

# Fintech Leader Protects Millions of Consumer Accounts with Arkose Labs

CASE STUDY

## Key Results



Elimination of bot attacks targeting its Internet platform



Increased good user throughput rate



Consumer accounts protected from ATO, card testing, and other cyberattacks

## Overview

A leading fintech company that saves millions of consumers more than a billion dollars each year was facing a variety of cyberattacks, including account takeover (ATO), new account fraud, credential stuffing, and card testing. It sought proactive measures to protect accounts without compromising the consumer experience. The company implemented Arkose Labs solutions to protect login and sign-up processes, resulting in the elimination of automated bot attacks, increased throughput of legitimate users, and effective protection of user accounts from account takeovers.

## The Business Problem

The company's primary goal was to proactively fight cyberattacks that could target its platform and users, while at the same time not impacting the online experience for legitimate consumers. This company is known for its optimal user experience and digital ease of use, and it wanted to address these concerns before they became a larger issue. The fintech firm also wanted to defend against automation used in card testing attacks, where bots conduct large-scale testing of stolen payment credentials on checkout pages.

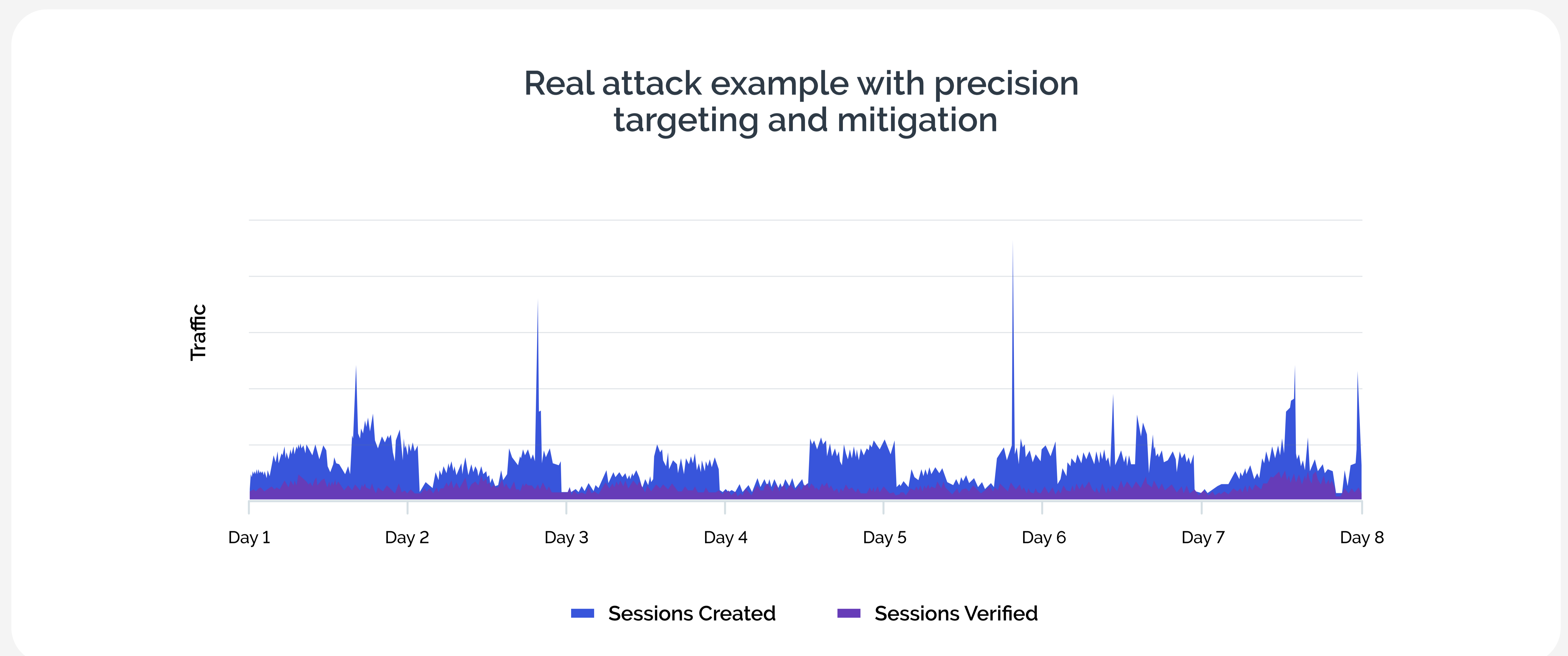
## The Arkose Labs Solution

The company implemented the Arkose Labs platform to defend against cyber threats. The solution 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 cybercriminals while enhancing the good user experience.

The Arkose Bot Manager 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. The strategy of

precision targeting addresses high-risk traffic without hindering the customer experience, ensuring legitimate users navigate unimpeded. Through context-based Arkose MatchKey challenges, suspicious sessions are confronted, effectively thwarting both automated and human-driven account takeover attempts and reducing the profitability of attacks.

The Arkose Labs Security Operations Center (SOC) monitoring and threat management service works hand-in-hand with the fintech company. It observes and stops evolving threats while providing actionable insights and clear visibility into attacks. Robust dashboards also give the company a visual, interactive look at traffic and attack patterns.



## 🔗 Demonstrated Results

Arkose Labs worked with the fintech firm to proactively prevent cyberattacks 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, the solution enabled genuine consumers to maintain the seamless digital experience that they were accustomed to.

“Our 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.”

– VP, enterprise cyber security

Arkose Labs, a trusted leader in bot management and account security, safeguards the world's largest B2C enterprises, Fortune 500 companies, and trailblazing businesses. Its AI-powered Arkose Bot Manager platform provides detection and protection, precisely distinguishing legitimate consumers from malicious bots and diminishing adversaries' financial gains by increasing attack effort and cost. G2 consistently ranks Arkose Labs high for customer satisfaction and extensive market presence, based on verified customer reviews. Innovating the first cybersecurity industry guarantee program, the company offers \$1 million warranties for credential stuffing, card testing, and SMS toll fraud. Arkose Labs is headquartered in San Mateo, CA, with global offices in Asia, Australia, Central America, and South America.

**Schedule  
Demo**

[demo@arkoselabs.com](mailto:demo@arkoselabs.com)  
[arkoselabs.com](https://arkoselabs.com)