Honey Keeps Millions of User Accounts Safe with Arkose Labs

CASE STUDY

Customer: honey by PayPal

⚠ Business Problem

- User accounts were potential targets for fraudsters
- Client sought to be proactive in protecting accounts
- Sought to stop fraud without impacting user experience

Solution

- Arkose Labs implemented on login and new sign-up flows
- Advanced ML and data analytics classify traffic in real-time
- Long-term deterrence so fraudsters are compelled to stop attacking

Results

- Elimination of bot attacks targeting platform
- Increased good user throughout rate
- User accounts protected from ATO attacks

Overview

Honey, a subsidiary of PayPal, is a digital platform that automatically scans for and applies coupons for consumers during the checkout process. Honey is compatible with more than 30,000 ecommerce sites globally. It also provides a suite of other money-saving tools for online consumers, including notifying shoppers when a price drops on select items, to helping them find the lowest prices for goods online. Overall, Honey has helped millions of people around the world find more than $1 billion in savings in the past year alone.

The Business Problem

Honey's goal was to be proactive in fighting fraud attacks that could target its platform and users, while at the same time not impacting the digital experience for customers. The company is known for its optimal user digital experience and digital ease of use; that's why it took proactive steps to prevent fraud attacks that were targeting its platform. Fraudsters often target user accounts in the digital commerce space in order to do things like change user credentials, manipulate delivery schedules and make fraudulent purchases.

Honey also wanted to proactively defend against automation that would be used in card testing attacks, where bots conduct large-scale testing of stolen payment credentials on ecommerce checkout pages and make fraudulent gift card purchases. Since Honey puts such a high priority on creating a safe and seamless experience for customers, it wanted to address these concerns before they became a larger issue.

The Arkose Labs Solution

Honey decided to implement Arkose Labs to defend against fraud and online abuse. The Arkose Labs Platform classifies traffic based on the underlying intent of users and deploys appropriate countermeasures to remediate attacks in real-time. By going beyond mitigating individual attacks, Arkose Labs delivers a long-term solution that deters fraudsters while enhancing the good user experience.

The Arkose Labs platform seamlessly combines best-in-class intelligence and analytics with adaptive step-up challenges that are designed to stop both persistent attacks from bots as well as coordinated human attacks.

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

Demonstrated Results

Arkose Labs worked with Honey to proactively prevent fraud on its platform, including streamlining the account sign-up process and preventing fraudsters from using stolen or fake user credentials to set up bogus accounts. The platform also stopped ATO attacks targeting user accounts, as well as detected and prevented automated scripts from verifying stolen credentials and card testing.

At the same time, Arkose Labs enabled good users to maintain the same digital experience that had been used to, meaning that customers were not impacted in the fight against fraud. For digital platforms such as Honey, it is imperative to balance eliminating fraud with maintaining a seamless user experience.

The Arkose Labs Advantage

Advanced Risk Classification
Real time signals, historical attack patterns, ML-powered anomaly detection.

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.

Constantly Learning Platform
The Arkose Labs Platform continually adapts to detect and stop evolving threat.

Optimal User Experience
Good users are never blocked, which reduces false positives and helps the bottom line.

Quick Implementation
New customers will see results within days, not weeks or months.

> PayPal's brand is built on the trust of our consumers and we take all steps to prevent fraud and abuse on an ongoing basis. By collaborating with Arkose Labs, we continue to advance security and vigilance to a new level where merchants and consumers alike have even more confidence their transactions are safe.
>
> **Assaf Keren**, VP, Enterprise Cyber Security at PayPal.

Arkose Labs bankrupts the business model of fraud. Recognized by Gartner as a "Cool Vendor in Fraud and Authentication", the company offers an industry-first warranty on account protection. Its AI-powered platform combines powerful risk assessments with dynamic attack response that undermines the ROI behind attacks, while improving good user throughput.

Schedule Demo

demo@arkoselabs.com
arkoselabs.com