PRODUCT BRIEF

# Arkose Titan Platform

Stop Fraud at Every Touchpoint. Make Attacks Unprofitable.

**Arkose Titan** is the only fraud prevention platform that protects your entire user journey—from registration through ongoing platform activities—while making attacks economically unviable for bad actors.

## The Challenge: Fraud That Evolves Faster Than Your Defenses

Digital businesses face an escalating crisis that threatens growth, erodes customer trust and drains resources.

### Critical Pain Points

1. **Fragmented Security Gaps**
Companies struggle with separate vendors for different security needs, creating exploitable gaps for attackers. Point solutions for sign-up, sign-in and transactions miss cross-stage attack patterns, allowing sophisticated attackers to coordinate attacks across multiple touchpoints. Without unified intelligence, businesses lack visibility into coordinated campaigns spanning the entire user journey.

2. **Unsustainable Detection Arms Race**
Constantly retraining detection systems leads to alert fatigue and rising operational costs without guaranteed effectiveness. Security teams are overwhelmed by false positives requiring manual investigation, while fraud operations scale linearly with attack volume—increasing costs without improving outcomes. This diverts security teams from strategic initiatives to endless firefighting.

3. **Outpacing Legacy Defenses**
AI-powered bots, credential stuffing operations and human fraud farms defeat simple bot detection using residential proxies, device emulation and sophisticated evasion techniques. Attack methods evolve daily, rendering static rule sets obsolete within weeks. This leaves companies perpetually one step behind attackers who adapt faster than defenses can be updated.

## The Evolution of Threat Sophistication

Modern attacks have evolved through 4 distinct levels of sophistication, each requiring more advanced defenses.

**Level 1: Scaled Bot Attacks**
- Automated attacks using rotating IPs, device fingerprints and residential proxy networks
- Distributed across thousands of endpoints to avoid rate limiting
- Randomized timing and behavioral patterns to evade signature detection

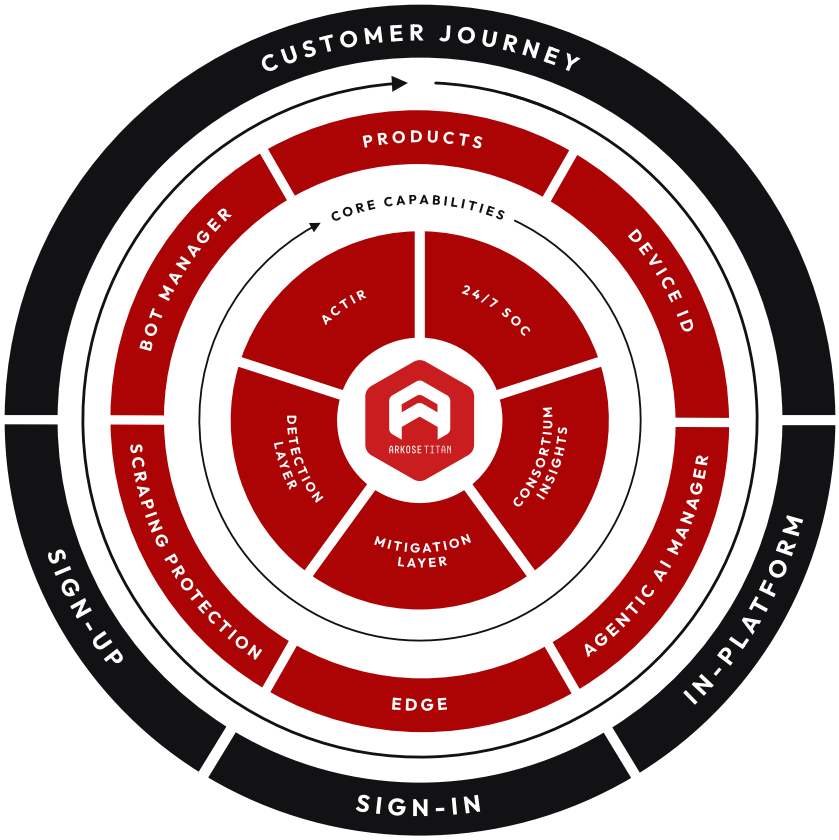
**Level 2: Hybrid Bot-Human Attacks/Fraud Farms**
- Humans solve CAPTCHAs while bots handle repetitive tasks (credential stuffing, SMS toll fraud, etc.)
- CAPTCHA farms where low-wage workers solve challenges for automated systems
- Browser automation tools operated by humans for fraud activities

**Level 3: Low and Slow Human Attacks**
- Organized operations with real humans, real devices and real locations performing fraudulent activities
- Account creation, fake reviews, social media manipulation, bonus abuse, referral fraud
- Sophisticated identity fabrication using bespoke infrastructure

**Level 4: Agentic AI Attacks**
- Autonomous AI agents that can probe defenses, learn detection boundaries, and generate novel attack strategies
- Real-time adaptation to security responses without human intervention
- Multi-vector coordination across different attack surfaces simultaneously

## The Solution: The Arkose Titan Platform

Arkose Titan fundamentally changes the fraud equation by making attacks financially unviable while keeping legitimate users moving seamlessly through your digital experience.




## Detection With Unified Intelligence

Arkose Titan integrates comprehensive signals across multiple detection vectors working together simultaneously.

**Network Intelligence:** IP reputation and TLS fingerprints identify suspicious traffic sources

**Behavioral Biometrics:** Mouse movements, keystroke dynamics and interaction patterns

**Device Intelligence:** Persistent device recognition across sessions and platforms

**Mobile SDK:** Native app protection with device attestation and runtime security

**Traffic Analysis:** Pattern detection identifies automated behavior and anomalies

**Agentic Analysis:** AI agent detection including large language models, browser automation and custom frameworks

**Email Intelligence:** 50+ signals across throwaway domains, tumbling patterns and fraud networks

All signals feed into comprehensive risk assessment, providing complete visibility impossible with point solutions.

## Adaptive Enforcement Makes Fraud Unprofitable

Arkose Titan deploys multiple enforcement mechanisms based on risk level.

**Proof of Work:** The minimal-friction solution breaks solver models and stops volumetric attacks.

**Economic Disruption Through Attack Economics:** Challenges exhausts attacker resources, making fraud campaigns financially unviable.

**Visual Challenges:** AI-resistant tasks evolve dynamically, forcing costly attacker API consumption.

**Zero Friction for Legitimate Users:** Invisible protection that uses behavioral biometrics ensures seamless legitimate authentication.

## Unified Platform Intelligence Eliminates Blind Spots

Arkose Titan's global intelligence network ensures attackers can't move between customers. Visibility propagates across the network through our embedded threat research unit.

### Consortium Intelligence Network

- 150B annual sessions analyzed across customer base
- 3B attacks stopped with signatures validated and shared
- 1B+ unique identities tracked across platforms
- 3B devices analyzed across PC, mobile, consoles, TVs
- 4B IP addresses with reputation data
- 4,000+ telltales stored for attack pattern recognition

### 24/7/365 SOC & Expert Support

- **Immediate Tuning:** Real-time defense adjustments based on emerging threats
- **Incident Response:** Proactive threat mitigation, not reactive "on call" support
- **Proactive Monitoring:** Continuous surveillance of attack patterns across global network
- **Direct Access:** Dedicated account managers and SOC provide strategic guidance and regular threat briefings

### Flexible Deployment Options

- Token-based authentication enables enforcement at any layer of your stack
- Active Mode blocks threats in real time
- Monitoring Mode provides risk assessment
- Custom rules and policies tailored to your risk tolerance and business requirements
- API-first architecture integrates with existing fraud prevention workflows

# What Sets Arkose Labs Apart

## Attack Economics as a Core Differentiator

Our approach to fraud prevention is unique. Traditional solutions focus on blocking attacks. Arkose Titan makes attacks financially unviable by fundamentally changing attacker economics.

- **Increase Attacker Costs:** Adaptive challenges consume attacker time and computational resources
- **Reduce Your Overhead:** Automated enforcement and 24/7/365 SOC eliminate manual review
- **Disrupt ROI Calculations:** Make fraud campaigns unprofitable by inflating costs per successful compromise
- **Sustainable Protection:** Economic pressure forces attackers to abandon campaigns and pursue easier targets

> This approach delivers sustainable protection because it attacks the root motivation—profit—rather than playing endless cat-and-mouse with evolving tactics.

## Complete Agentic AI Defense

The question has shifted from "Is this a bot?" to "Is this agent authorized?" Arkose Titan answers both and is purpose-built for AI-powered threats.

- **Advanced Agent Detection:** Identify AI agents, browser automation and custom frameworks
- **Behavioral Analysis:** Detect non-human patterns even when agents don't self-identify
- **LLM-Resistant Challenges:** Deploy multimodal reasoning tasks that resist automated solving
- **Classification & Governance:** Distinguish authorized agents from malicious automation

> No other platform provides comprehensive protection against agentic AI attacks while enabling legitimate automation use cases.

## Defense in Depth vs. Point Solutions

All detection systems and enforcement systems work together, enabling cross-channel insights that point solutions cannot offer.

- **Gap Risk:** Attackers exploit coordination gaps between separate vendors
- **Latency Risk:** Attacks succeed before point solutions can coordinate response
- **Learning Risk:** Each vendor learns independently with no compounding effectstuffing attacks

> Competitors offer point solutions for specific attack vectors. Arkose Titan provides complete coverage with shared intelligence that strengthens protection at every touchpoint.

# Key Platform Components

### Arkose Bot Manager
Advanced bot detection and mitigation that protects against automated attacks and AI agents; includes Arkose Phishing Protection for defense against adversary-in-the-middle (AITM) phishing attacks that compromise credentials and bypass MFA through reverse-proxy techniques.

### Arkose Device ID
Persistent, accurate device recognition that stops sophisticated evasion through AI-powered similarity detection.

### Arkose Scraping Protection
Comprehensive protection against content theft, price scraping and unauthorized data harvesting by bots and AI agents.

### Arkose Edge
Lightweight edge deployment that extends protection to CDN and edge computing environments, enabling fraud prevention at the network perimeter with minimal latency impact.

# Next Steps

## See Arkose Titan in Action

Schedule a personalized demonstration to see how Arkose Titan protects your specific use cases and delivers measurable business impact.

**Schedule Demo:** https://www.arkoselabs.com/book-a-demo/

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. 