Global Education Platform Protects Brand by Stopping AI-Assisted Exam Cheating with Arkose Titan

An online learning platform offering thousands of courses and professional certifications discovered that learners were using agentic browsers to answer exam questions in real time and at scale.

The Challenges

Certification Integrity at Risk: Online exams are vulnerable to AI-assisted cheating, threatening the trust that employers and partners place in platform-issued credentials.

Hard-to-Catch Abuse Vector: AI-powered browsers answer questions faster than any human can read them, a pattern that conventional security tools and in-platform monitoring were not built to detect.

Mid-Exam, On-Demand Cheating: Learners were selectively invoking AI agents for difficult questions while answering easy ones themselves, meaning blocking account creation alone would not solve the problem.

The Arkose Titan Solution

Visibility into Agent Activity: Arkose Titan's Agent Trust Manager analyzed approximately 59 million sessions over a seven-day window, giving the customer their first clear view into the volume and distribution of AI browser activity across exam attempts.

Agent Classification by Behavior: Arkose Titan classified sessions by interaction pattern, identifying AI-driven responses that no human could produce. Each flagged exam was categorized by the specific agent responsible, giving the platform a clear breakdown of who was cheating and how.

Enforcement Through Precision Detection: By identifying which sessions involved AI assistance and which did not (down to the individual question) Arkose Titan gave the customer the precision needed to act with confidence, distinguishing deliberate misuse from false positives.

AI Browser Identification: Perplexity Comet was identified in over 700 flagged exams with a 46% rate of suspicious activity. OpenAI Atlas showed the same pattern at lower volume, concentrated in technical and productivity courses.

Business Results

Visibility into a Hidden Problem: For the first time, the platform could see the true scale of AI-assisted exam cheating — nearly 15,000 agentic sessions and over 1,200 affected exams — giving Trust & Safety leadership the data they needed to act.

Agents Identified and Classified: Arkose classified the specific AI browsers involved as Perplexity Comet and OpenAI Atlas and mapped their behavior patterns, giving our customer a clear understanding of which agents were being used, how often, and in which courses.

Foundation for Policy and Enforcement: Armed with definitive evidence, the platform can now establish and enforce AI use policies across its certification programs, with attribution precision down to the individual exam and user level.

The visibility, classification, and enforcement capabilities that caught exam cheating at scale are the same ones Arkose Titan brings to account takeover, payment fraud, and AI-driven commerce abuse. One platform, one detection engine, defending across every threat surface where agents operate.

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. © 2026 Arkose Labs. All rights reserved.

©2026 Arkose Labs. All rights reserved.