HUMAN

Account Takeover Defense Case Study

Top Regional Bank Stops Account Takeover Attacks and Improves Performance During Peak Traffic Periods

This top regional bank has been recognized as one of the top performing banks in the nation. Its business is growing rapidly with 250 locations and nearly $27 billion in assets.

Challenge

As more customers switched to online banking, this top regional bank saw digital fraud attempts skyrocket. The bank discovered that its traditional cyberdefense tools—including web application firewalls (WAFs) and multi-factor authentication (MFA)—could not keep up with the flood of automated bot attacks.

Almost 70% of login requests on the bank's website came from malicious bots. The bots cycled through username/password combinations to try to break into user accounts. Although MFA reduced the likelihood of account breaches, bad bots regularly reached failed login attempt limits. This resulted in customers getting locked out of their accounts and flooding the bank's help desk with calls.

> **"With HUMAN, we have been able to precisely detect and block even sophisticated bots that emulated human behavior, bringing the false positive rate below 0.01%. The solution significantly reduced that amount of time that our team was spending on automated fraud."**
>
> — CISO, Top Regional Bank

Solution

The bank implemented HUMAN Account Takeover Defense to protect its website, mobile apps, and APIs from automated bot attacks. Account Takeover Defense had several key differentiators that lead to the decision:

IMPROVED EFFICIENCY

Utilizing the bank's existing WAF to detect automated bot attacks required continuous tuning and configuration changes that were laborious and time consuming. In spite of this additional effort, a large number of malicious requests were reaching login pages anyway. Account Takeover Defense enabled a behavior-based machine-learning approach with little human intervention.

UNPARALLELED ACCURACY

Account Takeover Defense leverages a combination of behavioral analysis, predictive methods and intelligent fingerprinting to accurately differentiate between malicious bots and legitimate users. The solution was much more effective than the bank's WAF in effectively blocking unwanted traffic.

DID NOT REQUIRE INFRASTRUCTURE CHANGES

Account Takeover Defense integrated seamlessly with the bank's WAF, MFA tool, and edge infrastructure. This allowed the business to avoid spending time, money and hassle on replacement and reconfiguration.

Results

Following the deployment of Account Takeover Defense, the bank experienced several immediate benefits:

- **Enhanced bot protection:** Over the first 72 hours, Account Takeover Defense protected 15.6 million page views. The solution accurately identified and blocked 11.7 million page views from malicious bots, 74.7% of total page views.
- **Maintained the ROI on existing investments:** Seamless integrations with the bank's existing infrastructure components—including its WAF, CDN, web server, and serverless edge compute service—allowed it to avoid huge cost outlays while deploying a highly accurate bot mitigation solution.
- **Reduced burden on customer support:** Positioning Account Takeover Defense between the WAF and the MFA significantly reduced the amount of malicious requests that reached the MFA pages. This enhanced performance, decreased the number of locked accounts and improved customer satisfaction.
- **Restored business and customer confidence:** Account Takeover Defense provided a frictionless yet secure banking experience for customers. The security team was confident that Bot Defender had them covered, so they could focus on more strategic tasks.

About HUMAN

HUMAN is trusted by the world's leading enterprises and internet platforms to prevent, detect, and respond to cyber attacks with unmatched scale, speed, and decision precision across their advertising, application, and account surfaces. Safeguard your customer journey end to end with complete confidence by consolidating with the Human Defense Platform.