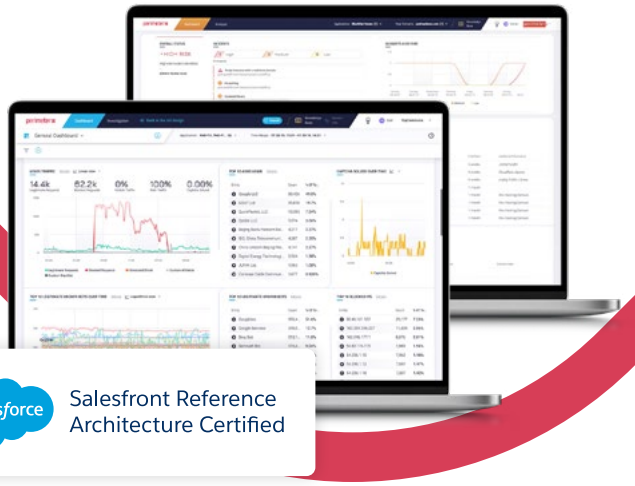
perimeterx | Product Brief

PerimeterX for Salesforce Commerce Cloud



salesforce Salesfront Reference Architecture Certified

Automated bots generate over 50% of the traffic to your website. While some bots are legitimate, such as search engine crawlers, most are unwanted or malicious. These bots try to take over your users' accounts, scrape your content and pricing, abuse your payment services and manipulate inventory. Malicious bots comprise a significant portion of bot traffic, and they continue to expand in numbers and evolve in sophistication. In addition to being security threats, bots also significantly affect operational costs and skew your business analytics which can lead to flawed decisions.

In addition, modern websites are shifting logic to the client side to increase performance and enrich the user experience. They also make extensive use of third-party scripts and open-source libraries to innovate faster and deliver rich new capabilities. These third-party scripts often account for up to 70% of the scripts that power a modern website, are outside of the site owners' visibility or control, create a major client-side blind spot and expose businesses to attacks like Magecart and digital skimming that compromise users' data.

As more and more businesses continue to invest in and grow their online storefronts, there is an increased need for businesses to fight bot attacks and client-side threats, ideally using a single platform. PerimeterX Bot Defender and PerimeterX Code Defender are directly integrated into your Salesforce Commerce Cloud (SFCC) storefront to provide comprehensive bot management and visibility into client-side threats. These solutions give you the flexibility and control to detect and protect your site from automated bot attacks and Magecart attacks in real time.

The PerimeterX Platform deploys out-of-band and mitigates bots at the edge ensuring low-latency without adding an additional layer of in-line traffic processing. The Platform uses a single lightweight JavaScript sensor that embeds easily into your web pages and collects key client-side signals on browser Document Object Model (DOM) activity, including network and storage access, to detect client side threats.

Benefits to Your Digital Business

Reduce Risk From Bot Attacks

Maintain your brand reputation, avoid costs associated with bot-related security issues and increase your users' confidence and trust by stopping bot attacks.

Reduce Risk From Client Side Threats

Detect and prevent digital skimming and Magecart attacks arising from first- or third-party code and ensure compliance with data privacy regulations like GDPR and CCPA

Improve Operational Efficiency

Enable your team to focus on innovation and growth, and save on resource consumption by blocking unwanted bot traffic at the edge and optimizing the use and performance of your web infrastructure.

Bot Defender and Code Defender Use Cases

- Account Takeover (ATO)
- PII Harvesting
- Web Scraping
- Denial of Inventory
- Digital Skimming and Magecart
- Skewed Analytics
- Carding

Login pages provide cybercriminals with the ability to introduce fraudulent purchases, siphon loyalty points and even hijack personal data using malicious bots. Account takeover and carding attacks use malicious bots to test stolen credit cards on checkout pages.

Scalping and hoarding bots can impact your entire inventory in seconds. Web scraping bots steal product descriptions, images and pricing from your website for use on third-party websites that damage your SEO rankings and lead visitors to your competitor. Good and bad bot traffic can skew your analytics so that 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.

Client-side attacks like Magecart and digital skimming can leak your users' data right from the browser, leading to the theft of credit card numbers and other personally identifiable information (PII).

PerimeterX Bot Defender

PerimeterX Bot Defender is a behavior-based bot management solution that protects your websites, mobile applications and APIs from automated attacks, safeguarding your online revenue, competitive edge and brand reputation.

PerimeterX Code Defender

PerimeterX Code Defender is a comprehensive client-side application security solution that protects your website from formjacking, Magecart and digital skimming attacks. It uses behavioral analysis and advanced machine learning to automatically detect vulnerable scripts, suspicious PII access and data leakage from your users' browsers.

How It Works

Collect

The Sensor collects and sends hundreds of non-PII client-side indicators and signals to the Detector. These signals are used for validation of human versus bot activity and identification of suspicious script activity to create the device and browser fingerprints and script baselines.

Detect

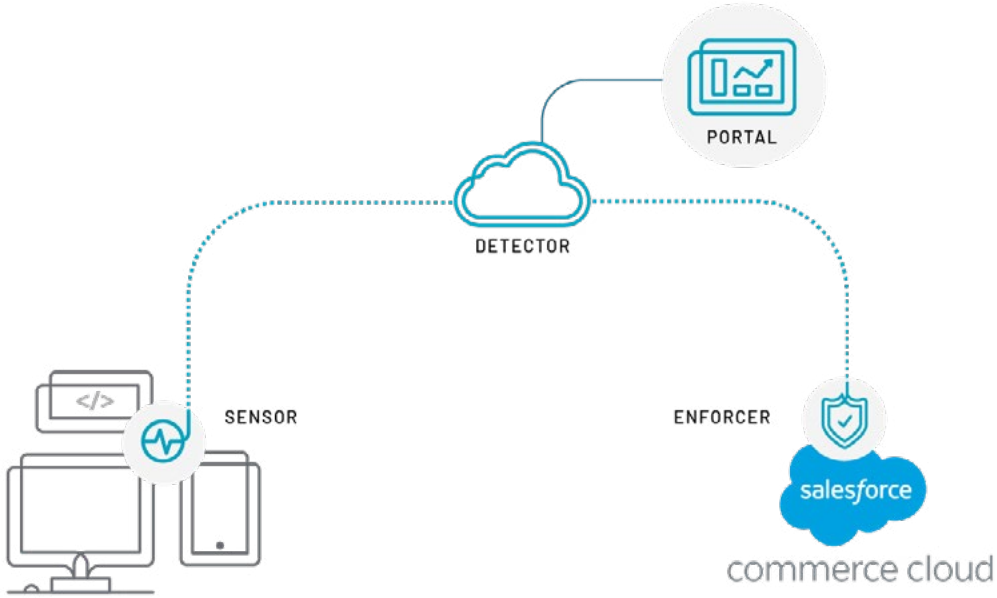
The machine learning (ML) based Detector continuously learns the common characteristics of attacks, correlates it with customer-defined policies and updates the Sensor with new intelligence. The Detector maintains a large, growing repository of known attacks.

Enforce

The 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 continuously learns and updates the Detector with relevant data.

Report

The Portal features advanced reporting and analysis capabilities. With it, you can investigate attacks and create custom reports.



The PerimeterX Advantage

Easy to Deploy and Integrate with SFCC

- Deploy the lightweight JavaScript Sensor quickly and easily into your web pages.
- Utilize the pre-built Enforcer integrations for the CDNs used by SFCC.
- Use certified SFCC cartridges for both Bot Defender and Code Defender.

Low-latency Architecture

- Deploy out-of-band without adding an additional layer of in-line traffic processing.

Full Visibility and Control

- Gain real-time visibility into first-, third- and Nth-party scripts.
- Detect unauthorized PII access, data exfiltration events and known script vulnerabilities.

Behavior-based Learning

- Leverage advanced machine learning models that automatically learn, inventory and baseline all script activity on your web pages.
- Receive prioritized alerts on suspicious script activities.
- Eliminate complex pre-configuration of policies.

Enterprise Level Customer Services

- PerimeterX security experts serve as an extension of your team and are available 24/7/365 over dedicated Slack channels, email or phone.

> We were looking for a solution that could provide us visibility into the client-side scripts. Code Defender was easy to deploy, leveraging the same Sensor and Salesforce Commerce Cloud cartridge as Bot Defender.

Lee Tarver, Sr. Manager, Security Architecture and Engineering, Sally Beauty

About PerimeterX

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