perimeterx | Case Study

Global E-commerce Retailer

Prevents Account Takeover, Carding Attacks and Review Fraud with PerimeterX

Company

This leading global e-commerce retailer distributes vitamins and supplements to customers globally through its website and mobile application.

Problem

The company was experiencing a high volume of account takeover (ATO) and carding attempts on their e-commerce website. ATO is when an attacker gains access to someone else's account to perform account abuse or sell the validated credentials. In this case, attackers were performing a type of ATO called credential stuffing, which involves validating stolen usernames and passwords for future use. In carding attacks, cybercriminals use bots to test lists of stolen credit, debit and gift card details on merchant sites. Without a bot management solution in place, their security team was working around the clock to stop attacks in real time.

The company also noticed attackers were using bots to automate fake reviews and 'like' the reviews in order to take advantage of monetary incentives. Along with the financial implications of rewarding attackers for leaving fake reviews, it compromised the authenticity of the website's reviews, making it difficult for real human customers to use the reviews to help with their purchasing decisions.

> "When it comes to detection, nobody does it better than PerimeterX. They make sure the bots get all the friction without touching the customer experience."
>
> Security Engineer, Leading Global E-commerce Retailer

Solution

The company needed a solution that would accurately identify and block malicious bot activity without impacting their user experience. It tried three bot management solutions, but found PerimeterX Bot Defender to have the most robust detection capabilities, including:

Protection against ATO and carding attacks: With its sophisticated machine learning, Bot Defender detects malicious behavior on websites in real time, stopping the most advanced bot attacks.

Product review monitoring: Bot Defender applies the same learning techniques to predict when a product review or rating is likely to have been submitted by a bot and challenges the review before it is published.

aws PARTNER

Flexible architecture with easy integration: The open architecture of the PerimeterX platform allows Bot Defender to easily interface with the company's existing web technology stack, including Amazon Web Services (AWS). Since Bot Defender sits in front of their AWS instances, it blocks malicious bot attacks before they reach the servers, maintaining performance and reducing overall server load. This ensures low-latency without adding an additional layer of in-line traffic processing. Bot Defender can also seamlessly integrate with a wide variety of CDNs, including Amazon CloudFront with AWS Lambda, to protect services hosted on AWS.

Results

The company saw immediate value from using Bot Defender as part of their multi-tier security strategy. The security team was impressed with the ability of Bot Defender to proactively fight malicious bot activity without impacting website performance or creating changes to their infrastructure.

Protect against ATO and carding attacks: The number of malicious bot attacks dropped dramatically, increasing website performance and customer satisfaction.

Prevent review fraud: The company significantly reduced the number of fake reviews being left on its product pages, restoring customers' confidence in using the website's reviews to inform purchasing decisions.

Increase operational efficiency: With the new solution in place, 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 core tasks.

> "We've seen a significant improvement in our ability to proactively prevent attacks which really takes the pressure off our team. Customer complaints have also decreased now that accounts are secure and we no longer have outages due to spikes in credential stuffing attempts."
>
> Security Engineer, Leading Global E-commerce Retailer

aws **Available in AWS Marketplace**

About PerimeterX

PerimeterX is the leading provider of solutions that detect and stop the abuse of identity and account information on the web. Its cloud-native 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 while disrupting the lifecycle of web attacks. PerimeterX is headquartered in San Mateo, California, and at www.perimeterx.com.

perimeterx
www.perimeterx.com