Leading Food Delivery Service Company

Switches from homegrown solution to fight ATO and scraping Attacks

Problem

As a leading food delivery service, it wasn't unusual for the company to experience unexpected peaks in traffic on their website or mobile application. But when it started to experience unusually huge spikes of unidentified traffic that overloaded its system, alarm bells went off. These spikes were ten times their normal peak traffic, which drew the attention of both the security and operations teams. Investigation showed that many of the spikes were bot attacks that originated from countries outside of the company's service areas. The attacks caused performance issues for its customers and restaurant partners, triggering customer escalations and complaints. To address the challenge, the security team started building a bot management system that relied on IP-based rules. They spent significant effort and hundreds of person hours attempting to understand the bot attacks, and working to get ahead of the next one. The attacks spanned scraping of web content and pricing, to account takeover attacks where the personally identifiable information (PII) of its customers was a key target.

The do-it-yourself approach led to resources being reallocated from other key infrastructure projects which impacted customer engagement and security.
The malicious bot activity was heavily affecting the online experience, which in turn was affecting the company's brand reputation, customer loyalty and ultimately, revenue.
The impact was felt internally as well, with ongoing disruption to staffing and constantly shifting priorities. The increased risk to the company's revenue and the reduction in operational efficiency, drove the company to look for a comprehensive bot management solution.

Company

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.

Solution

The leading food delivery service knew it needed to buy a solution versus continuing to fight bots with in-house resources and a homegrown solution. PerimeterX addressed the company's very stringent set of requirements with Bot Defender, a behavior-based bot management solution that protects web and mobile applications and APIs from automated attacks safeguarding online revenue, competitive edge and brand reputation.

- **Flexible architecture with easy integration:** PerimeterX Bot Defender™ provided an architecture that offered the flexibility to fit into the company's existing web technology stack, without impacting system performance. Bot Defender comes

> "The implementation of Bot Defender went smoothly, including the quick and easy integrations with Fastly, our CDN, and Datadog, our operations dashboard. The PerimeterX team continued to exceed expectations through the initial implementation and operated as an extension of our team."
>
> **CISO, Leading Food Delivery Service**

out-of-the-box with over 40 pre-built server-side integrations and its architecture is designed to easily integrate with a variety of widely used web infrastructure, such as the Fastly CDN.

- **Low-latency and manageability:** The low latency operation of Bot Defender was an especially appealing feature given the expectations for fast food delivery and service for which the brand was known. Bot Defender also provided the ability to detect and manage both good and bad bots accurately. The company effectively used Bot Defender analytics to determine the impact of attacks, and easily exported the bot analytics data to its third-party SIEM tools. By using its existing tools, the company was able to extend the value of its current analytics infrastructure.
- **Security expertise and support:** As the company transitioned its security and operations teams back to their day jobs, they required a vendor who would feel like an extension of the company's own team. PerimeterX offers proactive best-in-class service and 24/7/365 support for stopping bot attacks and its team of experts fit the bill.

Results

With Bot Defender, the food delivery service was able to maintain peak system performance on its website and mobile application by blocking bot traffic at the edge. In addition, customer escalations and complaints were reduced, enabling the brand to keep its strong reputation as one of the top companies in the segment.

- **Reduced risk of bot attacks:** Upon implementation, the company was able to identify and appropriately manage bot attacks, relieving the strain on its systems and regaining control of the customer experience. The company was able to both mitigate the malicious bots that were taxing their systems, and to rate limit the flow of good bots traversing their website during any given time.
- **Improved operational efficiency:** The company was able to transition from fighting bot attacks reactively to proactively leveraging the behavior-based capabilities in Bot Defender. Rather than utilizing internal resources to keep ahead of the next attack, the company was able to leverage Bot Defender to improve operational efficiencies and return its security and operations resources to their core tasks.

> "We were able to transition from fighting bot attacks reactively to proactively leveraging the behavior-based capabilities of Bot Defender and regain control of the customer experience of our service."
>
> **CISO, Leading Food Delivery Service**

About Us

PerimeterX is the leading provider of application security solutions that keep your business safe in the digital world. Delivered as a service, the company's Bot Defender, Code Defender, and Page Defender solutions detect risks to your web applications and proactively manage them, freeing you to focus on growth and innovation. The world's largest and most reputable websites and mobile applications count on PerimeterX to safeguard their consumers' digital experience. PerimeterX is headquartered in San Mateo, California and at www.perimeterx.com.

© 2020, PerimeterX, Inc. All rights reserved. PerimeterX, the PerimeterX logo, PerimeterX Bot Defender, PerimeterX Code Defender and PerimeterX Page Defender are trademarks of PerimeterX, Inc. All other brand or product names are trademarks or registered trademarks of their respective holders.

perimeterx

www.perimeterx.com