PerimeterX Bot Defender on Lumen

Bot mitigation: Stop automated bot attacks

Consumer-facing websites are at greater risk from malicious bots than ever before. Due to the increasing adoption of distributed architectures, the explosion of third-party APIs, and increasingly sophisticated cyber attackers, organizations with digital e-commerce platforms, travel and hospitality sites, or any other application that collects user data have no choice but to prioritize bot mitigation.

Meeting these threats head-on requires a bot risk management solution that is prepared for a wide array of modern attack methods. Credential stuffing, account takeover (ATO), hoarding, and carding are just a few of the schemes that cyber security solutions must be able to thwart. Staying one step ahead of the next threat with a proactive bot risk management solution is key to help ensure that you and your end users are protected.

Stay one step ahead of attackers

PerimeterX Bot Defender uses machine learning and behavior-based analytics to help ensure that your website or application is protected against bots and threats by tracking attack patterns, fingerprinting devices and monitoring network characteristics to stop attacks at the source.

Rapid, low-maintenance deployment

Pre-integrated into the Lumen global edge, PerimeterX Bot Defender can be up and running in a matter of hours without complex development work. Your properties can be protected around the cloud while preserving end-user experience and page response times.

Dedicated security expertise

Rely on the intelligent fingerprinting, behavioral signals and predictive analysis capabilities of PerimeterX Bot Defender to detect bots on your web and mobile applications and API endpoints with exceptional accuracy.

> **Bot attacks increased 106% YoY in 2021."**
>
> – Automated Fraud Benchmark Report. PerimeterX. March 2022

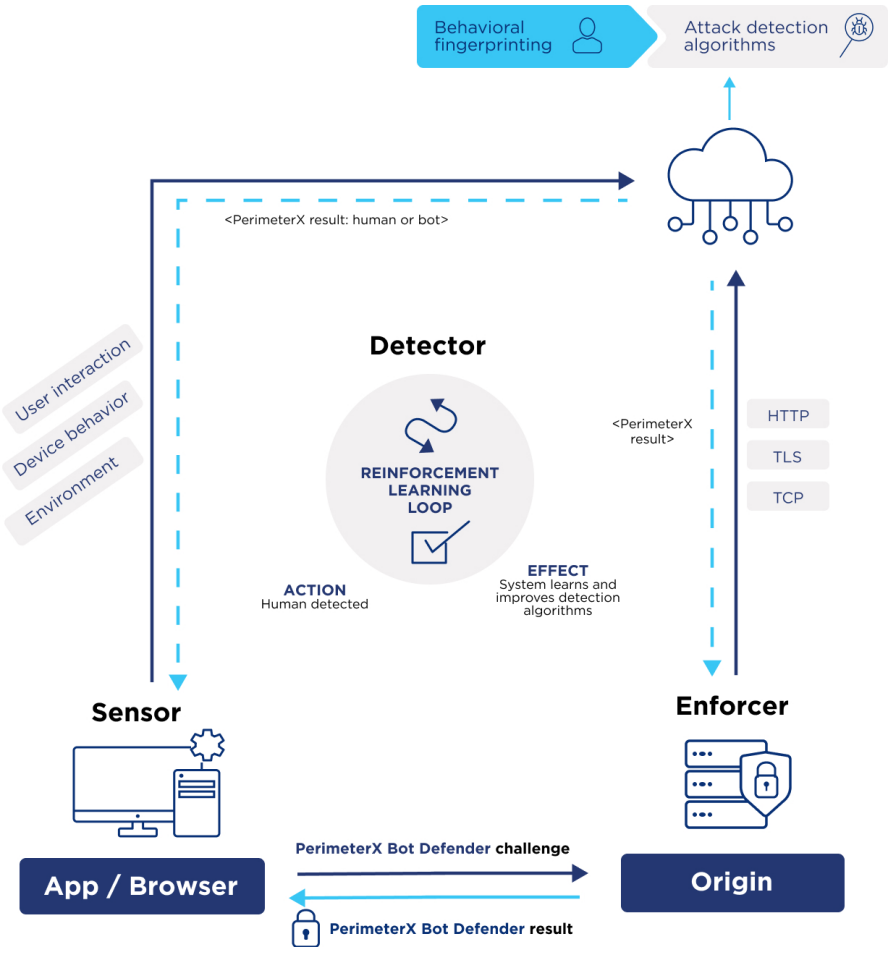
LUMEN TECHNOLOGIES

How it works

Collector: collects and sends hundreds of client-side indicators to the Detector. Signals are used to validate human vs. bot activity, as well as to identify suspicious scripts and malicious browser extensions. The Sensor collects signals asynchronously for the entire portfolio.

Detector: Machine learning-based, the Detector learns common characteristics of human interactions, correlates them with customer-defined policies and updates the Sensor with new intelligence. It maintains a repository of known attacks, shared among all customers. Updates are frequent based on billions of daily data points.

Enforcer: is the gatekeeper for threat response policies generated by the Detector. It enriches and mitigates automated traffic according to business needs. The Enforcer also learns and updates the Detector with relevant data. It can be deployed inline into any existing web architecture.



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.

Why Lumen?

At Lumen, we understand the security pressures our customers face. We offer a holistic and comprehensive approach to security. Lumen provides the flexibility your DevSecOps team requires for rapid, agile deployment – delivered via our common automation and orchestration platform: Lumen Application Delivery Solutions.

perimeterx

lumen.com | application.delivery@lumen.com

LUMEN® TECHNOLOGIES