Arkose Labs

Healthtech Firm Protects Customer Data Using Arkose Labs

CASE STUDY

Customer: A Major Healthtech Firm

Business Problem

- The company was the target of frequent bot attacks
- ATO attacks sought to compromise customer data
- Needed to stop attacks while not impacting user experience and remaining HIPAA compliant

Solution

- Arkose Labs was implemented on authentication pages
- Arkose Labs detected and stopped bot attacks targeting customer accounts
- Client's team worked closely with Arkose Labs internal experts to quickly remediate any issues

Results

- Nearly 1,000 attacks thwarted per day
- This saved the company upwards of $1,500 per day
- User privacy not impacted, as per HIPAA requirements

Overview

The client is a major healthtech company that offers a digital health savings account (HSA) that works alongside HSA compatible plans, with an aim to make navigating healthcare easier for everyone. It offers debit processing, healthcare deductible spend tracking, and zero fees for individuals and families. The company prides itself on an intuitive digital interface.

The Business Problem

The client is known for its top-notch digital user experience and is a leader in the healthtech space. Maintaining that robust customer experience is vital in attracting and maintaining customers. However, the platform was also the target of frequent account takeover attacks, both because of its all-digital nature, and due to the valuable customer data it held being a part of the healthcare industry.

The company was initially not working with a fraud vendor, and relied on tactics like rate limiting and blocking to fight fraud. However, that affected the customer experience, such as by such as by locking good users out of their accounts. Though some level of friction is tolerated since it operates in an industry that stores sensitive customer data, the company also didn't want an overly onerous process for customers.

Furthermore, these efforts failed to effectively fight bot attacks that targeted the platform. Fraudsters used bots to power account takeover attacks in order to obtain customer data. This information would be used by the attacker to commit downstream financial fraud, or be sold on the dark web.

The Arkose Labs Solution

After examining several vendors, the company decided to partner with Arkose Labs and deployed its platform on the company's login and new account creation pages to solve its fraud problems. Arkose Labs' advanced detection analysis looks at user behavior, rather than identity, to determine bot from human traffic, as well as good human users from fraudsters. Arkose Enforce, a proprietary authentication challenge, is designed to stop even the most sophisticated machine vision technology. This means bots are shut out while good users are not impacted.

Arkose Labs also collects no personal data from any user, except for IP address. This was critical for the client, which must remain in compliance with HIPAA statutes and other healthcare laws around sharing customer data.

The client also benefited from the robust data analysis and customized actionable insight into attack patterns. Other bot prevention solutions act only as a "black box;' just telling clients how much bad traffic got through, not how or why. The client also worked closely with the Arkose Labs internal team of experts, who are able to deliver customized analysis to clients to help remediate any issues.

Demonstrated Results

Shortly after being deployed, they saw a decrease of more than 1,000 fraud attacks per day. This saved the company approximately $1,500 per day, a significant amount of money.

Beyond that, the demonstrated results achieved with Arkose Labs allowed the client's fraud team to get a greater "seat at the table" with executive management to prioritize security initiatives.

"The fraudsters didn't stop attacking, but with Arkose Labs we were now thwarting the attacks. I appreciate that Arkose Labs is not a one-size-fits-all solution, but customized for us. They have great people who are always responsive, and it helps me sleep better at night."

-Head of Security

Key Advantages

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

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

Evolving Platform: The Arkose Labs solution constantly learns to adapt to new threats.

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

Protect Against Any Attack: Arkose Labs protects your business from a wide range of fraud attacks, from the simplistic to the most advanced.

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