SOLUTION BRIEF

Bonus Abuse

Smart defense against bonus misuse

Is your company one of the businesses suffering from the billions of dollars in losses each year due to promotional abuse and loyalty fraud? Fraudsters exploit welcome bonuses, referral programs, and loyalty rewards through multi-accounting schemes, orchestrating farms of fake identities to harvest incentives at scale. Arkose Titan breaks this exploitation model by compounding costs across every abuse vector—from multi-account creation and identity rotation to promo code testing and bonus extraction.

Arkose Titan for Bonus Abuse

Coordinated Intelligence Across the Stack

Arkose Titan's unified API coordinates device fingerprinting, behavioral analysis, email risk scoring and challenge-response mitigation in real time. When multi-account patterns emerge or promo code testing velocity spikes, the engine automatically calibrates difficulty and risk signals flow instantly to downstream fraud tools.

Challenge Technology Built for AI Resistance

Our next-gen challenges combine Proof-of-Work computation with multimodal reasoning tasks that cost attackers via LLM vision APIs. Each challenge adds substantial time per attempt, and with multiple retries required, bonus abusers burn through compute budgets fast.

Device Intelligence That Remembers

Device fingerprinting connects multiple bonus-claiming accounts back to the same device, while behavioral analysis detects the repetitive patterns of serial bonus abusers cycling through promotional offers. Real-time signals create risk assessments accurate enough to pass 99% of legitimate users with zero challenges.

Transparent Decisioning for Security Teams

Every authentication generates detailed telemetry: 175+ telltale rules showing why we assigned each risk score, complete device intelligence and behavioral analysis. Security teams see our decision logic as it happens, enabling immediate investigation of bonus abuse rings and referral fraud networks.

Consortium Intelligence Multiplier

Threat patterns identified at one customer instantly inform protection across our network. When Arkose Labs spots new bonus extraction methods, gift card fraud patterns or account farming infrastructure, every customer benefits from updated detection rules.

Platform Capabilities

- **Arkose Bot Manager**
  Advanced bot detection and mitigation
- **Arkose Email Intelligence**
  Real-time email authenticity validation
- **Arkose Device ID**
  AI-enhanced device identification
- **Arkose Scraping Protection**
  Comprehensive defense against unauthorized scraping
- **Arkose Edge**
  Lightweight server-side API security

> **It was like flipping a light switch - we immediately saw a reduction in abusive account creation**
>
> – Sparky Toews, Adobe

The Arkose Labs Advantage

225+ risk signals and assements shared
Intelligence to enrich and tune your decisioning

Financial warranties
Best efforts aren't good enough. We back our platform with million-dollar warranties and SLAs

Arkose Global Intelligence Network
We see 90% of internet traffic every 20 minutes. Benefit from global risk signals and mitigation intel

Trusted by the most recognizable brands
Built for enterprises, our technology, support, certifications and architecture meet your scalability requirements

Global, proactive support
24/7/365 real-time SOC support with proactive incident response vs "on call"

Harnessing AI to stop evolving threat vectors
We're leveraging AI to defend against AI-driven bots

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

Gaming Giant Stops Automated Attacks, Saves Millions

A leading sports video gaming company was facing significant fraud challenges due to its global reach and financial success. Fraudsters were using automated scripts and bots to create fake accounts, accumulate virtual currency and manipulate the in-game economy – costing the company millions of dollars.

Results with Arkose Labs

- 15x reduction in fraudulent activity
- Elimination of in-app auction house and virtual currency abuse
- A safe and seamless experience for genuine customers

Take Action Now

Ready to stop bonus abuse? To see how Arkose Labs can protect your promotional programs, Schedule a call with an expert today.

BOOK A DEMO

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.