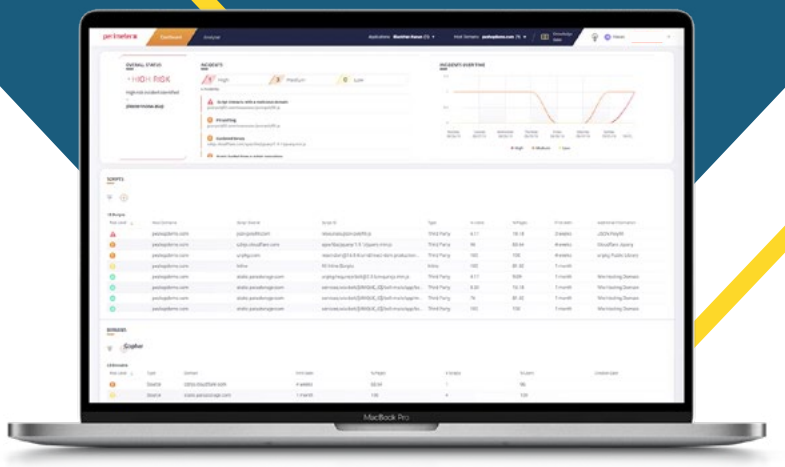
perimeterx | Product Brief

PerimeterX Code Defender

Protect Your Client-side From Magecart and Digital Skimming Attacks



Modern websites shift logic to the client-side to increase performance and enrich the user experience. In fact, almost 70% of the scripts on a typical website are third-party. Website developers need the freedom to innovate using open-source technologies and third-party services while maintaining a safe and secure user experience. These scripts run outside of the site owners' visibility or control, creating a major blind spot. At the same time, infosec teams need visibility and control over the client-side scripts to ensure that users' PII data is protected from data breaches stemming from Magecart and digital skimming attacks and to achieve compliance with data privacy regulations like GDPR and CCPA.

Protect Your Client-side

PerimeterX Code Defender is a comprehensive client-side visibility and protection solution for your website. Using behavioral analysis and advanced machine learning, Code Defender automatically detects and alerts on vulnerable scripts, suspicious PII access and data leakage from your users' browser, thus enabling you to detect and mitigate Magecart and digital skimming attacks in a timely manner.

Code Defender Use Cases

- Digital Skimming and Magecart Attacks
- PII Harvesting

Benefits to Your Digital Business

Reduce Risk of Data Breaches

Prevent data breaches from Magecart and digital skimming attacks. Ensure compliance with data privacy regulations like GDPR and CCPA.

Protect Your Brand Reputation

Defend your brand reputation from Magecart and digital skimming attacks. Ensure a safe user experience and preserve customer loyalty.

Improve Operational Efficiency

Enable innovation at digital speed. Minimize process overhead and streamline DevOps workflows.

The PerimeterX Difference

Easy to Deploy and Integrate Anywhere

Lightweight JavaScript sensor integrates quickly and easily into your web pages. No website architecture changes required.

Analytics and Reporting

Fully-customizable portal provides detailed visibility into script activity, timelines and prioritized actionable alerts.

Easy to Manage

Behavioral analysis and machine learning engine automatically learns, inventories and baselines all script activity on your website. No pre-configuration required.

Extensible Platform

Single JavaScript sensor protects your website against multiple security threats from malicious bots to unauthorized third-party code changes and ad injections on the client-side.

Threat Research Leadership

Dedicated PerimeterX research team of data scientists and cybersecurity experts analyzes billions of data points each day to identify and mitigate emerging threats.

Enterprise Level Customer Services

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

> "We have rigorous security procedures in place for managing third-party scripts, but with a rich portfolio of brands, each with their own websites, governance becomes an ongoing challenge. Having visibility into script changes will help us proactively protect our brands from potential risks instead of relying on manual processes."
>
> Associate VP, IT Security & Risk Management, Top E-commerce Retailer

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