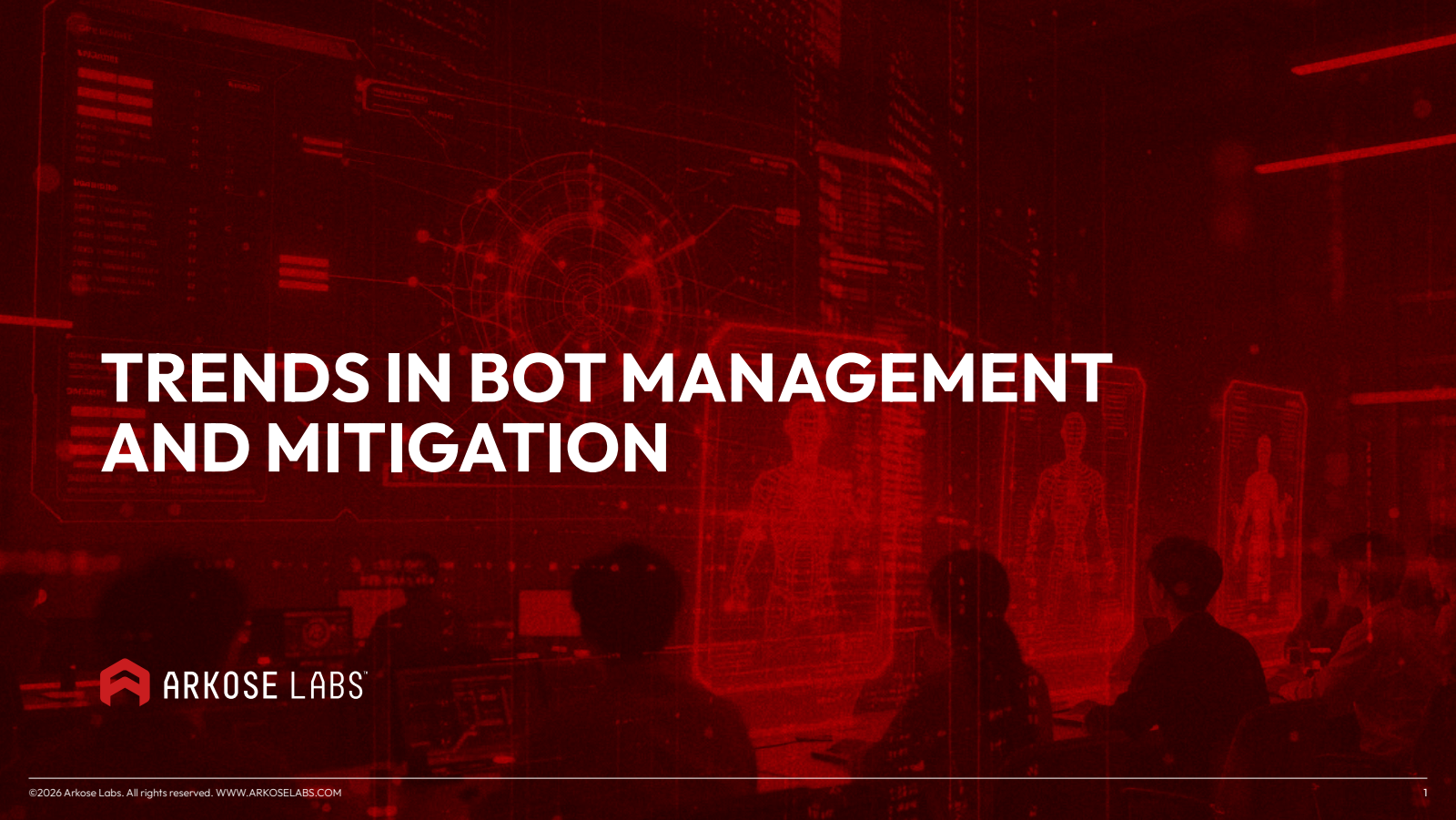
TRENDS IN BOT MANAGEMENT AND MITIGATION



ARKOSE LABS™

INTRODUCTION

Cybercriminals are getting smarter and faster. As bot-driven attacks surge, enterprises must rethink their security strategies or risk falling behind. Brand damage, data theft and revenue loss remain top concerns—fueling deep fears about long-term trust and financial stability.

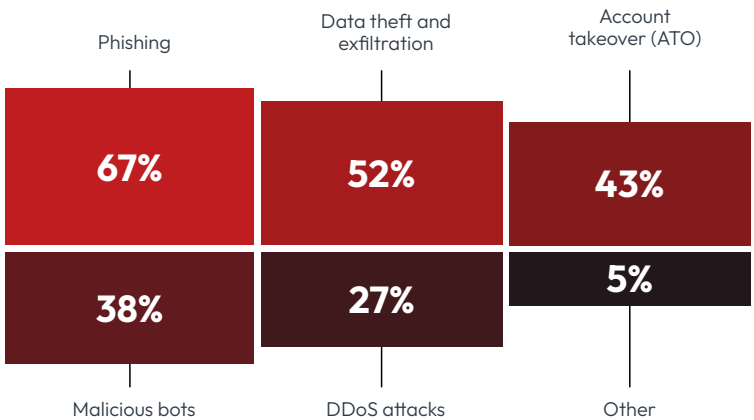
That's a key takeaway from a recent Arkose Labs bot management survey of senior decision-makers. This infobrief explores critical trends uncovered in bot management and mitigation, highlighting the most pressing threats businesses face today and the security strategies decision-makers are prioritizing.

Survey findings highlight escalating risks from fake account creation, account takeovers and SMS toll fraud—reinforcing the need for advanced, adaptive security strategies.

MOST CONCERNING ATTACK TYPES

Executives shared the top cyber threats they face. The results reveal a strong emphasis on identity-based attacks like phishing, data theft and account takeover (ATO).

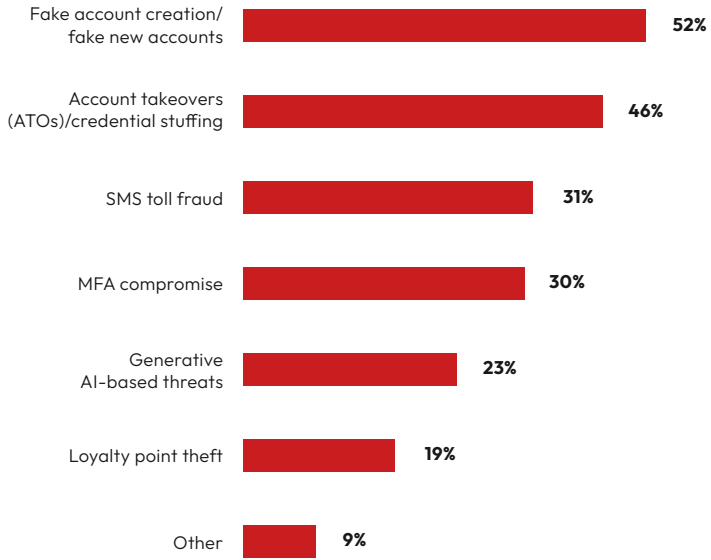
Phishing tops the list, fueled by generative AI that creates flawlessly crafted phishing emails. Meanwhile, ATO underscores rising threats to account security from automated attacks.



BOT-DRIVEN ATTACK THREATS

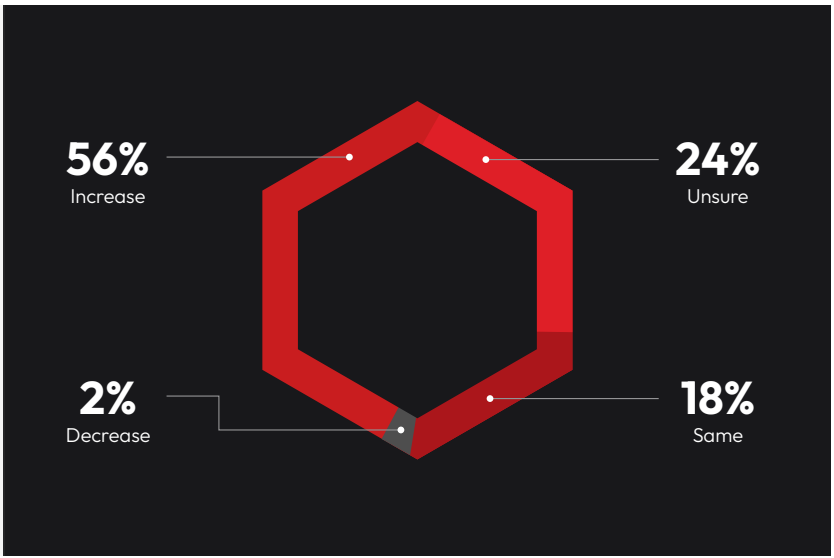
Executives were asked which bot-driven threats they are experiencing the most. Fake account creation and ATO attacks are dominant due to the rise of dark web marketplaces, where attack enablers sell their wares and attack automation services like phishing kits, which can be purchased easily by entry-level cybercriminals.

The growth of AI-powered threats suggests fraudsters are leveraging generative AI to bypass security measures. Additionally, MFA compromise (a reverse proxy phishing attack) signals that attackers are finding ways around traditional authentication methods.



AN INCREASE IN BOT-BASED ATTACKS

Over half (56%) of respondents report that bot-driven attacks have increased over the past year, aligning with broader cybersecurity research showing a surge in automated fraud and AI-driven cybercrime. A notable 24% are unsure, which may indicate visibility challenges in detecting evolving bot threats.



KEY CYBERATTACK IMPACTS

Reputation damage and data theft stand out as top concerns, reinforcing the idea that cybersecurity isn't just about financial loss but also about trust erosion. The fact that compliance issues rank lower suggests that regulatory penalties, while significant, may not be as immediately disruptive as operational downtime or data breaches.

Damage to brand and reputation

Data theft

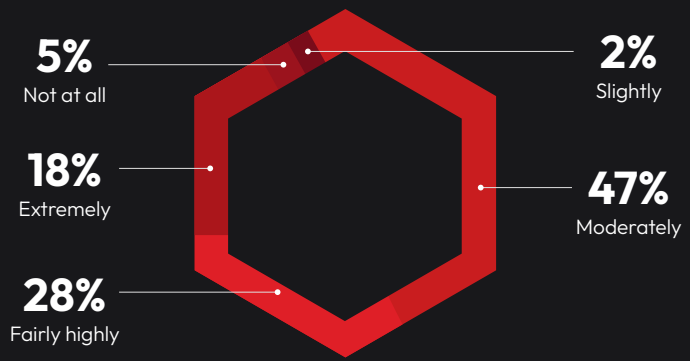
Revenue loss

System downtime

Compliance

CONFIDENCE IN SECURITY TEAMS LEVERAGING AI

While AI-driven security is gaining traction, confidence levels are mixed. When asked, “How confident are you in how your security team leverages AI to protect your company from bot-driven cybersecurity threats?,” the combined 46% for “fairly highly” and “extremely” suggests positive momentum. But the fact that moderate confidence is the largest category implies businesses still have concerns about AI maturity in security applications.



CHOOSING THIRD-PARTY SOLUTIONS

Given these confidence levels, many enterprises are looking to external vendors for AI-driven security solutions. The Arkose Labs report The Intersection of AI, Digital Fraud and Cyber Defenses found that 62% of respondents believe they gain more by purchasing AI-powered cybersecurity solutions rather than building them in-house. A key driver of this trend is the shortage of skilled personnel—51% of companies report lacking employees with both AI and cybersecurity expertise.

Reasons for turning to third-party solutions include the ability to help stay ahead of ever-evolving cybersecurity threats and the vendor's ability to fend off AI-led threats.

Vendor Considerations

- Ability to help us stay ahead of ever-evolving cybersecurity threats
- Overall cost of vendor's services
- Vendor's ability to fend off AI-led threats
- Efficacy in dealing with unique threats in my industry
- Ability to use AI in their solutions/platforms/products
- Managed customer support provided with the solution

CURRENT CYBERSECURITY OUTCOMES

When asked "Which of the following cybersecurity outcomes are you currently achieving?," 86% report reducing risk. But only 37% see cybersecurity driving business growth and 45% see it reducing costs—indicating security is viewed as a cost center rather than a competitive advantage. Additionally, customer satisfaction (56%) and relationship improvements (41%) suggest security is recognized as a contributor to user trust but not yet a key differentiator.

Importantly, reducing risk does not mean eliminating it. While many companies are making progress, gaps remain, particularly as threats evolve and attack methods grow more sophisticated.

Reducing risk
86%

Increasing customer satisfaction
56%

Reducing costs
45%

Improving customer relationships
41%

Driving growth
37%

CONCLUSION

The growing sophistication of bot-driven threats means enterprises must take a proactive approach to security. These findings indicate that while risk reduction is occurring, there's room for improvement in AI-driven threat prevention and business impact metrics. Investing in AI-powered, adaptable cybersecurity solutions will be key to staying ahead of rapidly evolving attacks.

The time to act is now. Will your enterprise rise to the challenge? We invite you to set up a personalized meeting to discuss these results and talk about your needs.

Methodology

Audience: Senior Decision-Makers

Industries

Sample Size
N=100

Methodology
10-Minute Online Survey

Timing
September to November, 2024

ABOUT ARKOSE LABS

Arkose Labs is the leading global provider offering a proactive fraud deterrence platform purpose-built to neutralize modern attacks, including those powered by Agentic AI and large language models (LLMs). Its comprehensive solution combines proprietary device identification (device ID), behavioral analysis, phishing protection, email intelligence, scraping prevention, API defense and bot management. Trusted by the world's leading consumer brands—including two of the top three banks, Microsoft, Meta, Roblox, and many others—Arkose Labs stops account takeovers, fake account creation, LLM-driven scraping and SMS toll fraud. The platform actively undermines attacker ROI by introducing dynamic friction, making it economically unsustainable for adversaries to persist. Its Security Operations Center (SOC) provides actionable insights from an extensive cross-industry intelligence network, which monitors legitimate traffic and attack patterns across global enterprises. With unparalleled proactive support for internal security teams, Arkose Labs goes beyond conventional security by actively partnering with customers to disrupt organized fraud networks such as Storm-1152. Headquartered in San Mateo, California, the company maintains a global presence with offices throughout APAC, Central America, EMEA and South America."

USA (San Mateo)

Australia (Brisbane)

United Kingdom (London)

Costa Rica (San José)

India (Pune)

Argentina (Buenos Aires)

Book a Meeting