Cloud Platform Eliminates Cluster Failures and Stops 95% of Fake Account Fraud

A premier cloud computing platform serving engineering teams at some of the world's largest organizations across financial services, retail, healthcare and more. Its popularity and free trial offering made it a prime target for fraudsters looking to exploit compute resources at scale.

The Challenges

Free Trial Abuse at Scale: Fraudsters used bots and human fraud farms to create fake accounts in bulk, exploiting free trial compute time for cryptocurrency mining and other high-intensity tasks.

Daily Cluster Failures: The resulting server strain caused cluster failures every day. During peak attack periods, up to 60% of clusters went down simultaneously.

Overnight Security Firefighting: Internal security teams were forced to work around the clock responding to attacks, driving up costs and pulling focus from higher-value work.

The Arkose Titan Solution

Registration Flow Defense: Arkose Titan was deployed on the new account sign-up flow as a first line of defense, immediately stopping the bulk of malicious bot traffic originating from coordinated attack networks.

Persistent Human Fraud Deterrence: When automated attacks subsided, fraud farms from multiple countries picked up the effort, attacking nearly 24 hours a day. Arkose served these sessions with escalating challenges designed to exhaust attacker resources until they abandoned the effort entirely — a pattern repeated across attack sources in Indonesia, Singapore and Portugal.

24/7 SOC Partnership: The Arkose SOC worked alongside the client's team throughout, continuously fine-tuning defenses as attack patterns shifted and providing actionable intelligence for long-term mitigation.

Business Results

95%+ Reduction in Fake Account Fraud: The vast majority of fraudulent new account creation was stopped, restoring the integrity of the free trial program.

Cluster Failures Completely Eliminated: Server stability was fully restored, ending the daily operational disruptions that had become the norm.

Internal Teams Freed from Firefighting: With attacks neutralized, security staff were no longer working overnight to fend off attacks, recovering significant time and operational capacity.

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.