![feroot]

Feroot Security Product Suite

At Feroot Security we believe customers should be able to do business securely with any company online, without risk or compromise. Using automated scanning and monitoring technology, Feroot secures client-side web applications so businesses can deliver flawless digital user experiences to their customers.

Feroot Inspector continuously scans and reports on JavaScript web application vulnerabilities and attacks.

PageGuard deploys JavaScript security permissions to ensure data exfiltration attacks are a thing of the past.
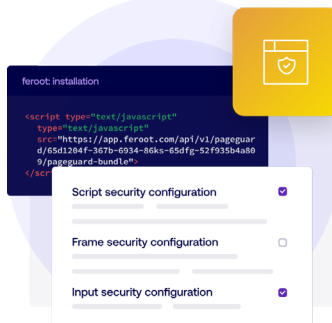
DomainGuard simplifies Content Security Policy management, allowing security and development teams to focus on mission critical tasks.
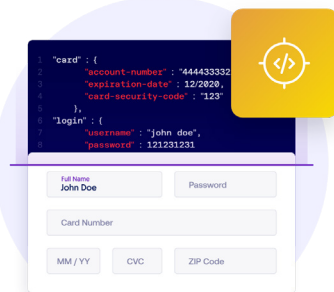
Inspector

Client-side security made easy with automated JavaScript monitoring, detection, and mitigation advice.

PageGuard

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

DomainGuard

Make Content Security Policy work for your business with automated policy generation, management, and violation reporting.

Feroot Security Inspector

Inspector Security Outcomes

- Identify your web asset inventory; reveal and protect your entire client-side attack surface.

- Stay ahead of client-side threats by patching hidden and exploited code vulnerabilities immediately.

- Significantly reduce cyber risk by uncovering abnormal web application behaviors and threats.

- Ensure effectiveness of your client-side security controls, including Web Application Firewalls (WAFs).

- Create, evaluate, and monitor your Content Security Policy.

- Thrive by continuously testing and protecting your web applications, websites, and your entire attack surface.

- Maintain compliance indefinitely by staying ahead of current and future data privacy regulations.

- Discover and utilize mitigation advice to stop e-skimming, cross-site scripting, formjacking, and other client-side attacks.

- Protect your business and your customers by uncovering JavaScript security issues in real-time, all the time.

About Inspector

Using automation, identify all your JavaScript web applications, third-party scripts, digital assets, and their data access. Feroot Security Inspector empowers you to manage your client-side attack surface to secure web applications from Magecart, XSS, and other client-side threats. Inspector finds JavaScript security vulnerabilities, reports on them, and provides specific threat remediation advice to security teams in real time. Inspector simplifies Content Security Policy management, allowing security and development teams to focus on mission critical tasks.
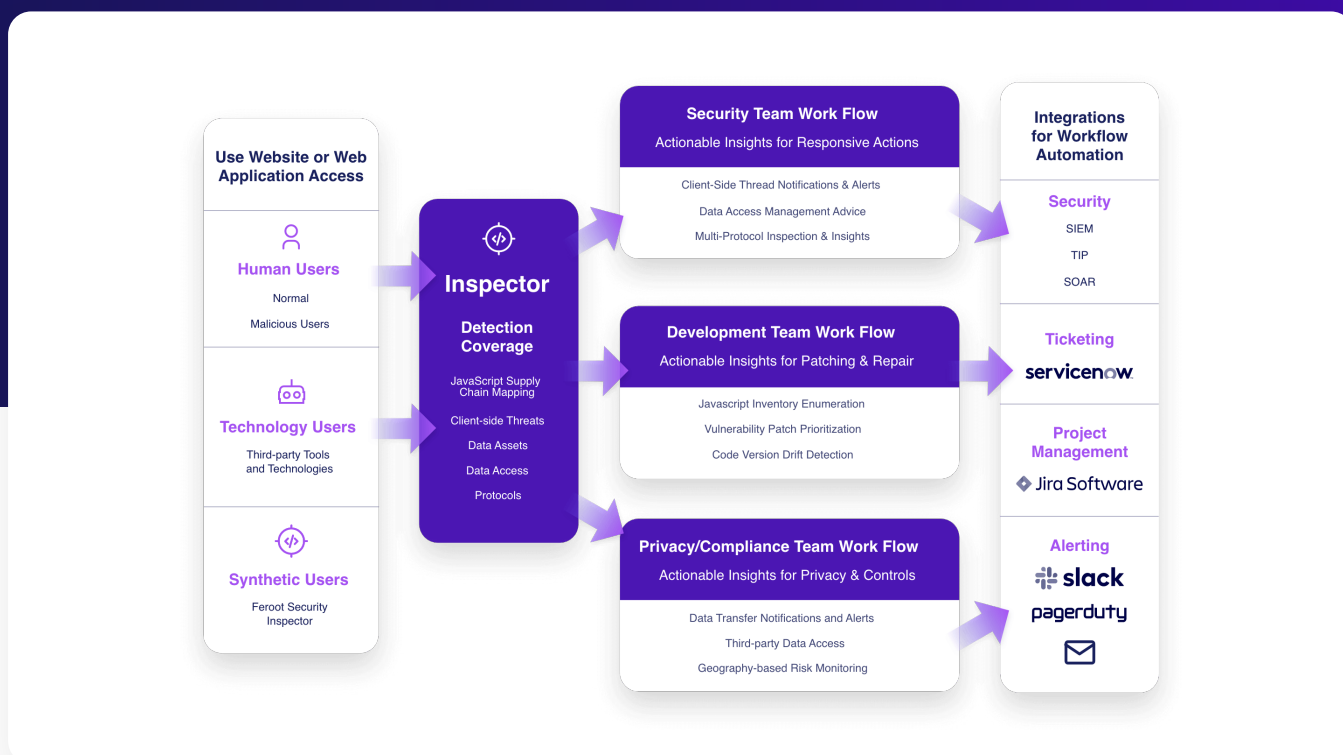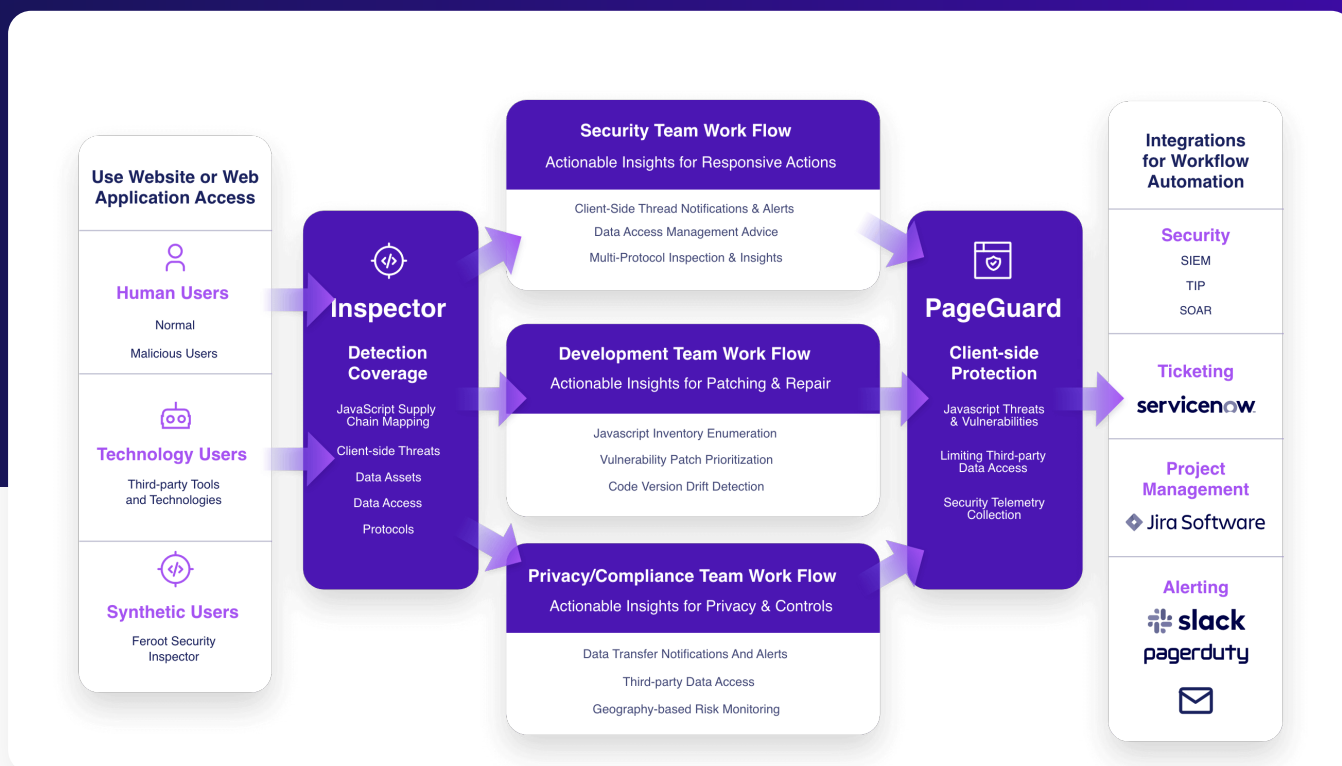

Inspector Integrations

PageGuard

PageGuard Client-side Security Outcomes

- Thrive with an automatically protected client-side attack surface.

- Significantly reduce cyber risk by uncovering abnormal web application behaviors and threats.

- Maintain compliance indefinitely by staying ahead of current and future data privacy regulations.

- Gain uncompromised client-side protection with JavaScript security permissions.

- Fully disable e-skimming, cross-site scripting, formjacking, and other client-side attacks.

About PageGuard

Add security permissions and policies to JavaScript-based applications to stop Magecart, XSS, and other client-side attacks. Feroot Security PageGuard is an automated JavaScript security solution that protects websites and web applications from client-side cyber attacks in real-time. Based on the Zero Trust model, PageGuard runs continuously in the background to automatically detect and block unauthorized scripts, client-side malware, and anomalous code behavior. PageGuard is always on, always monitoring, and always protecting your customers and your data.

Use Website or Web Application Access

Human Users

Normal

Malicious Users

Technology Users

Third-party Tools and Technologies

Synthetic Users

Feroot Security Inspector

Inspector

Detection Coverage

JavaScript Supply Chain Mapping

Client-side Threats

Data Assets

Data Access

Protocols

Security Team Work Flow

Actionable Insights for Responsive Actions

Client-Side Thread Notifications & Alerts

Data Access Management Advice

Multi-Protocol Inspection & Insights

Development Team Work Flow

Actionable Insights for Patching & Repair

Javascript Inventory Enumeration

Vulnerability Patch Prioritization

Code Version Drift Detection

Privacy/Compliance Team Work Flow

Actionable Insights for Privacy & Controls

Data Transfer Notifications And Alerts

Third-party Data Access

Geography-based Risk Monitoring

PageGuard

Client-side Protection

Javascript Threats & Vulnerabilities

Limiting Third-party Data Access

Security Telemetry Collection

Integrations for Workflow Automation

Security

SIEM

TIP

SOAR

Ticketing

servicenow

Project Management

Jira Software

Alerting

slack

pagerduty

Inspector Integrations

splunk>

DATADOG

JupiterOne

sumo logic

Amazon CouldWatch

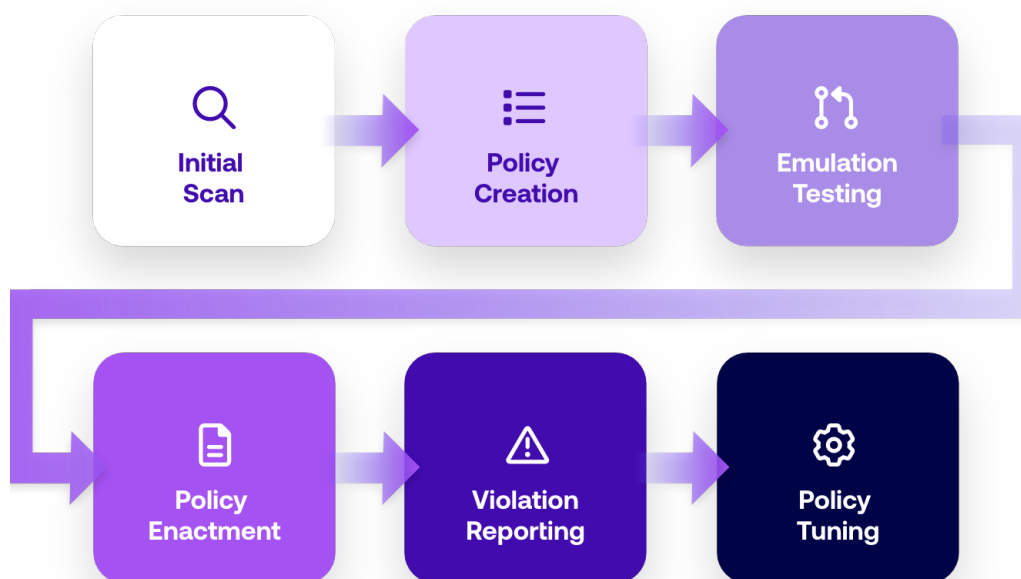Amazon CouldWatch Logs

logz.io

webhooks

DomainGuard

DomainGuard Client-side Security Outcomes

- Tailored and automated Content Security Policy creation based on customer specific web application scans and data collection.

- Content Security Policy version tracking, control, and automated enhancement to reduce cyber risk and quickly mitigate Content Security Policy violations.

- Significantly reduce Content Security Policy resource allocation and keep clean audits.

- Content Security Policy violation reporting integrated with security tools to complement current security processes and workflows.

- Granular Content Security Policy control to ensure proper balance between restrictive vs. lax policies.

- Meet regulatory and compliance standards such as PCI, HIPAA, and others.

About DomainGuard

DomainGuard is a purpose-built security solution for businesses who would like to control their client-side attack surface and reduce their client-side cyber threat exposure, by deploying and managing Content Security Policies on their web applications.

Using automation, DomainGuard identifies all your first- and third-party scripts, your digital assets, and the data they can access. DomainGuard then generates appropriate Content Security Policies based on scanned data and anticipated effectiveness. Customers deploy tailored Content Security Policies at the domain level for easy monitoring, management, version control, and continuous enhancement.

Initial Scan → Policy Creation → Emulation Testing → Policy Enactment → Violation Reporting → Policy Tuning

We are

Feroot Security

Businesses come to Feroot to enable proactive client-side security programs. Our data protection capabilities take the pain and ambiguity out of client-side security threat analysis, detection, response, and prevention.

Our products help organizations uncover supply chain risks and protect their client-side attack surface.

Chainloaded script

37% of users loaded

Pages:
Customer Chat
Contact
Submit Payment
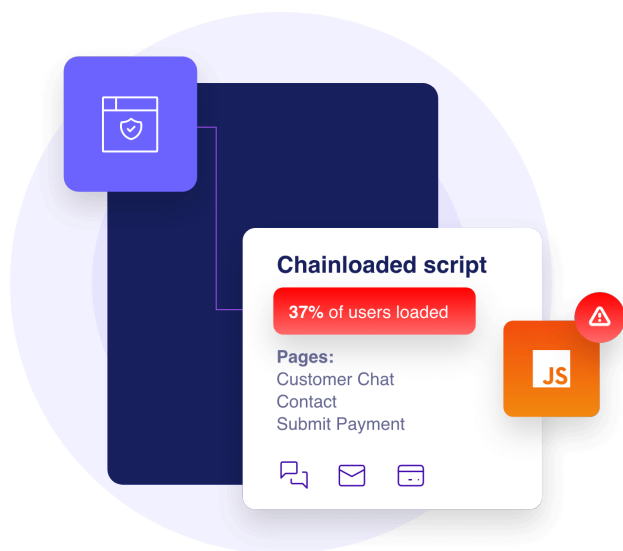
Ready to Protect Your Client Side?

Get a free web application scan and advice on how you can boost the security posture across your web assets. **As part of your assessment, one of our security experts will:**

- Conduct a real-time scan of your web application.
- Evaluate your current structure.
- Identify potential vulnerabilities.
- Offer a set of best practices to get you started with client-side security.

Send us an email at sales@feroot.com

About Feroot

Feroot Security believes that customers should be able to do business securely with any company online, without risk or compromise. Feroot secures client-side web applications so businesses can deliver flawless digital user experiences to their customers. Visit www.feroot.com.

feroot