Arkose Labs

ARKOSE LABS HELPS INSURER KEEP ATTACKERS OUT OF CLAIMS

CASE STUDY

Customer: A Major Consumer Tech Insurance Company

Industry: Insurance

Business Problem

- Client's customers were frequently targeted by phishing scams.
- Fraudsters abused stolen credentials to submit fake claims and get free phones.
- This ultimately hurt revenue and damaged customer experience.

Solution

- Arkose Labs deployed on claims funnel.
- Bot activity detected and fed anti-automation challenges.
- Human fraud rings also were served resources-sapping challenges.

Results

- Nearly all bot activity stopped.
- 98.2% passive mode on good users.
- 5.5 hours per day sapped from human sweatshops.

Overview

The client is a leading insurance provider for smartphones, tablets, appliances and other consumer electronics with nearly 300 million customers globally. The company offers robust insurance policies to protect mobile devices and partners with many of the top wireless network providers around the world. Its popularity and large customer base makes it a target for fraudsters.

The Business Problem

Targeted phishing attacks were carried out against customers by attackers pretending to be the client, saying they needed certain information about the insurance policy. Fraudsters then used that policy information to submit claims and get free phones and other devices, which they would resell on the black market. This fraud was costly to the firm and its wireless clients, as well as negatively impacting the end-user. To ensure a seamless user experience and protect its customers, the company needed a cutting-edge fraud prevention solution.

Arkose Labs Solution

The company decided to deploy Arkose Labs on its funnel for insurance claims. When fraudsters arrived at the insurance claim form, Arkose Labs would detect bot activity and feed it enforcement challenges that automated scripts were unable to solve. The platform also uses real-time data -- along with working together with the client's internal data analyst team -- to root out human fraud traffic and serve them with increasingly complex and time-consuming challenges that would sap the fraudster's time and resources. The Arkose Labs platform seamlessly combines best-in-class intelligence and analytics with adaptive step-up challenges that are designed against the latest in machine vision technology, meaning even the most advanced bots can't bypass it. At the same time, human fraud rings that attack sites are identified and fed increasingly complex challenges so that they give up their effort entirely.

Demonstrated Results

Shortly after being deployed, Arkose Labs greatly reduced fraud and phishing attacks, with no negative effect on the user experience. Firstly, more than 98% of good users did not see a challenge at all, meaning the Arkose Labs platform accurately detected good traffic from malicious activity. Good users who did see the challenge had a 98.8% pass rate - far higher than other forms of step-up authentication.

At the same time, more than 70% of suspicious traffic immediately dropped off after seeing an enforcement challenge. And increasingly complex challenges fed to human fraudsters led to a cumulative 5.5 hours per day of time wasted by fraud rings attempting to solve them.

Key Advantages

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

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

Evolving Platform: Utilizing machine learning, the Arkose Labs solution adapts to new threats.

Powerful Remediation: Challenges on the Arkose Labs platform can not be solved by automated scripts.

Protect Against Any Attack: The platform defends your business against spam, fake reviews, denial of inventory, new account origination, account takeover and other complex attacks.

"Arkose Labs enables us to continue to deliver the great digital experience our customers have become used to, while eliminating fraud attack and malicious bots."

-Fraud Manager

Schedule Demo

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

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.