ARKOSE LABS™

Execute These 5 Strategies to Defend Against AI Cyberattacks

AI-powered cyberattacks are the new reality, and the losses are staggering. Our report The Intersection of AI, Digital Fraud and Cyber Defenses reveals that 53% of enterprises have lost between $10 million to over $500 million in the past two years due to the negative consequences related to cyber threats—and the rise of AI-powered attacks is accelerating this trend.

As cybercriminals weaponize AI to launch adaptive and stealthy attacks, traditional security measures are no longer enough. It's time to fight fire with fire. The following five critical strategies will help you develop a more resilient cybersecurity posture.

Strategy #1:
Prioritize and Secure High-Risk Entry Points

In the battle against AI-powered cyberattacks, it's crucial to identify and fortify the most vulnerable entry points to your enterprise, particularly account sign-up and sign-in processes.

- Implement AI-resistant authentication measures like adaptive authentication and behavioral biometrics
- Deploy dynamic security protocols that continuously monitor and adjust to evolving threat patterns
- Strengthen verification and access controls for linked accounts

76% of enterprises say ATO/credential stuffing is their top concern.

Strategy #2:
Harness the Power of Threat Intelligence

Staying one step ahead of cybercriminals requires a proactive approach to threat intelligence.

- Actively participate in threat intelligence sharing communities
- Integrate real-time threat data feeds into your AI-powered defense systems
- Regularly update your threat intelligence sources

46% of enterprises cite improved threat intelligence as the top benefit already realized by AI-powered cybersecurity solutions.

Strategy #3:
Cultivate an AI-Ready Cybersecurity Culture

Developing a strong, AI-ready cybersecurity culture is essential for ensuring your company can effectively adapt to the evolving threat landscape.

- Invest in AI-focused training and upskilling programs for your cybersecurity team
- Encourage a mindset of continuous learning and experimentation
- Promote cross-functional collaboration to leverage the full potential of AI in cybersecurity

51% of enterprises report a shortage of personnel with combined AI and cybersecurity expertise.

Strategy #4:
Adopt a Multi-Layered, AI-Powered Defense Architecture

In the face of sophisticated AI-powered attacks, traditional perimeter defenses are no longer enough.

- Implement AI-powered solutions across multiple layers, including network, endpoint and application security
- Integrate AI capabilities with existing tools for a seamless, holistic defense
- Continuously monitor and optimize your AI-driven security systems

70% of enterprises are already using AI for bot management, highlighting the importance of multi-layered defense.

Strategy #5:
Embrace Specialized Partnerships for AI Defense Excellence

Collaborating with specialized AI cybersecurity vendors can significantly accelerate your defense capabilities and help you stay ahead of the curve.

- Seek out vendors with deep AI expertise and proven track records of success
- Focus on solutions that deliver measurable security outcomes and align with your business objectives
- Foster strong, long-term relationships with your AI defense partners

62% of enterprises prefer buying AI-powered cybersecurity solutions over building in-house.

It's Time to Embrace AI

AI-powered cyberattacks pose an unprecedented threat. By prioritizing these five strategies—securing high-risk entry points, harnessing threat intelligence, cultivating an AI-ready culture, adopting multi-layered defenses and embracing specialized partnerships—your enterprise can build a strong, adaptable cybersecurity posture.

The time to act is now. Start fortifying your defenses today and secure your position as an industry leader in the fight against advanced cyber threats. Schedule your personalized consultation today.

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.

Book a meeting