PerimeterX for Travel and Hospitality

Preserving your competitive edge in a highly competitive online industry is a constant endeavor. Consumers actively seek the best pricing and availability of travel accommodations and transportation. The user experience of your website makes all the difference to drive both conversions and brand loyalty. It's an interesting dynamic: airlines and hotels both compete and cooperate with search and travel sites. Every travel provider strives to have the best prices, best look-to-book ratio, high customer loyalty, a positive and secure user experience, and zero negative brand associations. Airline seats and hotel rooms are perishable products. Cyberattacks on the travel industry can result in millions of dollars in lost revenue and chargebacks. In all cases, what makes a travel and booking website attractive to customers will also make a site ripe for both competitive and malicious threats.

Protect Your Competitive Edge and Look-to-book Ratio

Login Pages

Login pages are critical to travel sites. Once a user logs in, they can get personalized travel tips and recommendations, checkout faster, and review loyalty point balances. As a business, you learn user buying preferences and can improve their online experience and your conversion rates. Unfortunately, malicious bots target login pages to make fraudulent purchases, siphon off loyalty points and steal users' personal data.

> It is no surprise that bot-powered account takeover (ATO) attacks, in which criminals take unauthorized ownership of online accounts using stolen usernames and passwords, have **grown by 65% from 2018 to 2019.**

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 and Pricing Pages

Web scraping bots take your product descriptions, images and pricing on your website—without permission—for use on your competitor's websites. They keep customers from finding you by hurting your SEO ranking when search engines detect pages with duplicate content.

> Bot traffic can account for 40 to 50% of traffic to a site, skewing your data 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

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, and result in chargebacks and regulatory fines.

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

> In 2019, British Airways paid **$230 million** in regulatory fines—all stemming from a Magecart attack in 2018.

Scalping and hoarding bots impact your entire inventory in seconds. In the case of flight tickets, hotel rooms or vacation packages, bots either buy it out or continuously add it into shopping carts without purchasing, making it unavailable to real customers. These attacks sabotage your bookings and negatively impact your profits. Extensions on users' browsers send potential customers away from your site, degrading your users' experience and driving away bookings.

Digital businesses pay a heavy price for online fraud. Every dollar lost to online fraud actually costs three times as much to recover due to the damage done to their reputation, credibility and brand. For hotels, same-day bookings are far more likely to be booked using a stolen credit card. The criminal is often long gone before the card owner or the hotel figure out the fraudulent transaction.

Top Threats for Checkout Pages:

Digital Skimming/ magecart

Carding

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 cloudbased 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