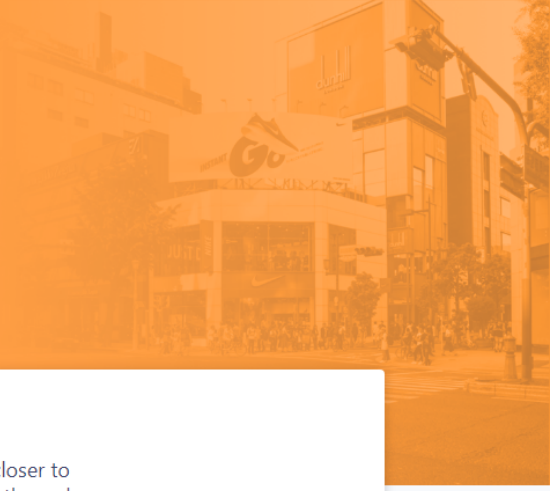
GEETEST



Case Study

A Top-tier Shoe Company

Overview

The top-tier shoe company is cutting intermediaries to get closer to customers and transitioning into a direct-to-customer model through online channels. This new strategy requires a laser-like-focus on collecting customer data to utilize it for predictive analysis.

Challenge

Top shoe company's online stores are targeted by fraudsters who are scalping limited edition or high-demand items all year round. Fraudsters register large numbers of accounts in advance and use automated tools to snap up valuable items during the activity times. After the scalping is complete, the second sale is carried out on 3rd party platforms. As a result, the skewed analytics data affect the top shoe company's business strategy as it relies on the data to make business decisions. Moreover, malicious automation creates an unfair environment for genuine customers, reducing brand loyalty, engagement, and trust.

Solution

In 2018, the top-tier shoe company's online channels deployed Geetest's captcha on its operational gateways like login, add-to-cart, and check-out. After the deployment was complete, Geetest revealed that automated programs made up to 99.9% of the requests during promotions. Geetest's AI-powered risk analysis engine uses behavioral and environmental analysis and intelligence from its global defense network to detect automated software and malicious actors in real-time with pinpoint accuracy and safeguard the online stores. Upon detecting bad actors, Geetest's flexible integration communicates with the threat response mechanisms within the clients' end-to-end fraud detection infrastructure to decisively wipe out fraudsters.

Key Results

Bot detection rate at critical gateways increased by 35%

Chargeback ratio reduced by 32.8%

Number of fake accounts reduced by 90%