Arkose Labs

GPT Prompt Compromise

A Strong Safeguard Against the Compromise of GPT Prompts

Enterprises are increasingly deploying chat GPTs to boost efficiency, enhance customer experiences, and drive innovation. A PwC survey shows 73% of U.S. companies have integrated AI, with 54% specifically using generative AI in various business areas. Key applications include chatbots and virtual assistants for 24/7 customer support, technical troubleshooting, and enhancing digital experiences with interactive guides and real-time feedback. However, GPT prompt compromise is a rising threat, such as prompt scraping, where malicious bots gather confidential information. For instance, as companies deploy GPT applications in customer service functions, bots can steal PII during identity verification processes. Arkose Bot Manager offers comprehensive protection against GPT prompt abuse.

Arkose Bot Manager for GPT Prompt Abuse

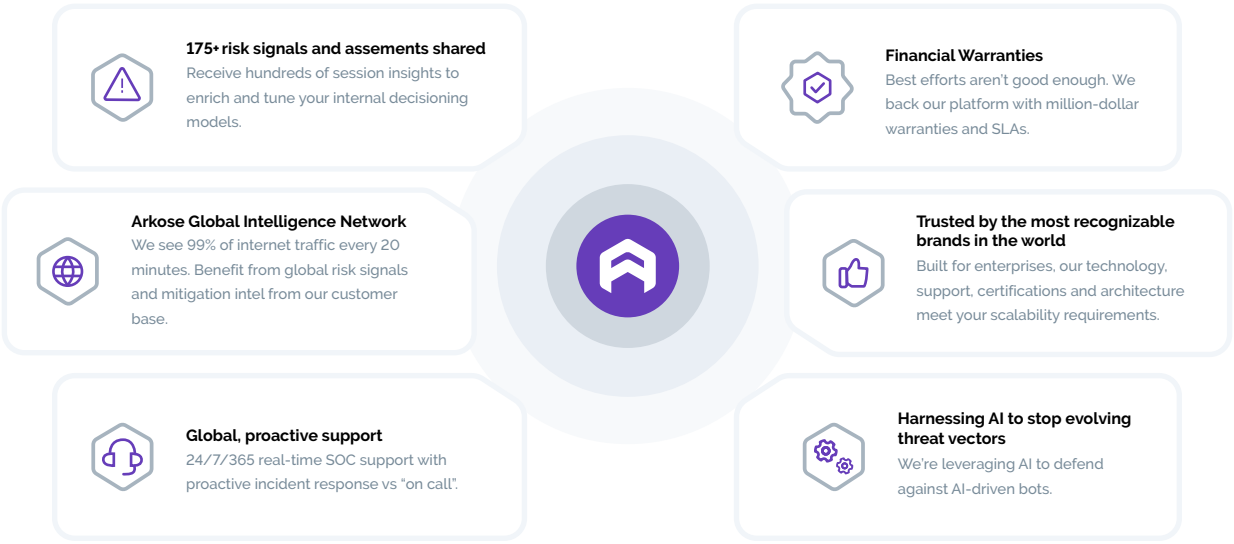
Arkose Bot Manager significantly reduces the risk and impact of emerging threats like GPT prompt compromise by providing a secure digital environment that optimizes the user experience. It enhances risk management by refining risk models, which in turn improves threat intelligence and mitigation strategies. This ensures that businesses can maintain their reputation and service quality without compromising on security or user satisfaction. Arkose Bot Manager includes Arkose GPT Protection, specifically designed to guard against malicious bots conducting prompt scraping and LLM platform abuse. This capability prevents attackers from harvesting confidential and proprietary information at scale in GPT applications, maintaining the confidentiality and integrity of sensitive customer data.

Enterprise Platform Highlights

- → Patented decisioning platform
- → Real-time feedback loop
- → Global intelligence network
- → Real-time data visibility and integration
- → Enterprise-grade scalability
- → GDPR privacy compliance
- → WCAG 2.2 Level AA accessibility certification

> "Fraudsters' mindsets ultimately come down to money. We recognized that the cost of circumventing the Arkose Labs solution was prohibitively high, whereas the cost-benefit analysis was in the fraudsters' favor for alternative fraud controls."
>
> **– Identity Lead, Microsoft**

The Arkose Labs Advantage



ACTIR and the Arkose Labs SOC: Proactive Defense

Arkose Labs operates as an extension of your team, rapidly countering attacks and providing actionable insights without overburdening your internal resources. The Arkose Cyber Threat Intelligence Research (ACTIR) unit conducts proactive threat hunting, risk intelligence gathering and other counterintelligence methods to provide vital, fresh intelligence. Meanwhile, the 24/7/365 Security Operations Center (SOC) team focuses on identifying and stopping large-scale attacks immediately.

The SOC continuously monitors for new threats and collaborates with ACTIR. This feedback loop ensures a seamless collaboration between the SOC and ACTIR, enhancing the overall accuracy, timeliness and effectiveness of your cybersecurity defense.

Arkose Bot Manager in Action

Global AI Company Elevates User Experience

A global AI research and deployment company faced unprecedented cyberattacks, including LLM platform abuse, SMS toll fraud, account takeover, new account fraud and advanced phishing. These attacks exhausted its processing capacity, costing tens of millions monthly and preventing genuine users from accessing services while bots ran rampant. Additionally, the company needed to ensure its services weren't accessible in prohibited countries

Results with Arkose Labs

- → 2 billion bot attacks detected and mitigated in first 6 months
- → > 99% reduction in LLM platform abuse
- → 99% good user throughput

BOOK YOUR DEMO