fastly

perimeterx

Fastly & PerimeterX

Protect your website from malicious bots with Fastly and PerimeterX Bot Defender

The Fastly and PerimeterX value

With malicious bot activity on the rise, and becoming more sophisticated, effective bot mitigation needs to start at the edge. Fastly has partnered with **PerimeterX** to offer complete coverage of bot detection and mitigation at the edge, without impacting performance.

Fastly and PerimeterX Bot Defender™ protect your site from a range of malicious bots, from basic automated ones to more sophisticated fourth generation bots. PerimeterX Bot Defender is the only solution capable of detecting highly sophisticated man-in-the-browser bots which reside inside infected browsers and control users' machines or use advanced browser automation tools. Unlike other solutions, Fastly and PerimeterX enable you to protect both cached content and origin content, so you can keep more in cache without the risk of bot abuse.

54.4% of all web traffic comes from human users — the rest comprises of good bots (27%) and bad bots (18.6%).

Aberdeen Group, September 2016

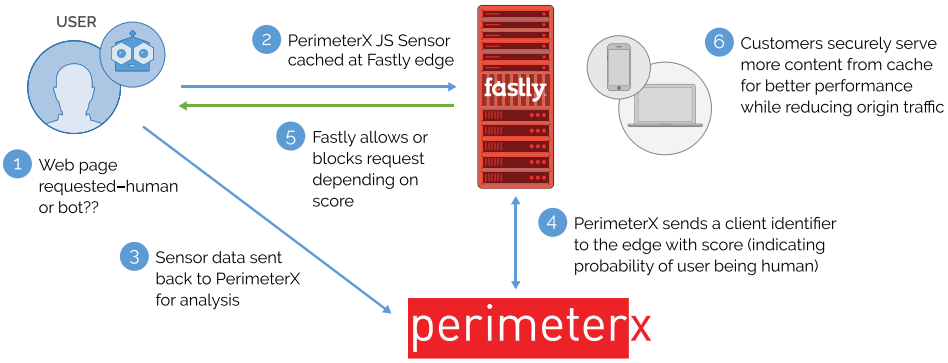
How does it work?

The solution involves placing a snippet of JavaScript on your site. This loads the PerimeterX Sensor into the user's browser to gather behavioral and statistical data. Data gathered is then analyzed in real time to generate a trust score for a client. The score is encrypted and stored in a cookie which is placed on the client's device for further identification. PerimeterX provides real-time dashboard visibility to all client behavior trust scores (including misbehaving clients), and detailed forensics and reporting.

When a browser requests access to your website, Fastly caches and delivers the PerimeterX JavaScript sensor, in addition to the requested content. Based on the PerimeterX trust scores set for each client, Fastly can either allow or deny access to your website. Additional levels of control can also be applied before granting access. For example, you can further validate the client's authenticity using Google's reCAPTCHA or serve a redirect to an error page, or honeypot breaking automation. You can also set additional header values for further client isolation and tracking.

If the client doesn't allow PerimeterX to set a cookie, it's a good indicator that the request is coming from a bot and not a human. In this case, Fastly can merge additional header information, fetched through a dedicated API with PerimeterX, to validate the client and block abuse.

Fastly and PerimeterX combine powerful behavior-based bot detection with mitigation at the network edge. By extending your abuse policy to the edge, you can significantly reduce malicious origin traffic, saving on backend server resources and reducing fraud.



Fastly and PerimeterX Bot Defender

Protect against:

- Account takeover
- Fake user creation
- Carding
- Marketing theft
- Content theft / scraping
- Checkout abuse / scalping
- Layer 7 DDoS attacks

Business benefits

Prevent account takeover

Bot networks often use lists of common and stolen user and password combinations, attempting to log into client accounts. Those accounts contain sensitive information which might be sold or abused.

Protect marketing budget

With affiliate fraud, malicious bots collect referral fees for customers who visit your website directly without being referred by an affiliate. Ad click fraud acquires fake traffic through bots clicking on online ads. These activities can cause you to allocate marketing budgets based on fraudulent campaigns, thereby negatively impacting your return on investment. Bots imitating human behavior can heavily skew your analytics, hide actual trends and obfuscate your actual user behavior.

Control pricing & content strategy

- **Price Scraping –** Advanced bots can create fake accounts and perform "price intelligence" services to help competing websites, selling similar products, to be slightly cheaper and appear higher in various price comparison engines.
- **Scalping –** Bots can mimic human behavior, buying from websites that sell tickets or limited stock merchandise and selling them at a much higher price. This activity skews the supply and demand balance, making it hard to control the buyer's experience.

Block Layer 7 DDoS attacks

Fourth generation bots can imitate legitimate browser behaviors, making them much harder to detect at layer 7. PerimeterX's Bot Defender detection can differentiate between a real user and a man-in-the-browser bot. Fastly's enforcement capabilities can then block this advanced threat vector at the CDN edge, protecting your website from disruptive DDoS attacks.

Getting started

For more information, on Fastly and PerimeterX Bot Defender, please contact us at PerimeterX@fastly.com. We would be happy to set you up with a trial account to explore the benefits of this joint offering.