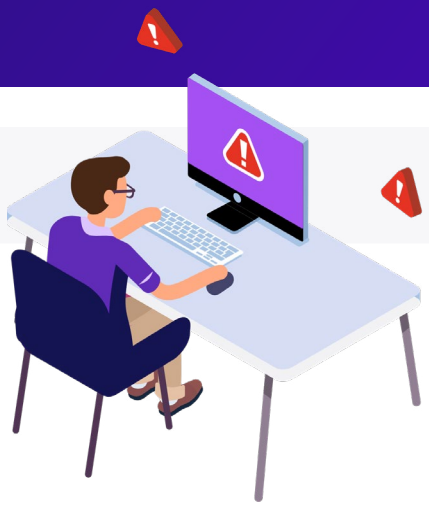
feroot

Data Sheet

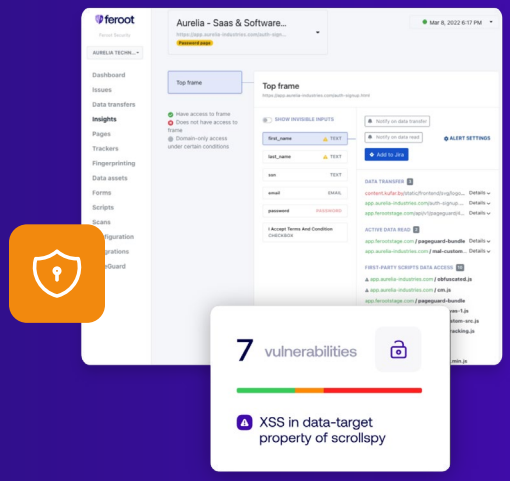
Client-Side Security Technologies

Find out the limitations in older existing client-side technologies and how the latest client-side solutions can protect from attack and data exfiltration through automation and advanced synthetic user technologies.



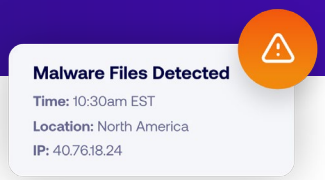
Client-Side Security Technologies	Limitations
Web Application Firewall (WAF)	Can't protect businesses from: • Sophisticated skimming malware. • Drive-by skimming. • Supply chain attacks. • Sideloading attacks. • Chainloading attacks.
Content Security Policy (CSP)	If used as a sole security control, may expose businesses to e-skimming breaches due to: • Misconfigurations and excessive "allow list" rules. • Bypass techniques. • Incorrect implementation or tradeoffs. • Difficulty developing and deploying a comprehensive policy.
Penetration Testing and Vulnerability and Security Assessments	Even if conducted on a regular basis, pentesting and vulnerability and security assessments: • Are time and resource intensive. • Are expensive. • Reflect conditions based on a single point in time. • Are limited in scope to certain applications, technologies, and networks. • Require skilled and experienced personnel to conduct the tests or assessments. • Rely on specialized tools and technologies.
Vulnerability Scanners	Because vulnerability scanners are not designed to support the client side, they: • Scan only server-side (back-end) assets, not web applications and websites. • Aren't able to detect and enumerate JavaScript code and vulnerabilities. • Can only view a single domain, not all of the links that are part of it.
Code Scramblers and Obfuscators	Code scramblers and obfuscators come with some significant issues, such as: • Scrambled code cannot be easily unscrambled. • It is much more difficult to find vulnerabilities and problems in obfuscated code. • If the obfuscated script includes third-party code, it becomes difficult to identify malicious or corrupted third-party content.

Advanced Client-Side Security Technologies



Client-Side Attack Surface Monitoring

- Newer, advanced threat detection technology.
- Identifies and classifies data and threat intelligence to detect and report on client-side security vulnerabilities and attacks.
- Automatically discovers all web assets and reports on their data access.
- Uses headless browsers to navigate through all JavaScript contained on the website and web application pages.
- Gathers real-time information about how the scanned website works from the end-user perspective.
- Deploys synthetic users during threat detection scans to act and interact as a real human would.
- Logs and monitors each web application interaction.
- Uses behavioral analyses and injects logic into each page to gather information that is difficult to collect manually.



JavaScript Security Permissions

- Automatically applies security configurations and permissions for continuous protection from malicious client-side activities and third-party scripts.
- Blocks all unauthorized and unwanted behavior in real-time across an organization's web assets.
- Prevents data exfiltration.
- Integrates directly into the runtime environment of every user browser session to enable proactive monitoring and defense.
- Deploys the Zero Trust model on JavaScript applications.
- Runs continuously in the background to automatically detect unauthorized scripts and anomalous code behavior.
- Monitors and responds to browser-level security events in real-time by auto-instrumenting on every website and applying security configurations to every user browser session.

feroot

About Feroot

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

Contact Us

sales@feroot.com | www.feroot.com