PerimeterX Code Defender™

As logic moves to the front end, attackers are taking advantage of the increased attack surface on the client side. Website front-end code consists mostly of third-party scripts or scripts from third-party libraries, creating an easy target for attackers. PerimeterX Code Defender™ helps you get control of your front end code.

SHIFT TO THE CLIENT SIDE

Modern web sites shift more logic to the front end to increase performance and improve the user experience by rendering and running the logic where the user is. The improved performance is important for customer engagements but creates significant security and privacy risk as scripts are running outside of the site owners' visibility or control, and are exposed to vulnerabilities and malicious activities that will go unnoticed. This increased surface presents new opportunities for attackers to inject malicious code to the front end in order to steal, tamper, and hijack personal data and payment information.

PerimeterX Code Defender™ protects from client-side attacks that are stealing or manipulating your users' data.

BUILDING THE SAFE, MODERN WEBSITE

Modern websites pull code and data from varied sources. Your developers use available code components, libraries, and third-party scripts to build user-friendly web experiences, and offer new capabilities faster. This process often lacks adequate security or quality oversight, and thus may introduce outdated or vulnerable code that exposes your site and users to data loss or compromise. When a script runs in a page it gets access to every element and data on the page. Because it is all happening on the user's browser, it limits visibility into the different operations these scripts perform on the browser or the data and page elements they access. Specifically, if a script is changed, introducing breached or malicious code, it can cause significant damage to your users and business without your knowledge. These scripts may be stealing or manipulating data.

CLIENT SIDE THREATS—WHAT COULD THE ATTACKERS GET BY BREACHING YOUR CLIENT-SIDE CODE

Digital Skimming

Hijack payment and billing data

PII Harvesting

Steal users PII data by snooping or tricking users into providing additional data

Watering Hole Attacks

Leverage the website reach and target specific users to unintentionally install malware

Cryptocurrency Mining

Discreetly leverage the user's browser resources, to mine cryptocurrency

THIRD AND FIRST-PARTY SCRIPTS CREATE RISKS

Third-party scripts, from trusted partners and vendors, and developer libraries can be or already have been breached. Magecart, an online card skimming attack—affected many well-known companies through vulnerable third-party scripts, in what is called supply chain attack, where the attackers target a 3rd party vendor to gain access to the target site, and may go undetected for months. Even when served as first party, external Javascript libraries (open-sourced or vendor provided) used by developers to build applications contain many of the same risks as third-party scripts. External libraries could be breached or contain vulnerabilities, enabling attackers to access, change or manipulate these scripts and gaining access to the users and their data.

Third-party javascripts make up 70% of the scripts running on your website*

PerimeterX Code Defender™ provides visibility into scripts running on the client-side, and alerts on scripts stealing or manipulating your users' data.

PerimeterX Code Defender™ monitors the web page architecture and scripts' behavior, by tracking changes and manipulations to the DOM, activities they perform on the pages, access to elements, and information sent to external domains. Code Defender leverages PerimeterX rich and proven expertise in behavioral analysis, machine learning and data analysis, utilizing advanced models for the most accurate detection and validation of scripts. PerimeterX Code Defender detects and tracks suspicious scripts, new scripts and changes in the behavior of existing ones.

PerimeterX Code Defender™ sees and learns all scripts and associated activities—legitimate and malicious scripts—and flags anomalies including data that is being collected and sent outside to other domains. PerimeterX Code Defender actively collects key metrics on DOM activity, unauthorized scripts accessing user data, suspicious and/or behavioral changes from partner or vendor's scripts and suspicious code injections like malware, extensions, and plug-ins that may be harmful—enabling full visibility of what happens on the client side.

WHY PERIMETERX

1. Expertise in understanding user behavior and detection of data anomalies
2. Proven expertise in client-side implementation with no effect on user experience
3. Deep knowledge and understanding of how attackers think and act
4. Smart learning models with a continuous feedback loop
5. Real-time visibility and alerting
6. Consolidated reporting with easy interaction with SIEM/SOC systems for centralized alert and reporting management
7. Unique out-of-band architecture designed for modern infrastructure
8. Synergy with PerimeterX Bot Defender™

TAKE CONTROL ON THE CLIENT SIDE

Gain visibility

Track and monitor page elements and gain visibility into scripts' activity and alerts on suspicious signs and changes

Prevent data loss/leak

Prevent unwanted scripts from accessing your users data and enforce strict data access policies

Monitor open source and vendor scripts

Track behavior and changes in client-side libraries and scripts

Only 23 percent of developers reported testing for vulnerabilities in components at every release

ABOUT PERIMETERX

PerimeterX is the leading provider of application security solutions that keep your business safe in the complex 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. Bringing together an elite engineering team, security research to continually update its solutions with current intelligence, and best-in-class customer enablement and support, the world's largest and most reputable websites and mobile applications count on PerimeterX to safeguard their consumers' digital experience.

**source: Top 18,000 Alexa websites*

perimeterx
www.perimeterx.com