

AI Innovator Neutralizes Compute Abuse and Slashes GPU Costs

A pioneer in the AI space, this organization focuses on developing reliable, interpretable, and steerable AI systems, including a globally popular large language model (LLM).



The Challenges

Unsustainable Compute Burn: Bad actors were creating mass volumes of free accounts and cycling through them to exploit free tier limits, driving up massive compute and GPU costs.

Revenue-Expenditure Imbalance: While maintaining millions of users, the organization faced a critical gap between revenue and the high costs of supporting a non-paying majority during a phase of rapid growth.

Ineffective Legacy Defense: Previous third-party "point solutions" failed to provide the efficacy needed to curb sophisticated, automated abuse, leading to a "sticker price" issue for security that didn't deliver results.

The Build vs. Buy Dilemma: Despite having world-class engineering capabilities to build in-house tools, the organization needed a more expedient and expert-led solution to address the problem immediately.



The Arkose Titan Solution

Holistic Platform Defense: Deployed Arkose Titan, a unified platform that replaces disparate point solutions with a comprehensive suite including bot management, email intelligence, and behavioral biometrics.

Proof of Value (POV): Conducted an intensive POV that demonstrated superior effectiveness over the incumbent competitor by identifying and neutralizing malicious traffic in real-time.

Arkose Device ID: Created persistent digital fingerprints that identify and track nefarious devices even when they attempt to hide their tracks.

Automated "Banning" Logic: Leveraged Arkose Device ID signals to set up automated response workflows that identify and ban returning bad actors within 10 minutes of their reappearance.

Expert Human Intelligence: Augmented automated defenses with the Arkose SOC team, providing 24/7/365 monitoring and deep-dive insights into evolving AI-driven attack patterns.



Business Results

Immediate Financial Relief: During the POV period this customer saved between \$120,000 and \$150,000 in compute and GPU costs.

Rapid Time-to-Value: Choosing Arkose Titan proved more expedient than an internal build, allowing the company's engineers to stay focused on core AI research rather than security infrastructure.

Deterred Organized Abuse: Effectively stopped the cycle of free-account creation and LLM platform abuse, restoring economic balance to the free-user tier.

Superior ROI: Displaced the underperforming incumbent by delivering high-fidelity detection and material savings that far outweighed the cost of the platform.

**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. © 2026 Arkose Labs. All rights reserved.