Adobe Cuts Fake Account Creation by 90% and Slashes User Friction

One of the world's largest software companies, Adobe serves everyone from independent creators to global enterprises. Its trusted domain makes it a prime target for attackers seeking to exploit account registration for phishing and spam.

The Challenges

Fraudulent Account Creation: Attackers created fake email accounts on Adobe's registration flow to launch phishing campaigns that exploited the legitimacy of Adobe's domain.

Good Users Caught in the Crossfire: Existing defenses challenged 10% of all traffic with CAPTCHA, creating unnecessary friction that hurt sign-up rates and drove excess support tickets.

Limited Detection Insight: The incumbent solution provided only a static risk score, leaving internal teams without enough signal to efficiently triage sophisticated, low-and-slow attacks.

The Arkose Titan Solution

Registration Flow Protection: Arkose Titan was deployed on Adobe's account registration flow, applying real-time risk assessment to distinguish bots, fraud rings and genuine users with far greater precision.

Bot-Proof Enforcement: Suspicious sessions were served challenges purpose-built to defeat machine vision, frustrating automated scripts without impacting legitimate users.

Real-Time Intelligence and 24/7 SOC: Arkose shared raw risk signals in real time and collaborated with Adobe's team to fine-tune detection. Custom telltales tracked suspicious traffic patterns, while the Arkose SOC provided round-the-clock monitoring to neutralize emerging threats.

Business Results

90% More Fraudulent Accounts Detected: Significantly more fake account creation attempts were caught, reducing the volume of phishing-ready accounts being created on Adobe's domain.

80% Reduction in Challenge Rate: Trusted users were challenged at just 2%, down from 10% with the previous solution, delivering a smoother sign-up experience and fewer support tickets.

Leaner Internal Operations: Freed from manual account triage, Adobe's security team redirected time toward higher-value work, improving operational efficiency across the board.

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.