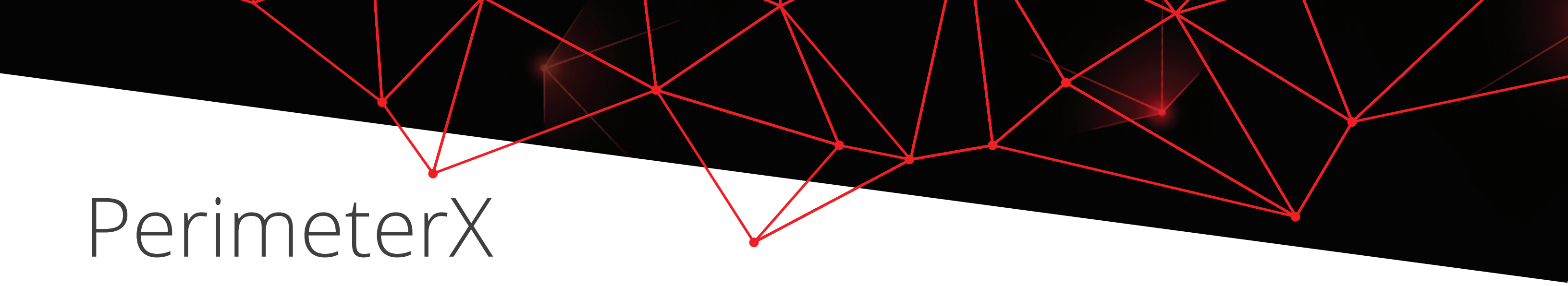


PerimeterX Bot Defender for Digital Commerce

PerimeterX Bot Defender prevents automated attacks by detecting and protecting against malicious web, mobile and API behavior.

Digital Commerce providers depend on safe, reliable, and seamless buying experiences for customers. With the increased usage of mobile, digital commerce providers now have an additional channel to interact with customers which opens a parallel door for automated bot attacks. An attractive site for customers is also an attractive site for bots. Bots hijack accounts through advanced account takeover attacks (ATO), scrape for product and pricing information, impact your marketing budget through click fraud, and skew your web and mobile metrics affecting your bottom line. It is estimated that online sales will surpass $530 billion by 2020* making it a prime target for attacks.

EFFECTS OF BOTS ON DIGITAL COMMERCE

- **Loss of competitive advantage**
- **Inaccurate business intelligence**
- **Financial loss from fraudulent purchases**
- **Reduced conversion from fake accounts**
- **Increased payment network fees**
- **Stressed infrastructure elasticity**

BOTS ARE PROBLEMATIC FOR DIGITAL COMMERCE

Bots aren't particular on the way they access your service, whether through your website, your mobile apps, or APIs. They are after the same thing—to gain access through account takeover, carding, scraping, scalping, and fraud. Preventing bot attacks have previously relied on the rate of attacks, blacklists, and static threat signatures. These methods are becoming less and less effective as bot threats are quick to morph, leaving site owners with thousands or millions of old threat profiles and increasing difficulty in identifying new ones. This in turn, increases the amount of false detections due to outdated signatures resulting in preventing access from legitimate users. Stopping attacks by accurately determining 'is the current user a human or machine' is critical. Attackers can take over real user's browsers, hijacking sessions to bypass most of the techniques used to identify automation in the past. Behavioral detection expands detection and prevention by incorporating hundreds of indicators from network, browser and device-based data, combined with user behavioral patterns to determine if the activity is associated with a human as well if there is malicious human activity, such as malware, often unbeknownst to the user. PerimeterX Bot Defender, incorporates behavioral profiles, machine learning and real-time sensor data to accurately detect and prevent the most sophisticated automated bot attacks.

Digital commerce providers understand the importance of protecting their value and brand from account abuse, carding, scraping and fraud.

ACCOUNT TAKEOVER

Hackers launch account takeover attacks using stolen credentials (user login, password) and tools which are easy to detect after the fact but not easy to prevent in real-time. The key to stopping account takeover and abuse attacks is to focus on behavioral anomalies and characteristics—how the user is interacting with the browser and the application (website or mobile app). Analyzing the user behavior and interaction rather than the request itself provides in-depth information to effectively detect and block malicious users.

CARDING

Payment fraud with credit cards or gift cards is always a concern. Gift card fraud may occur within the account takeover attack—stealing or co-opting gift cards by using or transferring balances—or it may be a direct attack on the commerce system by testing gift card numbers or stolen credit cards. In both cases there are direct loses to the digital commerce provider as well as customer services issues.

SCRAPING

Price is a primary indicator for online purchases. Customers are savvy online buyers—using cost and availability as key drivers for a purchase. While competitors are finding more and more ways to gain product intelligence to push their offerings to the forefront of the buyers attention. Bots are one of the easiest ways of gathering this data. Protecting product inventory, pricing and availability from bot scraping is critical for online success.

CLICK/MARKETING FRAUD

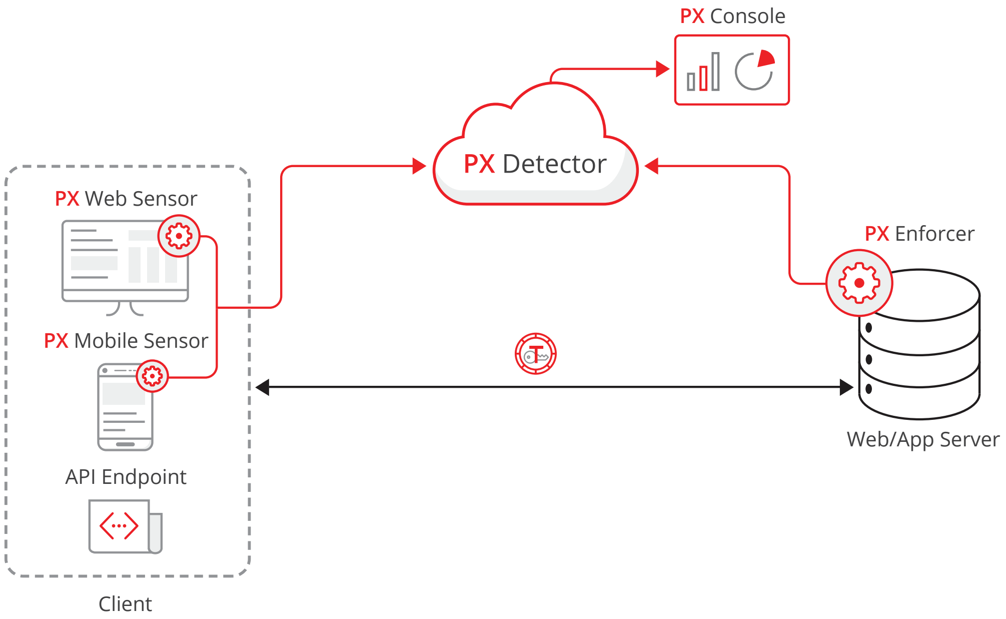
It is known that fraudulent clicks abuse business ROI, and impact company brand, SEO rankings and marketing activities including retargeting campaigns. Bots are employing tactics that mimic users and devices, click through rates and mouse movements evading the majority of detection offerings.

SKEWED ANALYTICS

Visitor data is presumed to be legitimate human traffic. Surges and trends are reported and analyzed to determine the effectiveness of your various campaigns—where to spend on advertising, what referral programs are working, and indicative of the most impactful ways to drive traffic and revenue. Automated bot attacks reduce the effectiveness of your analytics tools by construing your campaign data, inhibiting meaningful insight. The effort to discern actual visitor data from the crush of malicious bot traffic is frustrating without the correct solution.

THE SOLUTION: PERIMETERX BOT DEFENDER WEB, MOBILE AND API

PerimeterX developed behavior-based threat protection technology that advances state-of-the-art detection of automated bot attacks. Our approach is focused on dynamic behavior profiles of real customers—what a good customer looks like. We target the behavior and environment of users, rather than historical signatures of bad bots, focusing on the interactions with the applications, fingerprints from devices and profiling the network characteristics. This approach leads to highly effective identification of bad bot traffic including new threats not previously seen. PerimeterX Bot Defender catches, in real-time, automated attacks with unparalleled accuracy, auto tuning to improve detection while easily integrating into your existing infrastructure enabling detection and blocking within seconds.



*https://www.digitalcommerce360.com/2016/05/02/amazon-accounts-60-us-online-sales-growth-2015/

perimeterx

www.perimeterx.com
info@perimeterx.com