Application Protection Case Study

Leading Food Delivery Service Company Switches from Homegrown Solution to Fight ATO and Scraping Attacks

This leading online and mobile food-ordering and delivery service company has one of the largest networks of restaurant partners in the world. The company operates through a variety of brands worldwide and processes over half a million orders daily.

Challenge

This leading food delivery service was experiencing unusually huge spikes of unidentified traffic that overloaded its system. These spikes were ten times their normal peak traffic, which drew the attention of both the security and operations teams. Investigation of the traffic showed that many of the spikes were bot attacks originating from countries outside of the company's service areas.

The bot attacks caused performance issues for its customers and restaurant partners, triggering service escalations and complaints. This affected the company's brand reputation, customer loyalty and, ultimately, revenue.

To address the challenge, the security team started building a homegrown bot management system that relied on IP-based rules. The do-it-yourself approach consumed hundreds of hours and took resources away from other key infrastructure projects. Despite this effort, sophisticated bot attacks kept coming. This increased risk to the company's revenue and reduced operational efficiency.

Solution

The company knew it needed to buy a solution, rather than continue to fight bots with in-house resources. HUMAN Application Protection was the clear answer for the following reasons:

ACCURATE BOT DETECTION AND MITIGATION

Application Protection is a machine learning-based bot management solution that protects web and mobile applications and APIs from automated attacks in real time. The solution uses behavioral analysis, predictive methods and intelligent fingerprinting to detect and mitigate bad bots with unparalleled accuracy.

FLEXIBLE ARCHITECTURE WITH EASY INTEGRATION

Application Protection integrated with the company's existing web technology stack, including Fastly. Application Protection supports a wide range of content delivery networks (CDNs), load balancers, and web and application servers.

LOW-LATENCY

Application Protection blocks bots at the edge to improve website performance. Having a low latency solution was especially important given customer expectations for quick online food ordering.

ROBUST ANALYTICS

Application Protection provides real-time attack data, which the food delivery company can easily export to its third-party SIEM tools and use to determine the impact of attacks. By using its existing tools, the company was able to extend the value of its current analytics infrastructure.

SECURITY EXPERTISE AND SUPPORT

The company required vendor support that would act like an extension of their own team. HUMAN offers best-in-class service 24/7/365 via Slack, phone or email.

Results

With Application Protection in place, the food delivery service was able to identify and mitigate malicious bot attacks, as well as rate-limit the flow of good bots traversing their website during any given time. This relieved the strain on their systems, decreased customer service tickets, and helped build back consumer trust.

The company was able to stop reactively fighting bot attacks and instead leverage Application Protection to block bots automatically in real time. This improved operational efficiency and allowed the company's security and operations resources to their core tasks.