Global AI Platform Stops LLM Abuse and Saves Millions in GPU Costs

A global AI research and deployment company faced unprecedented cyberattacks including LLM platform abuse, SMS toll fraud, account takeover and advanced phishing, costing millions monthly.

The Challenges

LLM Platform Abuse at Scale: Bad actors proxied the company's premier model to circumvent API fees entirely, straining platform resources during a global GPU shortage.

Processing Capacity Exhaustion: Estimated 4-5% of millions of daily prompts were suspicious, posing massive financial risks and overwhelming GPUs to the point where legitimate users couldn't access services.

Subscription Fraud and Resale: Attackers sold subscriptions to consumers, proxied services to other users, and used fake credit cards while operating in prohibited countries.

Multi-Vector Attack Surface: Attacks across registration, sign-in, password recovery, developer portal and profile update flows required comprehensive defense strategy.

The Arkose Titan Solution

Adaptive Defense Strategy: Initially secured registration flow to stop fake accounts and SMS toll fraud, then dynamically pivoted to protect chat prompts, login, password recovery, developer portal, and profile updates as attacks shifted.

Advanced Challenge Technology: Deployed Arkose MatchKey challenges and token enforcement with LLM-resistant design, increasing attack costs until attackers resorted to expensive human fraud farms.

Proactive Threat Intelligence: ACTIR team researched attacker GitHub repositories and Discord channels to anticipate countermeasures in real time, staying ahead of evolving tactics.

Business Results

2 Billion Bot Attacks Mitigated: Detected and stopped 2 billion bot attacks within first 6 months of deployment.

99%+ Reduction in LLM Platform Abuse: Virtually eliminated platform abuse where bad actors proxied premier models to bypass API fees.

GPU Resources Protected: Preserved tens of millions monthly in processing costs during GPU shortage.

Shut Down Attacker Infrastructure: Prominent attacker GitHub repositories closed within weeks as attacks became economically unviable.

SCHEDULE CALL WITH AN EXPERT

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. Headquartered in San Mateo, California, the company maintains a global presence with offices throughout APAC, Central America, EMEA and South America.