Social Networking App Strengthens Security Posture and Slashes SMS Toll Fraud Costs

This widely used social networking platform serves over 300 million users, primarily in a younger demographic, making it a high-value target for sophisticated cyberattacks.

The Challenges

Fake Account Proliferation:
This customer struggled with bad actors creating fake accounts and needed a way to remove them without harming the user experience.

Rising SMS Costs:
Fraudsters using premium-rate numbers for account verification were driving up SMS expenses, often costing dozens of cents per message.

Latency and Effectiveness Concerns:
The company questioned the effectiveness of its existing security solution and needed a way to reduce latency while scoring session risk.

The Arkose Labs Solution

Proof of Value (POV) Assessment:
Conducted a 3.5-week POV in observatory mode to risk-score transactions and identify "telltale" signals of fraudulent behavior.

Managed SOC Support:
Provided a 24/7/365 Security Operations Center with dedicated analysts and solution architects familiar with the customer environment.

AWS Partnership:
Integrated the Arkose Titan platform seamlessly with AWS CloudFront and WAFv2 to handle high-scale traffic and ensure infrastructure availability.

Dynamic Challenge Orchestration:
Enabled the customer to perform challenge orchestration based on high-field risk data to treat sessions appropriately and prevent fraudsters from entering the funnel.

Business Results

Significant SMS Savings:
Dramatically reduced the volume of SMS messages sent by preventing fraudsters from creating accounts, directly lowering security costs.

Improved Risk Classification:
Utilized over 80 data fields to classify risk into medium and high categories, identifying a higher number of dubious login attempts.

Superior Posture & ROI:
Achieved a "trifecta" by improving end-user security, removing bad actors, and demonstrating direct business ROI.

Collaborative Security Playbook:
Empowered the customer to co-write customized security playbooks, providing a unique level of vendor interaction and proactive monitoring.

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.