Feroot Security PageGuard

feroot

An automated JavaScript security solution that protects websites and web applications from client-side cyber attacks in real-time.

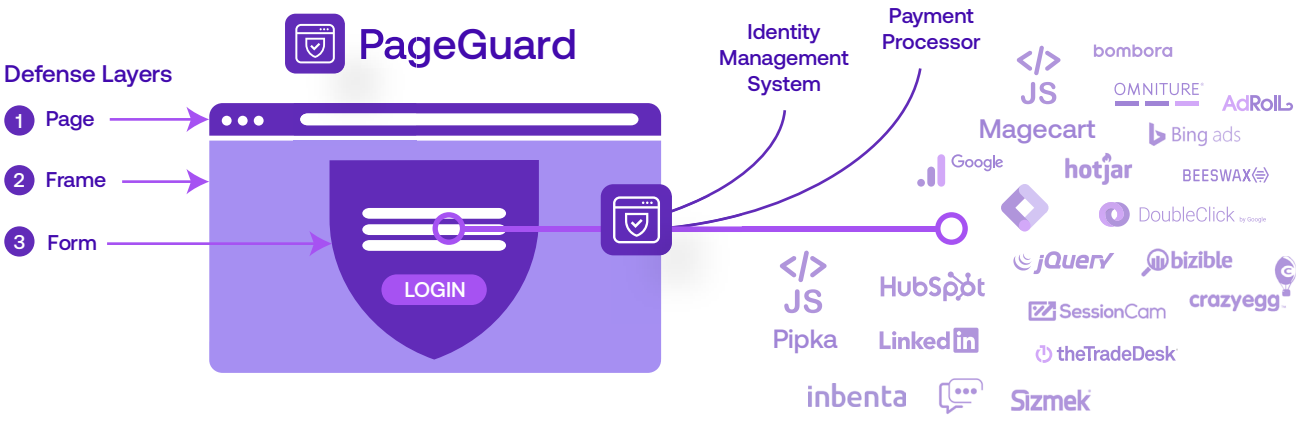
Client-side Security Outcomes

- Thrive with an automatically protected client-side attack surface.
- Gain uncompromised client-side protection with JavaScript security permissions.
- Significantly reduce cyber risk by uncovering abnormal web application behaviors and threats.
- Fully disable e-skimming, cross-site scripting, formjacking, and other client-side attacks.
- Maintain compliance indefinitely by staying ahead of current and future data privacy regulations.

Based on the Zero Trust model, PageGuard runs continuously in the background to automatically detect unauthorized scripts and anomalous code behavior. After detection, PageGuard blocks all unauthorized and unwanted behavior in real-time across an organization's web assets.

PageGuard adds security permissions and controls to JavaScript. Protecting every page of a website or web application, PageGuard automatically applies security configurations and permissions for continuous monitoring of and protection from malicious client-side activities and third-party scripts.

See it in action. Request a demo.



PageGuard is always on, always monitoring, and helps businesses guard their web assets from cyberthreats including:

- Cross-site Scripting (XSS)
- DOM Based (XSS)
- Magecart
- Digital skimming & e-skimming
- Data harvesting & exfiltration
- Formjacking
- Side-loading
- Chain-loading
- Credential stuffing

Deploy PageGuard in three simple steps:

1. Configure initial settings
2. Install PageGuard by adding a few lines of code to your web site or web applications
3. Start monitoring, analyzing, and protecting your web assets

FEROOT.COM

Feroot Security PageGuard Features

Automated Client-side Threat Protection

PageGuard continuously analyzes all scripts from the user perspective to uncover unauthorized activities.

PageGuard allows businesses to:

- Protect their websites and web applications form skimming and Magecart attacks.
- Deploy JavaScript security access controls to eliminate customer data exfiltration risk.
- Observe browser-level code activities to identify and stop malicious activity in real-time.
- Automate client-side web security operations.

Continuous Client-side Security Coverage

PageGuard enables companies to drive continuous client-side security to protect their most valuable asset, their customers.

PageGuard enables businesses to:

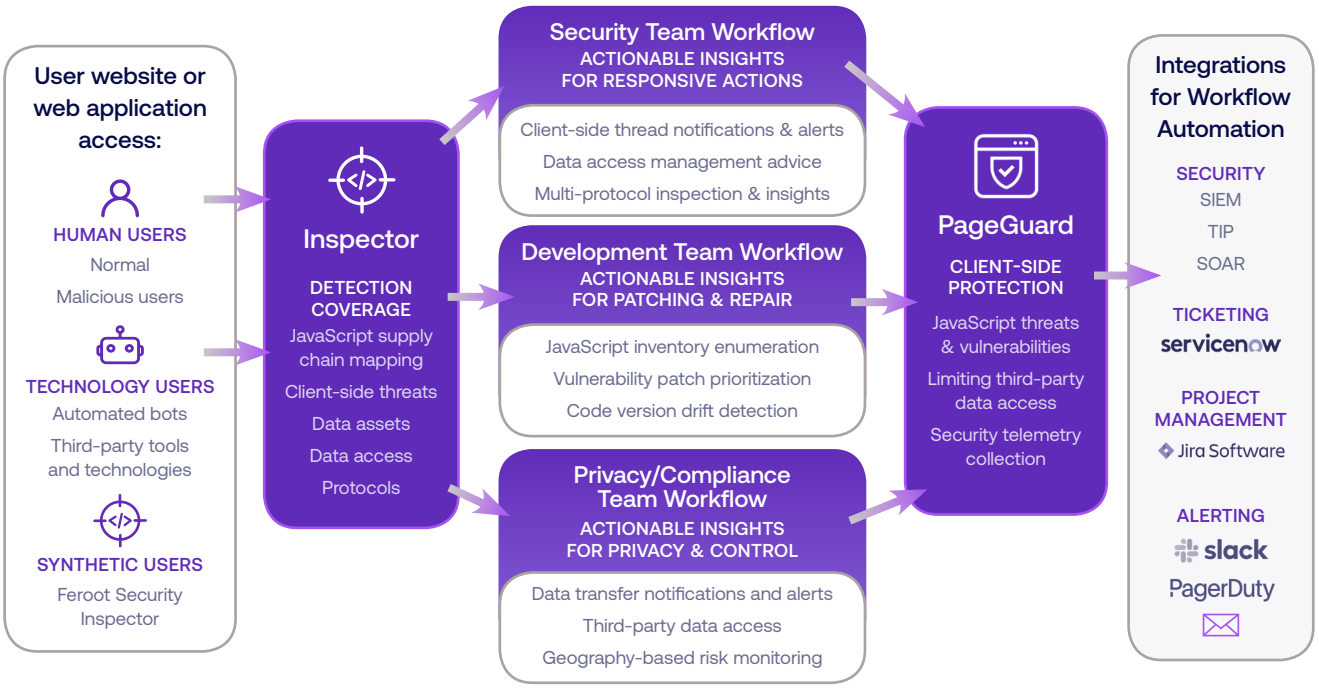
- Build, monitor, and protect their client-side attack surface across all of their user journeys.
- Classify mapped assets based on their function, value, and level of potential vulnerability.
- Automatically monitor, detect, prioritize and act on new scripts, code changes, and changes in code behaviour, to enable client-side web asset protection.

Protection Regardless of Version or Patch Priority

PageGuard protects client-side applications and websites regardless of their version or availability of exploits.

PageGuard automatically blocks:

- Unauthorised scripts
- Unauthorized frames
- Known web vulnerabilities
- Standard input value access
- Non-standard input value access



Integrations

PageGuard allows customers to ingest client-side telemetry and threat intelligence into their security products for intelligence aggregation and collection. Customers enhance their externally sourced and server-side collected cyber threat intelligence (CTI) with client-side collected and aggregated CTI from PageGuard. Current integrations include:

splunk> DATADOG JupiterOne sumo logic Amazon CloudWatch AWS CloudWatch Logs logz.io webhooks

Contact us: sales@feroot.com www.feroot.com

feroot