WHEN AI BECOMES THE ULTIMATE TECHNOLOGY PLATFORM HACKER

Key Data Insights from New Research:
The Intersection of AI, Digital Fraud and Cyber Defenses

ARKOSE LABS™

©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

WHEN INNOVATION MEETS INFILTRATION

Technology companies operate at the intersection of innovation and vulnerability. In the digital battleground, tech platforms are not just potential victims—they are key pioneers in defensive technologies. But can they outpace the innovation of bad actors who have a headstart leveraging AI in all its forms? For many tech platforms it comes down to adapt fast or become digital casualties even faster.

The stakes are existential. This isn't just about protecting revenue; it's about maintaining the fundamental trust that powers the digital world. Technology enterprises today are navigating multi-dimensional minefields of rising attacks and a critical skills gap where adversaries are constantly evolving, outmaneuvering and reshaping the battlefield.

This infobrief is packed with industry insights from our new research, The Intersection of AI, Digital Fraud and Cyber Defenses. It explores how tech companies can use AI to outsmart evolving threats, turning defensive strategies into powerful offensive weapons in the ongoing digital arms race.

"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

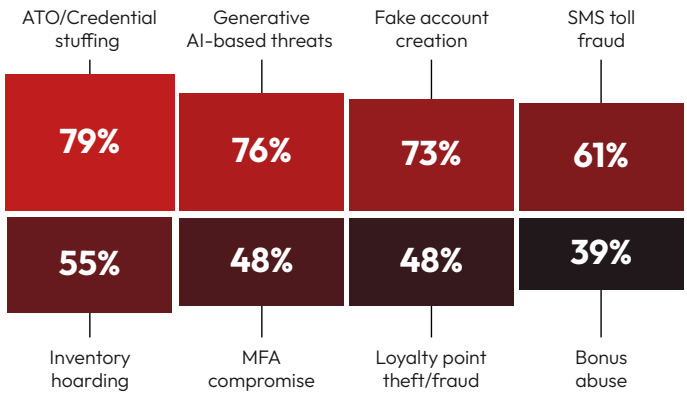
©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

EXPOSED ATTACK SURFACES

Tech platforms face a wide range of threats to their critical business applications, with account takeovers persisting as a major vulnerability. Notably, generative AI-based threats and SMS toll fraud outpace cross-industry averages by 10% and 6% respectively.

Which attack types are seen as the most pressing? Here are the top threats tech platforms believe pose significant risks to their business operations and customers' experience, along with the percentage of enterprises concerned to a moderate or large extent.

Most Concerning Attack Types

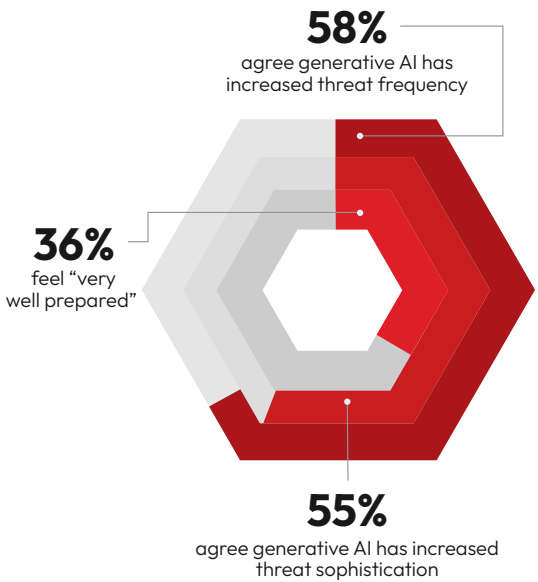


©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

THE PREPAREDNESS LANDSCAPE

Meanwhile, generative AI has amplified the sophistication of these threats, making fraud not only more frequent but harder to detect. The harsh reality is that while cybercriminals are well-prepared to launch AI-powered attacks, a majority of enterprises are playing catch-up.

To wit, nearly two of three tech respondents don't consider themselves "very well prepared" to defend against AI-powered threats. This lack of preparedness is a significant concern, especially when considering the pace at which cybercriminals innovate.

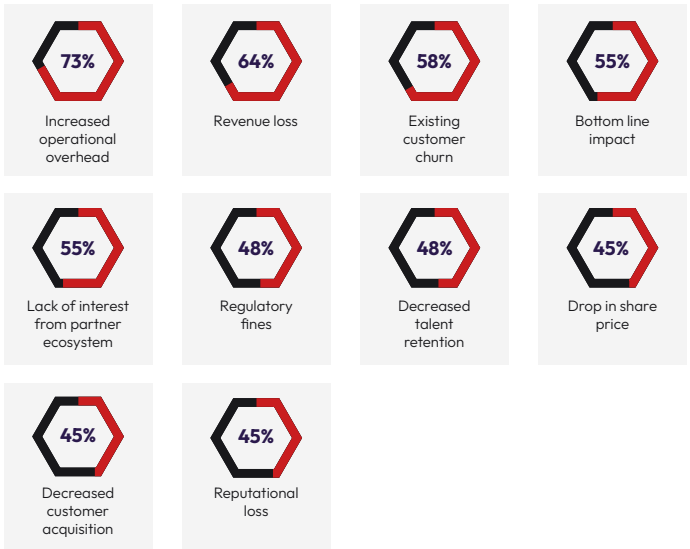


©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

THE TRUE COST OF DIGITAL VULNERABILITY

The high concern over cyber threats is warranted, as the consequences of failing to address these attacks are severe. Of particular note is increased operational overhead, where tech enterprises outpace cross-industry averages by 12%.

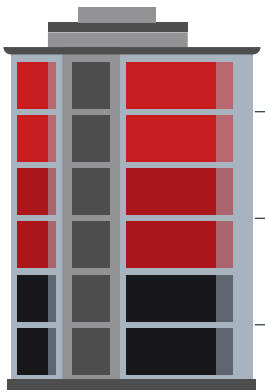
These interrelated, negative consequences ultimately impact business operations and profitable growth. This vulnerability comes at a time when cybercriminals are leveraging AI to outpace traditional defenses, turning fraud into a scalable, lucrative operation. The percentage of tech platforms reporting these negative outcomes:



©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

FINANCIAL FALLOUT ZONES

The negative financial consequences since 2022 are staggering. Among the tech platforms surveyed, 67% reported losses between $1M to $99M during the past two years due to the negative consequences related to cyber threats—with 18% reporting even higher losses.



$1M to $9.9M: Losses affecting nearly half of the large tech platforms.

$10M to $99M: Common losses among larger tech enterprises.

$100M to $500M: Losses for nearly one in five tech companies, highlighting the potential for substantial financial impacts.

©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

AI: FROM THREAT TO SHIELD

The good news? Tech companies are recognizing that AI isn't just a threat—it's the solution. Technology firms stand out for implementing AI-driven security measures at a rate exceeding the cross-industry average. This distinction likely reflects the higher stakes within this sector, where the volume of PII data and the consequences of breaches are particularly pronounced.

It's also worth calling out that 76% of technology companies 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.

Actions Tech Platforms Are Taking

76%
Report leveraging AI to enable faster response time to security incidents

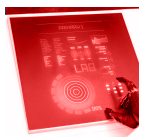
76%
Report using AI to analyze historical data and identify vulnerabilities

67%
Report using AI to predict future security threats

67%
Report automating processes with AI to reduce manual tasks

67%
Report deploying AI tools to continuously monitor infrastructure

61%
Report analyzing cybersecurity data in real time with AI tools



©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

THE ADAPTIVE DEFENSE

AI-powered solutions are delivering tangible results for cybersecurity teams. In the technology sector, 64% report improved threat intelligence, while 61% say they are better equipped to defend against basic bot attacks.

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.

Already Realized Benefits

- Improved threat detection and response
- Improved threat intelligence gathering
- Reduced overall cost of securing my business
- Better defense against basic bot attacks
- Better defense against AI-powered bot attacks
- Better defense against generative AI-powered attacks
- Better defense against human fraud farm attacks

©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

OVERCOMING STRATEGIC LIMITATIONS

Despite progress, challenges persist. A global skills gap in AI and cybersecurity expertise remains a significant hurdle, with more than half of tech enterprises reporting a shortage of personnel with AI plus cybersecurity expertise.

Additionally, 39% say integrating AI-powered solutions with existing systems is too difficult, and the same percentage highlight restrictions on using AI in cybersecurity models due to strict model governance requirements. This underscores the tension between innovation and operational challenges in the field.

©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

However, tech firms are finding ways to overcome these obstacles by partnering with specialized vendors. Collaboration with AI-focused cybersecurity providers enables these enterprises to leverage industry-specific solutions, access cutting-edge threat intelligence, and stay compliant with evolving regulations.

Report gaining more value by buying AI-powered cybersecurity solutions than building the solutions in-house

©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

THE STAKES: WHY ACTION CAN'T WAIT

"AI companies are everywhere, and they're all after data to fuel their models. With new companies sprouting up daily, we need to recognize that while we're solving the current problem, we're also tackling a larger challenge." That comment from a senior engineering executive in the tech industry 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.

Meanwhile, the cost of inaction is rising. Technology platforms face mounting pressure from customers and competitors to strengthen their defenses. At the same time, AI continues to evolve, offering criminals new tools to exploit vulnerabilities. For the tech industry, the question is clear: Will you lead the way, or be left behind?

To truly secure their future, enterprises must invest in AI solutions that not only meet today's challenges but anticipate tomorrow's. This requires a bold approach—embracing innovation, tackling hurdles, and partnering with experts who can help navigate the complexities of AI-powered security.

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.

©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM

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

©2026 Arkose Labs. All rights reserved. WWW.ARKOSELABS.COM