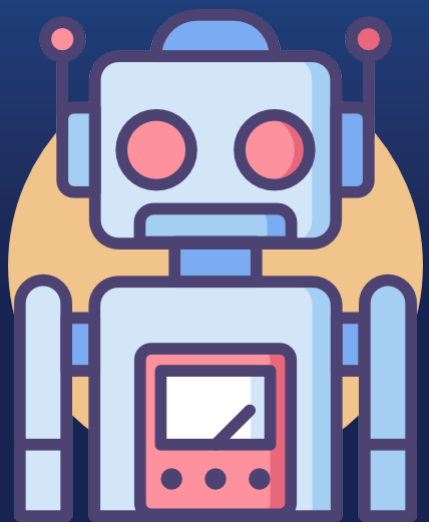
Automated Bot Protection from Bad Bots



Overview

A leading construction company that helps buyers with home projects from the very beginning to the end. They needed a very fast & responsive website with a great user experience for the company's success. But unfortunately, they were affected by Bot attacks from their competitors. The prospect leveraged Prophaze BotCry v2 to protect their website without impacting legitimate traffic.

The Challenges that they experienced

Their website was scraped and abused by the malicious bad bots and these automated bad bots pillaged customer accounts, skewed conversion metrics, and committed fraud. This made the prospect anxious about the possibility of losing revenue due to slowdowns and downtimes. Competitors were using different kinds of scraping bots to keep a watchful eye on the prospect's details, prices, and inventories. Also, they used to collect data and sell it to different competitors who monitored and might even copied the prospect's selling and marketing strategies.

After an intensive selection process, Prophaze BotCry was chosen as the preferred vendor. After deployment, the customer was able to turn on a backend automation solution that thwarted malicious bots from attacking their site and focused on the business of selling products for home improvement.

The Results

Prophaze BotCry v2 helped to utilize their human resource in other focusing areas by avoiding manual bot-blocking with a smarter, and faster approach using the Threat Score Value (TSV). The team would go in and block the traffic using custom rules and data groups at our WAF solution to throw off bad actors or block unauthorized traffic.

BotCry v2 report revealed that 43% of the business's traffic came from malicious bots. The customer was able to reduce man-hours spent in security and testing, and filter out malicious bots automatically that skewed their analytics using the Prophaze Dashboard. They were able to put an immediate stop to entire classes of cybersecurity threats, including account takeovers, web scraping, online frauds, unauthorized vulnerability scans, and application denial of service.