Arkose Labs

Social Media App Prevents 300M Spam Attacks a Month with Arkose Labs

CASE STUDY

Social Media Networking App

Business Problem

- Bogus new account creations
- Millions spam and phishing attacks
- Decreasing legitimate activity due to abuse

Solution

- Arkose Labs replaced reCAPTCHA
- Spam intercepted and challenged
- Never blocked users

Results

- Decrease of 300m spam reports in 30 days
- Automated attacks became untenable
- Fraudsters and click farms frustrated

Overview

One of the top 10 most downloaded social networking apps was receiving hundreds of millions of spam attacks every month. The app was favored by many for its largely unregulated registration web application, which preserves user anonymity by allowing accounts to be registered without a telephone number being provided. Spam had become such a significant problem for the app that it introduced a new team of specialists dedicated to eliminating the problem.

The Business Problem

Abuse was primarily driven through high volumes of spam messages that targeted users with phishing attacks, inappropriate friend requests, and other activities that ultimately lured users into sharing personal financial information. Attackers monetized these spam attacks by automating their operations to achieve economies of scale.

The ongoing problem placed the app under intense scrutiny. Automated spam attacks had become so frequent that the app measured a month-on-month decrease in user acquisition. Numerous unsuccessful attempts at stopping the attacks meant that customers had increasingly negative perceptions of the app.

reCAPTCHA, ultimately proved incapable of stopping automated processes from exploiting the app, and frustrated legitimate users. Attempts to manually block questionable users led to extensive false positives, with many abandoning the app after being misclassified as inauthentic. Custom defenses, which were built in-house, also provided little long-term resistance to attackers, who were continually changing tactics and investing more resources to overcome the app's defenses.

The Arkose Labs Solution

The company decided to deploy Arkose Labs in order to identify risky activity and use interactive enforcement challenges to intercept spam. Arkose Detect, a sophisticated risk engine, worked in hand with Arkose Enforce, a challenge-response system to provide targeted friction.

Attackers made a number of high-profile attempts that sought to bypass enforcement challenges through automation, but the system remained uncompromised and was able to eliminate automated attacks. Therefore, attackers were forced to shoulder untenable operational costs that would not yield a return on investment.

Frustrated by their failed attempts to automate a work around, attackers operationalized digital sweatshops, where human users are paid to remotely solve hundreds of authentication challenges per hour. This activity has many distinct characteristics that are clear telltales, and Arkose Labs was able to intercept such requests to appropriately classify them as inauthentic.

Demonstrated Results

Within 30 days of trialing Arkose Labs, the social media app measured a decrease of 300 million spam reports per month before the solution was deployed. By making it very costly to attack, Arkose Labs was able to push attackers beyond the window of economic opportunity necessary to commercialize their abuse. Since first implementing the solution, automated spam operations have virtually disappeared from the social media app.

The solution protected the app against different automated attack vectors, while simultaneously removing the risk of blocking legitimate users. This protected the commercial viability of the app, with less true users deterred by spam on the app.

The Arkose Advantage

Powerful Remediation:
Challenges on the Arkose Labs platform can not be solved by automated scripts, even those using advanced machine vision technology.

Managed Services:
Arkose Labs works with businesses as true partners in fighting fraud, delivering custom insights.

Evolving Platform:
Arkose Labs solution adapts to new threats and has a constant feedback loop between risk assessments and challenges.

Seamless Customer Experience:
Good users are never blocked, which eliminates the false positives that hinder customer experience.

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a 2020 Cool Vendor, its innovative approach determines true user intent and remediates attacks in real time. Risk assessments combined with interactive authentication challenges undermine the ROI behind attacks, providing long-term protection while improving good customer throughput.

Schedule Demo

demo@arkoselabs.com
(800) 604-3319
arkoselabs.com