

Application Protection Case Study

FanDuel blocks credential stuffing and ATO

FanDuel Group is an innovative sports-tech entertainment company that is changing the way consumers engage with their favorite sports, teams and leagues. FanDuel Group's portfolio includes products for sports betting, casino, daily fantasy sports and horse racing. The premier gaming destination in the United States, the company has **more than 12 million customers and a sports betting presence in 50 states.**

Problem

FanDuel experienced unprecedented growth in 2018 following a US Supreme Court ruling that allowed wagers on professional sporting events in the US. As the company's popularity and product portfolio grew, it became a large target for account takeover (ATO) attacks and experienced up to 10 million malicious login attempts per day.

FanDuel originally explored a homegrown bot management tool, but ultimately pivoted to consider vendor offerings instead.

"We seamlessly integrated Application Protection at our platform edge [AWS CloudFront] to ensure maximum protection against automated bot attacks, but also to minimize latency."

— Alan Murray, Senior Director,
Architecture at FanDuel

Solution

FanDuel implemented [HUMAN Application Protection](#) because of its ability to protect against the volume of attacks its platform had to endure. In addition, HUMAN delivered the following benefits that allowed FanDuel to mitigate ATO attacks without sacrificing their users' online experience:



Accurate bot protection

based on behavioral analytics, advanced machine learning techniques and predictive models that blocks a wide range of automated attacks



Custom parameters

allowed FanDuel to store specific data points, which was a key differentiator for the company



Seamless integration

with AWS CloudFront allowed FanDuel to integrate HUMAN via an edge Lambda function, preserving page load performance and ensuring low latency



Improved efficiency

and optimized the use of FanDuel's internal security resources and infrastructure costs.



Helpful customer support

available 24/7/365 via Slack, email or phone.

In addition, FanDuel was impressed with HUMAN's innovative product portfolio. They were particularly interested in our ability to flag and stop logins with compromised credentials in real time. Part of Account Takeover Defense, this capability proactively mitigates credential stuffing attacks and allows FanDuel to get ahead of account fraud.

Results

Application Protection turned away **99.9% of malicious inbound traffic** to FanDuel's site. The solution routinely blocked **more than 3,000 bad login attempts per second**, even though these requests had already passed through a web application firewall (WAF) and other traditional security controls.

HUMAN's credential monitoring capability gave FanDuel an early-warning system for stolen credentials and proactively mitigated account fraud. This reduced the economic viability of credential stuffing attacks on FanDuel's site and deterred future attempts.

Application Protection is continuously evolving to keep up with new technologies and threats from bad actors. HUMAN has helped prevent ATOs and protected FanDuel's reputation and bottom line.

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.