Social Network Slashes Scraping by 22% and Boosts Legitimate User Engagement

A major social media platform with more than 600 million users, this organization is a prime destination for professional networking and content sharing. Its scale and publicly accessible user data make it a high-value target for automated scraping attacks.

The Challenges

Profile Scraping at Scale: Fraudsters deployed bots to systematically harvest public user profiles, fueling downstream abuse including synthetic identity fraud and targeted phishing campaigns.

Revenue at Risk: User data is the platform's core commercial asset. Large-scale scraping by bad actors was diverting millions of dollars in potential revenue away from the business.

Blunt Tools Hurting Good Users: Existing controls couldn't reliably distinguish automated scrapers from legitimate users, forcing a choice between blocking real users or allowing abuse to continue unchecked.

The Arkose Titan Solution

Behavioral Detection at the Session Level: Arkose Titan monitored for suspicious patterns such as rapid, unauthenticated profile browsing and flagged sessions exhibiting scraping behavior in real time.

Escalating Enforcement for Bad Actors: Suspicious sessions were served interactive enforcement challenges purpose-built to defeat machine vision, with complexity increasing on repeat attempts to erode attacker ROI and make scraping economically unviable.

Zero Friction for Real Users: Legitimate users were rarely challenged, and those who were could resolve it quickly with no disruption to their experience.

Business Results

22% Reduction in Scraping: Automated data harvesting dropped significantly, protecting both user privacy and the platform's commercial data assets.

19% Uplift in Good User Throughput: Legitimate users moved through the platform more freely, with fewer false positives interrupting their experience.

Millions in Revenue Protected: By shutting down unauthorized data harvesting, the platform reclaimed control over its core commercial asset.

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.