PerimeterX for E-commerce

It's an all-too-familiar pattern: an e-commerce business becomes successful and it doesn't take long before cybercriminals start to follow the money. Securing your web or mobile application is critical to maintaining visitor satisfaction and revenue. But, it cannot come at the expense of poor user experience. The web experience for your users should remain optimized, keeping them on their path to purchase, even while you safeguard them from a variety of evolving threats.

Cyberattacks on the e-commerce industry can result in millions of dollars in lost revenue and chargebacks. In all cases, what makes an e-commerce website attractive to users will also make a site ripe for both competitive and malicious threats.

Protect Your Online Revenue and Brand Reputation

Login Pages

Login pages are critical to e-commerce sites. Once a user logs in, they can get personalized product recommendations, checkout faster and review loyalty points. And, as a business, you learn user buying preferences and can improve their online experience and your conversion rates. Malicious bots target login pages to make fraudulent purchases, siphon off loyalty points and steal users' personal data.

> It's estimated that **40–80%** of retail login attempts are from bad bots

It is no surprise that bot powered account takeover attacks have grown by 65% from 2018 to 2019, and have accounted for $5 billion in losses across online retailers.

The common approach of relying primarily on reCAPTCHAs to detect and block bots fall short. ReCAPTCHAs are easier for bots to solve than humans and can significantly increase user interruptions and ultimately lower conversions.

Top Threat for Login Pages:

Accout Take Over(ATO)

Product Pages

Web scraping bots take the product descriptions, images and pricing on your website—without permission—for use on third party websites. Sometimes that usage is okay if it directs additional traffic to your site. Other times, your content ends up on your competitors' websites. In this case, competitors damage your SEO ranking since search engines detect pages with duplicate content and are unsure which is the original. As a result, it is difficult for consumers to easily find and visit your site.

> Bot traffic can account for 40 to 50 percent of traffic to a site, skewing the analytics and leading to bad business decisions.

As a result, many of your KPIs and metrics, including user tracking and engagement, session duration, bounce rates, ad clicks, look-to-book ratios, campaign data and conversion funnel are unreliable.

Ad injections can come from several sources such as ad networks and browser extensions. Users are redirected away from the intended path to purchase by these unauthorized ads.

Top Threats for Product Pages:


Scraping


Skewed Analytics


Ad Injection

Checkout Pages

Some of the most sophisticated attacks happen on the path to the checkout page or during the checkout process. Since the checkout page is where commerce happens, it is a high-value target for bad actors. A successful attack on the checkout pages can significantly impact customer confidence and brand reputation, lead to loss of revenue, result in chargebacks and regulatory fines.

Carding attacks use malicious bots to test stolen credit cards with small-dollar value purchases on a retailer's checkout pages. Carding represents a massive problem that must be addressed to prevent lost revenue due to credit card chargebacks and frustrated customers whewn they learn their gift cards have been emptied by an attacker.

Digital skimming attacks like Magecart manipulate your checkout page and skim credit card data. Third-party code on your site like your live chat service provider might be compromised and harvesting your user data without your knowledge.

Scalping and hoarding bots impact your entire inventory in seconds. They either continuously add it into shopping carts without purchasing, making it unavailable to real customers. Or, they buy and resell it at inflated prices on another site. On hot product sales, up to 90% of actual checkouts are not human. These attacks sabotage your sales and negatively impact your profits.

Extensions on users' browsers send potential customers away from your site, degrading your users' experience and driving away sales.

Retailers pay a heavy price for online fraud. Every $1 lost to online fraud actually costs retailers three times as much due to the damage done to their reputation, credibility and brand.

> In peak sales periods, **over 40% of all e-commerce orders are fraudulent**. Transactions larger than $500 have a fraud rate of 11.5%.

Top Threats for Checkout Pages:


Digital Skimming/ magecart


Carding


Browser Extension

PerimeterX Protects Your Web and Mobile Applications

PerimeterX safeguards your online business, freeing you to focus on growth and innovation.

PerimeterX products identify and stop attacks before they affect your websites, applications or APIs.

Leveraging machine learning and behavior-based analytics, PerimeterX products detect and block automated bot attacks and client-side threats with unparalleled accuracy. Your online business is protected while preserving user experience and page response times.

Unlike other solutions that limit your web architecture options, PerimeterX is cloud-based and platform-agnostic. Using machine learning, we constantly update our library of attack patterns based on interactions with applications, fingerprints from devices and network characteristics to protect against the next new threat.

Fully Compatible with Your Existing Infrastructure

PerimeterX products can be deployed anywhere and are fully compatible with your existing infrastructure including cloud services and any content delivery network (CDN) solution.

PerimeterX Products for Travel and Hospitality

PerimeterX Bot Defender

Secure your web and mobile applications from automated bot attacks. Detect and mitigate bots used by your competitors to scrape your products and pricing and mess your inventory.

PerimeterX Code Defender

Protect your users' data from client-side attacks like Magecart. Deploy a solution powered by AI and pattern matching that performs runtime analysis to identify anomalous client-side behavior and on modifications to live site code.

PerimeterX Page Defender

Keep your users on the path to purchase. Eliminate browser extensions and ad injections that steal your users and redirect them to competitors.

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.

perimeterx
www.perimeterx.com