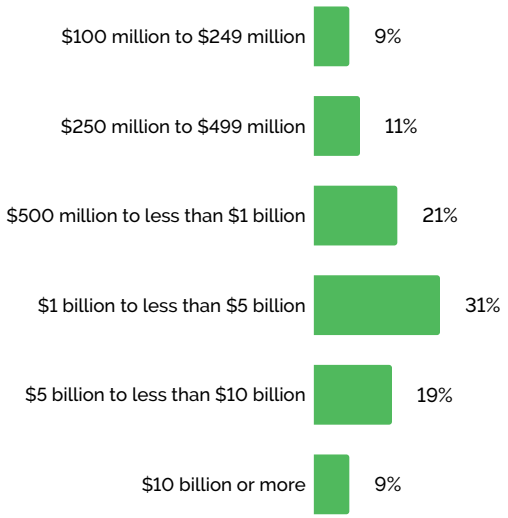
Industry

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

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

For the world's leading brands, Arkose Labs delivers real-time digital risk intelligence to ensure a seamless experience for legitimate users and enhance internal cybersecurity and fraud models. Arkose Labs protects against account takeovers, fake account creation, MFA compromise and other attacks from bots and bad actors before they make impact.

BOOK YOUR DEMO

Arkoselabs.com