Dropbox Protects Millions of Accounts, Slashes Intervention Rates 70%

With over 600 million registered users across 180 countries, Dropbox is a trusted repository for critical data that requires a high-priority approach to account integrity.

The Challenges

Target for Mass Abuse:
Dropbox was a prime target for fraudsters attempting account takeover (ATO) and abusing the sign-up process for account enumeration.

Friction-Heavy Legacy Tech:
Previous spam and abuse tools provided excessive friction, disrupting the login experience for legitimate users without effectively stopping attacks.

Seamless Security Requirement:
The company needed a "first line of defense" that could stop organized fraud while providing a frictionless experience for its global user base.

The Arkose Labs Solution

Intelligent Risk Decisioning:
Implemented the Arkose Titan platform to analyze real-time signals and behavior patterns to determine if an authentication challenge is necessary.

Adaptive Authentication:
Depending on the session risk profile, the solution adjusts the complexity of challenges, ensuring they remain easy for humans but resilient to machine vision automation.

Machine Vision Innovation:
Employs challenges that diminish the profitability of attacks by making them economically non-viable for fraudsters to solve at scale.

Business Results

70% Lower Intervention:
Successfully slashed intervention rates for legitimate customers by 70%, significantly improving throughput.

Resilient ATO Defense:
Built greater resilience against account takeover and stopped the abuse of new account registrations.

Reduced Operational Burden:
Lower intervention rates reduced the volume of customer service tickets and the associated costs for in-house teams.

Long-Term Deterrence:
Shifted from reactive defense to proactive deterrence, keeping millions of accounts protected from evolving attack patterns.

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.