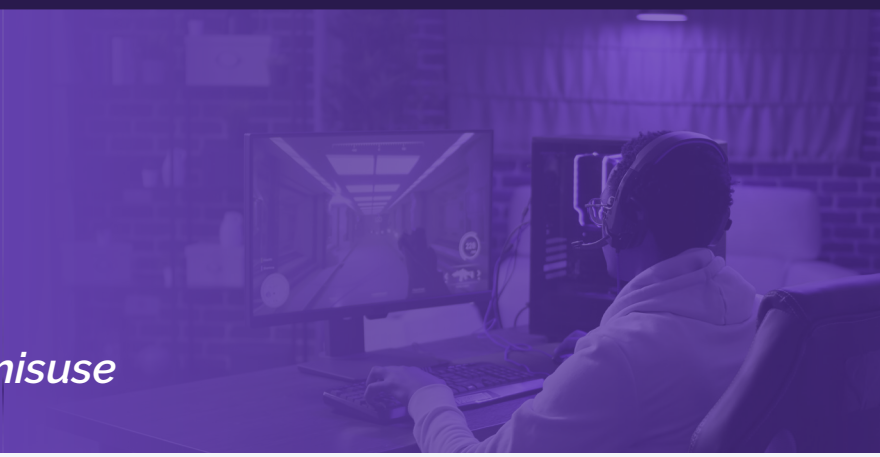
Arkose Labs



Bonus Abuse

Smart defense against bonus misuse

Is your business suffering from the estimated $89 billion in losses each year due to promotional abuse and loyalty fraud, according to research by PYMNTS? While enticing customers with special offers and incentives is a proven strategy to drive engagement and sales, the rampant exploitation of these deals can lead to significant financial losses. Fraudsters often use multiple accounts or false information to repeatedly claim bonuses and promotions, undermining the intended benefit of these incentives. This not only skews your marketing analytics but also drains resources that could be better spent on genuine customer acquisition and retention. Arkose Bot Manager can help. Our innovative solution allows businesses to stay ahead of bonus abuse by detecting and mitigating suspicious activities in real time. With advanced analytics and the power of a global data consortium, Arkose Bot Manager ensures that your promotional efforts reach legitimate customers, preserving the integrity of your marketing campaigns and boosting your bottom line.

Arkose Bot Manager for Bonus Abuse

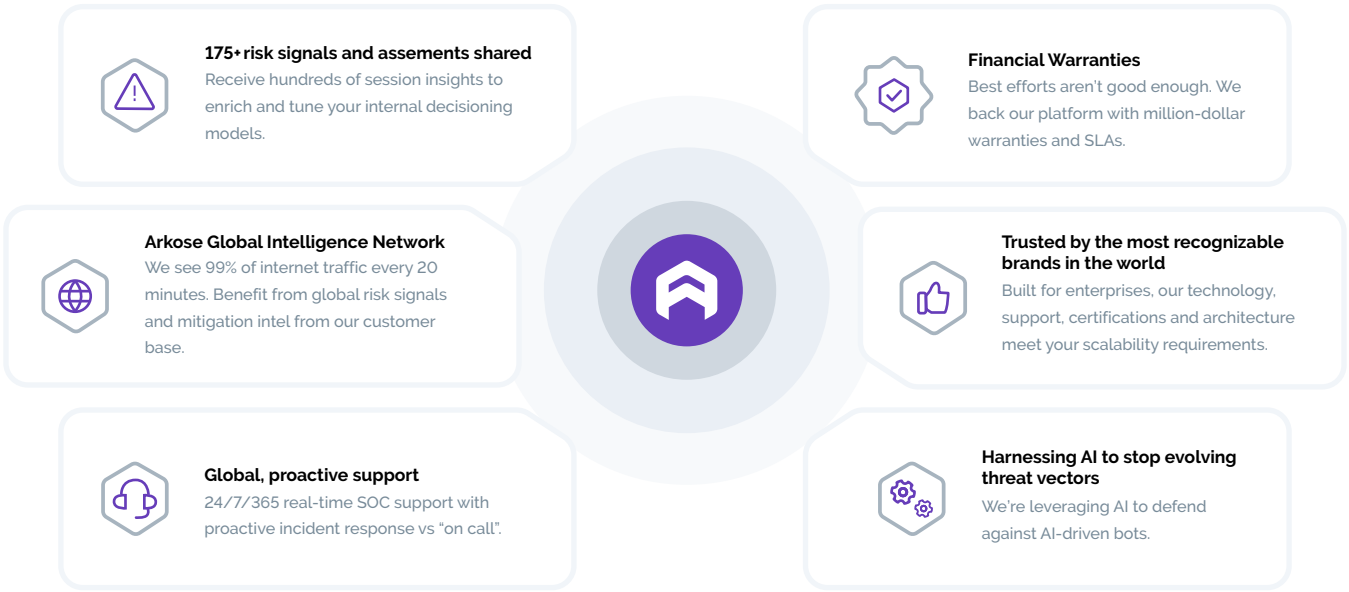
The Arkose Bot Manager platform is the leading solution for proactively identifying and combating promo abuse. Its robust engine gathers high-risk data from a global network, thoroughly analyzing digital intelligence to evaluate user intent and assign risk scores. By leveraging an advanced algorithm, it assesses over 125 live signals to deliver adaptive, dynamic responses. The platform's detection models ensure seamless and secure digital interactions for legitimate users. When malicious traffic is detected, Arkose Bot Manager quickly deploys a series of cutting-edge challenges, offering top-tier security in real time.

Enterprise Platform Highlights

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

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

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

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

BOOK YOUR DEMO