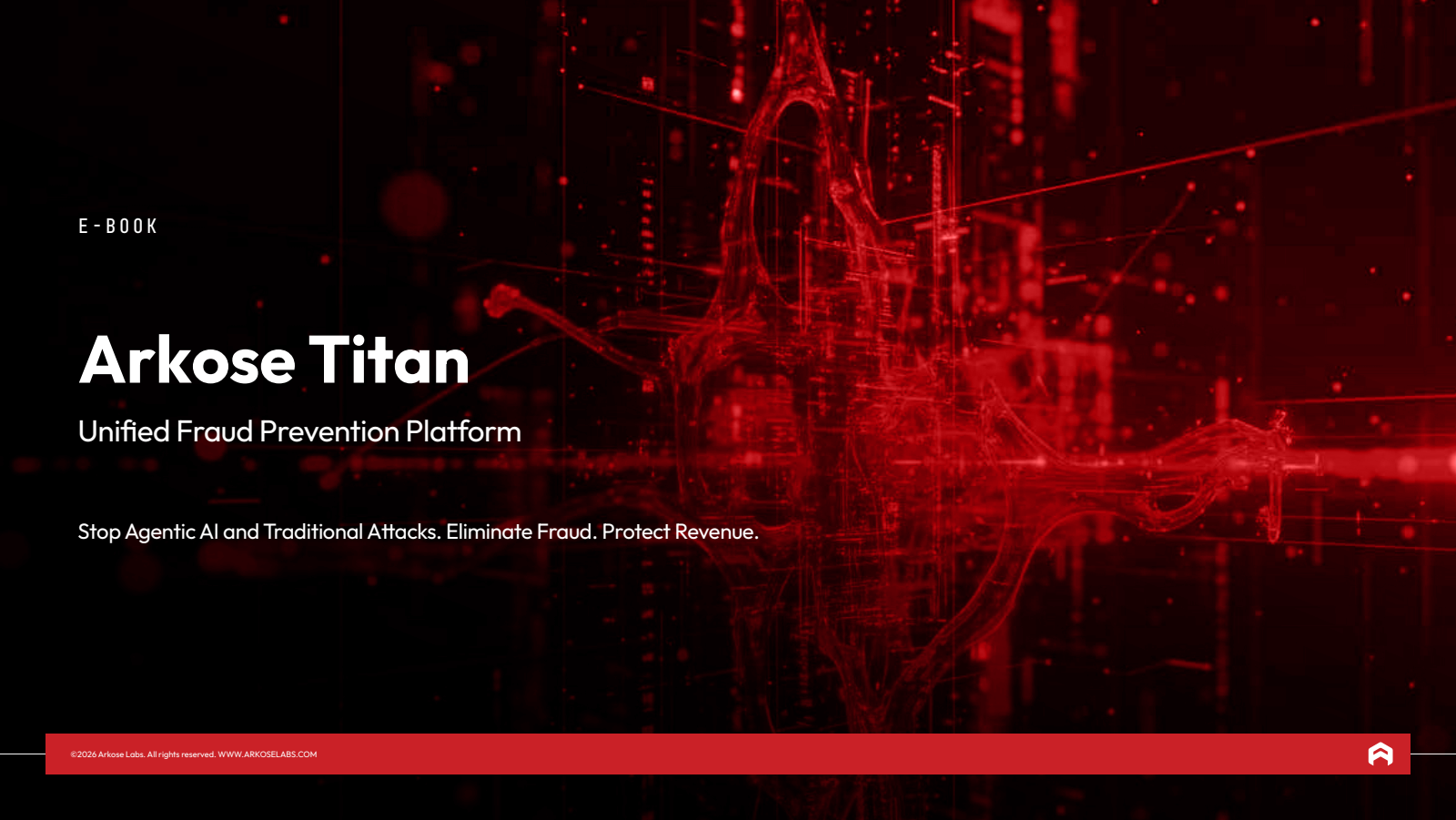


E-BOOK

Arkose Titan

Unified Fraud Prevention Platform

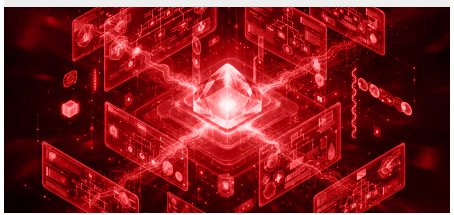
Stop Agentic AI and Traditional Attacks. Eliminate Fraud. Protect Revenue.

The Evolving Threat Landscape

Enterprises face sophisticated attacks from multiple fronts: traditional bots, human fraud farms and now—autonomous agentic AI.

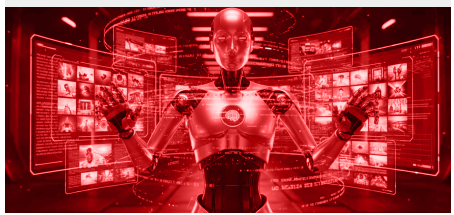
Agentic AI Attacks

Autonomous agents that learn, adapt and scale infinitely with near-zero marginal cost to attackers



Automated Bots

Credential stuffing, fake account creation and scraping operations at massive scale



Human Fraud

Coordinated operations of manually executed attacks using legitimate-looking infrastructure

Traditional defenses can't keep pace with attacks that evolve faster than your security updates.

Why Traditional Approaches Fail

One unified system beats a patchwork of disconnected tools.

Point Solutions

- ✗ **Fragmented tools** - Multiple vendors, incompatible systems, endless maintenance
- ✗ **Security sprawl** - Coverage gaps between solutions that attackers exploit
- ✗ **Integration nightmares** - Months-long implementations with costly custom work
- ✗ **Coverage gaps** - Attackers find the seams between your security layers
- ✗ **Black box decisions** - No visibility into why actions were taken or blocked
- ✗ **Reactive only** - Detect and respond after attacks are already underway

Unified Platform

- ✓ **Comprehensive solution** - Single vendor, integrated architecture, streamlined management
- ✓ **Single integration** - One implementation covers all attack vectors comprehensively
- ✓ **Defense in depth** - Multiple protection layers working in concert, no gaps
- ✓ **Economic deterrence** - Make attacks too expensive rather than just blocking them
- ✓ **Full data transparency** - Complete visibility into every decision and signal
- ✓ **Proactive + reactive** - Prevent attacks before they start, respond when needed 24/7/365

The attackers aren't playing defense. Why should you?

Introducing Arkose Titan

Not just detection. Deterrence.

A unified platform that makes attacking you more expensive with every attempt.

Identification Validation	Attack Prevention	Advanced Threat Protection
Device ID Advanced fingerprinting that identifies real devices from fraudulent ones	**Bot Manager** Stop automated attacks before they reach your applications	**Phishing Protection** Stop MFA compromise by detecting reverse-proxy phishing in real time
Email Intelligence Validate email reputation and detect disposable addresses instantly	**Scraping Protection** Prevent automated data theft and content scraping	**Edge** Lightning-fast protection at the network edge for API access

Arkose Titan is powered by agentic intelligence—disrupting attack economics through adaptive challenges that make every AI-driven attempt more costly than the last.

BY THE NUMBERS

99% of legitimate users never see a challenge

24/7/365 SOC protection

Billions of sessions analyzed daily

How Economic Deterrence Works

Each layer forces attackers to spend more resources - until the attack becomes unprofitable.

STAGE 1 **Initial Detection, Threat Identified**
Arkose Titan detects suspicious behavior and deploys first defenses.

STAGE 2 **First Evasion, Cost Multiplies**
Attack triggers adaptive enforcement; difficulty and resource costs scale exponentially.

STAGE 3 **Continued Attack, Cost Explodes**
Persistent attempts face increasingly sophisticated defenses and attack ROI collapses.

Traditional Vendor CAPTCHAs:
Cheap to attack

Arkose Titan Challenges:
Exponentially more expensive

Traditional Vendor Solve Time:
Solved quickly

Arkose Titan Solve Time:
Dramatically longer

Every layer imposes cost. Every evasion costs more money. Attacking you becomes the worst business decision they'll ever make.

Know Every Device. Understand Every Behavior.

The foundation: truly understanding every device and interaction. Here's how we identify threats by analyzing what devices are, not just what they claim to be.

Advanced device intelligence Multilayered identification strategy analyzes hardware, software, network characteristics and behavioral patterns to create unique identifiers.

Behavioral biometrics Contextualized insights into how devices behave, not just what they are – distinguishing genuine users from bots and bad actors.

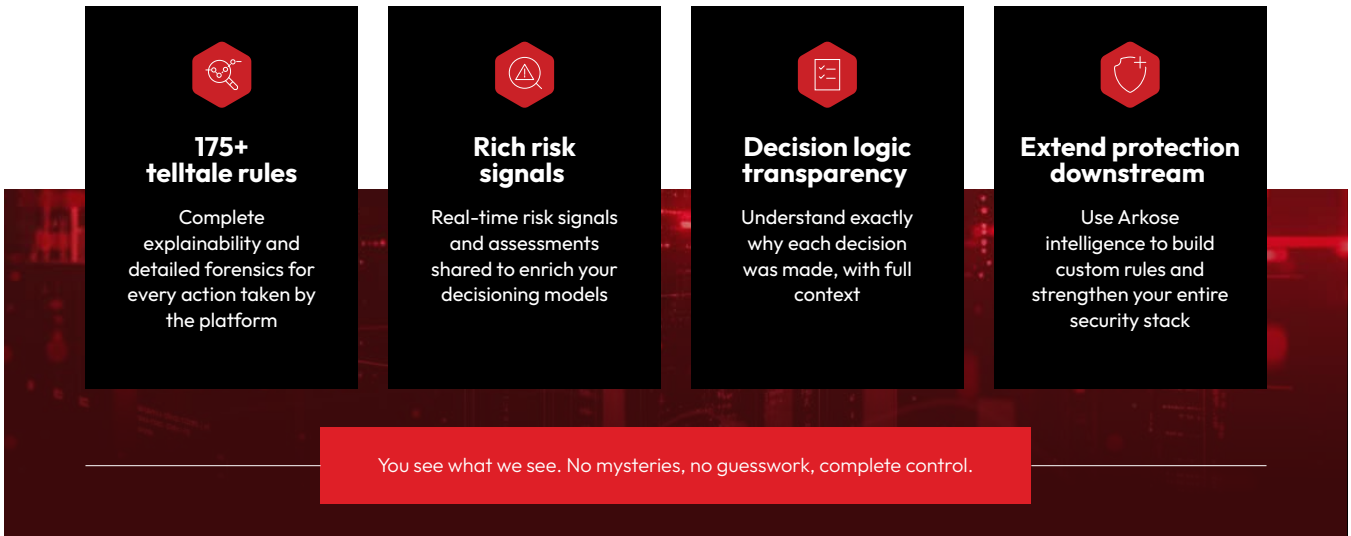
Adaptive enforcement Automated spoofing detection and intelligent rate limiting that responds to suspicious patterns without impacting legitimate users.

Real-time risk decisioning Instant threat assessment at every interaction, analyzing multiple signals simultaneously to determine risk levels and appropriate enforcement actions.

Agentic AI can mimic actions, but it can't mimic authentic device behavior and human patterns. The combination creates an insurmountable barrier for automated attacks.

Data Transparency: Full Visibility Into Every Decision

Most competitors operate as black boxes. Arkose Titan shows you everything.



Round-the-Clock Protection + Intelligence

Our Security Operations Center (SOC) and Arkose Cyber Threat Intelligence Research (ACTIR) unit work in tandem—expert analysts actively managing your defenses and proactively hunting emerging threats 24/7/365. You get both the technology and the team.

Seamless Experience For Legitimate Users

Arkose Titan's sophisticated defenses operate invisibly for your users. Maximum security with zero impact on user experience or conversion rates.

- ✓ Seamless login experiences - Legitimate users authenticate in seconds
- ✓ Zero added friction - No extra steps, no visible challenges for real users
- ✓ Invisible protection - Security operates transparently in the background
- ✓ Maximum conversion - No drop-off from security measures impacting business

99%

of legitimate users never see a challenge

The best security is security your users never see. Arkose Titan delivers both: uncompromising protection without compromising experience.

Take Control With Arkose Titan

Ready to make attacking you unprofitable?

Transform your security posture from reactive detection to proactive economic deterrence.
Schedule a call with an expert today.

About Arkose Labs

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. Trusted by the world's leading consumer brands—including two of the top three banks, Microsoft, Meta, Roblox, and many others—Arkose Labs stops account takeovers, fake account creation, LLM-driven scraping and SMS toll fraud. The platform actively undermines attacker ROI by introducing dynamic friction, making it economically unsustainable for adversaries to persist. Its Security Operations Center (SOC) provides actionable insights from an extensive cross-industry intelligence network, which monitors legitimate traffic and attack patterns across global enterprises. With unparalleled proactive support for internal security teams, Arkose Labs goes beyond conventional security by actively partnering with customers to disrupt organized fraud networks such as Storm-1152. Headquartered in San Mateo, California, the company maintains a global presence with offices throughout APAC, Central America, EMEA and South America.

USA (San Mateo)

Australia (Brisbane)

United Kingdom (London)

Costa Rica (San José)

India (Pune)

Argentina (Buenos Aires)

TALK TO AN EXPERT