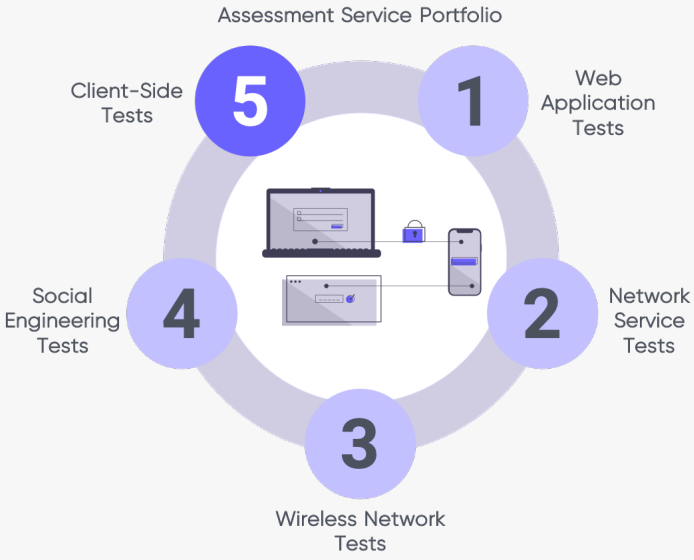
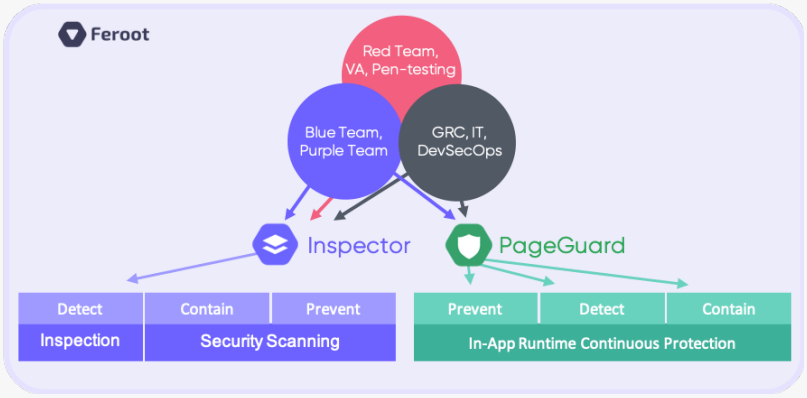
Feroot Adds DevSecOps Capabilities To Protect Web Application's Front End Against Malicious JavaScript Attacks

New Enhancements Include Powerful In-app Client-Side Self-Protection and Real-time Security Monitoring Dramatically Boosting Defenders' Resilience

TORONTO, CANADA, June 1, 2020 /EINPresswire.com/ -- Feroot Security, the developer of the platform for securing digital user experience of web applications and websites, today announced major enhancements focused on maximizing efficiency and effectiveness in protecting every digital customer touchpoint against Magecart and equivalently malicious JavaScript elements.



Client-side assessment automation

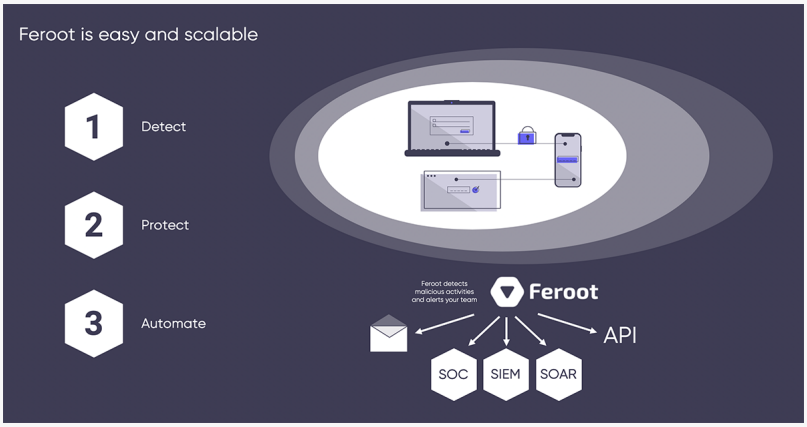


People, Processes and Functions

With these new In-App client-side runtime self-protection (RASP), anti-tampering hardening and real-time behavior detection capabilities, the Feroot Platform enables organizations to continuously safeguard user journey and monitor every point where their web applications and websites are ingesting business and customer information, including payment credit card details, financial transactions, identity details, and passwords.

The new release is designed to provide businesses with the freedom to innovate and securely operationalize the best of breed technologies of today to grow revenues, differentiate their offerings, and reduce costs with confidence.

“Organizations delivering digital financial services, banking, online retail, SaaS platforms, and many other sectors are moving the web application code to the front end. As companies are increasingly embedding the best of breed technologies, third-party vendors, and widgets into the digital user journeys of web applications and websites, the adversaries are now looking for weaknesses and the backdoors in the front end,” said Ivan Tsarynny, Feroot CEO and co-founder.



Easy and scalable

Enhancing the Security of Digital Customer Experience
Utilizing the Feroot platform, organizations are equipped to deliver enterprise-grade security defenses that are easy to activate and manage. Continuous and autonomous protection gives organizations the immunity against a wide range of adversaries, cyberattacks, and threats – from Magecart and PII harvesting to digital supply chain attacks.

> As companies are embedding third-party tools and widgets into the digital user journeys of web applications, Feroot empowers DevSecOps professional to shield data assets with zero-trust approach.”
> *Ivan Tsarynny, Feroot CEO and Co-Founder.*

Every user session is secured without the need for episodic manual penetration tests of the client-side with the error-prone and inconsistent results. Optional access control policies let security enforce zero-trust and least-privilege security model.

New capabilities of the platform empower DevSecOps professionals to perform intelligent real-time monitoring of code behavior of every user session’s digital touchpoint, enriching it with security, governance, and privacy compliance metrics.

• Attack Surface Monitoring: enhancements to PageGuard provides a complete view of the entire attack surface including all web assets and all dynamically generated forms and pages.
• Intrusion Attempts Alerts: real-time detection of browser-level PII harvesting and skimming attacks attempts.
• Asset Monitoring: Automatically determine which third-party or code element has access to assets and monitor for new assets, and changes in JavaScript code.
• Behavior Analysis: Identifies and prevents signature-less never-before-seen threats, including Magecart attacks, ensuring business and brand safety.

The Feroot platform gives peace of mind and helps organizations focus on performance, maximizing results, and customer-focused innovation.

For more information on the Feroot Platform, please visit www.feroot.com.

ABOUT FEROOT
Feroot is dedicated to protecting organizations and their customers by securing the digital customer experiences of web applications and websites. Feroot's platform is the Immune System For Web Applications and Websites against today's and tomorrow's threats. Feroot combines behavior-based intrusion detection with proactive defenses against digital web skimming and other emerging client-side risks. It provides actionable insights, enables collaborations between security, privacy, marketing, and other departments to help organizations protect business continuity, performance, and brand safety.

Ivan Tsarynny
Feroot Privacy
+1 4086926429
email us here