Arkose Labs

Fintech Neobank Slashes ATOs by 75% with Arkose Labs

CASE STUDY

Customer: Fast-Growth Neobank

Business Problem

- Bots targeted user accounts for credential stuffing at scale
- Compromised customer accounts were drained of funds
- Rampant attacks severely affected user experience

Solution

- Arkose Labs implemented to protect back end servers from being targeted directly
- Platform detected and stopped bots emulating remote clients and impersonating real users
- Arkose Labs provided actionable insights to remediate future threats

Results

- 75% reduction in ATO attempts
- Slashed compromised account costs previously hitting $100,000 per week
- Resources saved from reduction in resetting credentials on compromised accounts

Overview

The client is one of the world's most prominent fintech firms and provides consumer banking, personal financial management, credit monitoring, and other financial services. It has more than 12 million customers in the U.S. alone. It is known for its digital savvy and ease of use.

The fintech neobank has grown rapidly in popularity and grew its customer base by more than 50% during 2020. Users are attracted to the platform because of its all-digital nature and seamless user interaction.

The Business Problem

However, this digital convenience also led to numerous attacks on the platform. As the platform skyrocketed in popularity, fraudsters targeted the growing number of user accounts. At its peak, the company was seeing about 30,000 failed login attempts per day; the vast majority of these were credential stuffing attacks seeking to compromise customer accounts. This massive amount of requests also put a great strain on the platform's tech infrastructure.

In order to commit credential stuffing attacks as fast as possible, fraudsters would deploy bots that would directly target back-end API services. By bypassing web forms and talking to back-end servers directly, fraudsters could write more simple scripts that would allow them to carry out attacks at greater volume and velocity. Fraudsters would then drain the funds of customers whose accounts were compromised.

The Arkose Labs Solution

The fintech then decided to implement the Arkose Labs Fraud & Abuse Platform to protect its login forms and backend APIs. The solution embeds an Arkose Labs token into the web application or mobile SDK, and each request dynamically verifies that the token has passed from the client to the server. Arkose Labs monitors all traffic for known signals of abuse, using behavioral fingerprints, velocity, and rate monitoring, and a proprietary user IP database.

Known malicious bot traffic is served with a dynamic enforcement challenge; these are 3D visual puzzles generated in real-time. They are designed against the grain of machine vision technology, meaning they cannot be solved by bots.

Arkose Labs' professional services team also worked hand-in-hand with the client to monitor and stop evolving threats and provide actionable insights and clear visibility into threats. Robust dashboards give the client a visual look at traffic and attack patterns.

Demonstrated Results

After implementing Arkose Labs, the fintech saw a 75% reduction in failed login attempts that were associated with credential stuffing attacks. This not only greatly improved the customer experience, but saved the client time and money due to a vast reduction in customer service complaints about compromised accounts. The company also realized efficiency gains due to having fewer compromised accounts; it was losing about $100,000 per week in costs associated with compromised accounts. This figure was drastically reduced after implementing Arkose Labs.

Key Advantages

Adaptive Decisioning:

The Arkose Labs solution collects and analyzes digital intelligence, including data from the originating devices, networks, and locations to gain insights into user intent.

Continuous Intelligence:

Once combined with behavioral analytics, these insights help determine the underlying intent of the user, and an associated risk level is ascribed.

Depth of Challenges:

Suspicious traffic is presented with step-up enforcement challenges. These are 3D images presented in real-time and are designed specifically to foil machine vision technology. The challenges are continually being updated and new ones regularly created.

Seamless Customer Experience:

Good users are never blocked, which eliminates the false positives that hinder customer experience and drain revenue.

360 Degree Fraud Prevention:

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

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