

Feroot Adds PageGuard - Digital Skimming Protection To Its Cyber-defense Platform.

The company's latest, cutting-edge technology is purpose-built to provide comprehensive control for customers over their data security on the web.

TORONTO, ONTARIO, CANADA, December 5, 2019 /EINPresswire.com/ -- [Feroot](#), today added [PageGuard](#), a data protection technology (DPT) for web pages with checkout functionalities that are processing payment card information and other sensitive data.

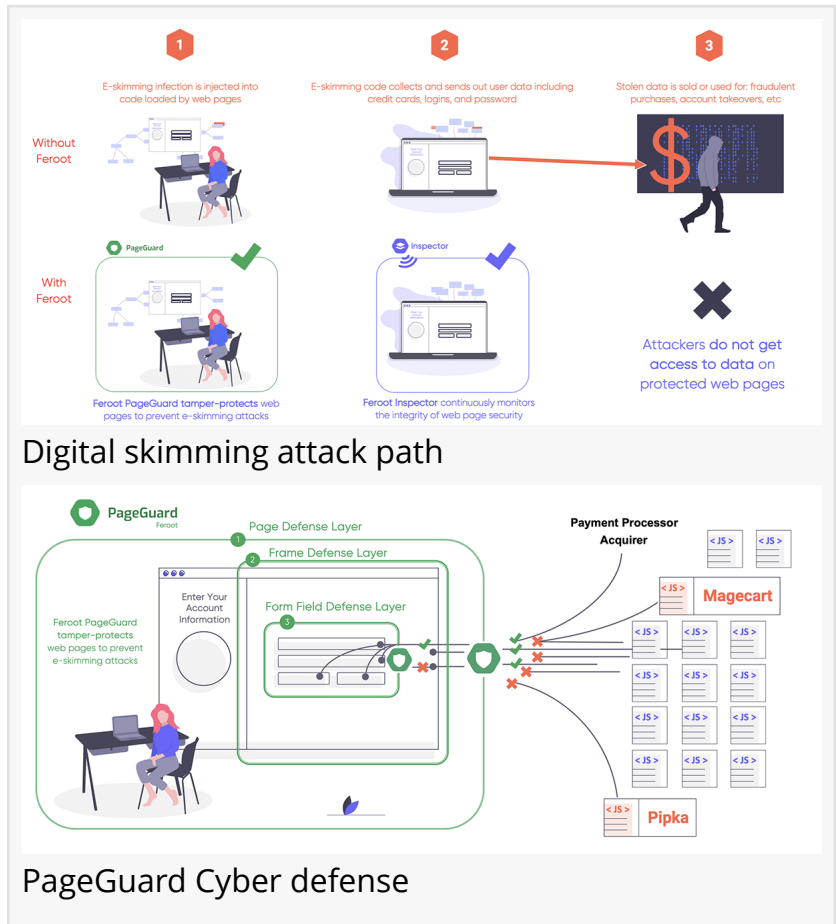
The release extends Feroot's footprint in protecting web applications and web pages that are processing sensitive data during financial transactions and user authentication against Magecart-style digital skimming attacks.

The company's latest innovation in the cybersecurity provides granular data access controls for web pages processing payment card information, PII, PHI, and other types of sensitive data, making it significantly easier to centrally control access permissions, resolve security configuration gaps, remediate vulnerabilities in real-time, confidently respond to incidents and demonstrate compliance with regulations, standards, and policies.

“

The security operations function is quickly moving into protecting data at the browser level. PageGuard protects customer data processed by web applications and web pages.”

Vitaliy Lim, CTO at Feroot



hundreds of thousands of organizations with the ability to protect and detect possible digital skimming breaches, also known as e-skimming breaches that do not have existing infection

signatures or definitions.

PageGuard is created to excel in SaaS environments and has no noticeable performance impact. Security analysts, web development, and system administrators can verify the integrity of the security posture, harden web pages, and be alerted of attacks and potentially malicious activities.

“Feroot PageGuard helps security teams protect key web assets at the browser level making the customer experience more secure and resilient against attacks,” said Lim. “Presently, when development and security teams need to protect against supply-chain attacks, they are forced into implementing Content Security Policy (CSP) or custom workarounds involving separate sandboxed iframes which may lead to reengineering the structure of the web pages or rely on web application firewalls leaving data exposed to browser-level skimming breaches. All too often, companies are left exposed to skimming breaches. PageGuard consolidates defense capabilities onto an easy-to-deploy tool that gives protection across all of the organization’s web assets.”

About Feroot

Feroot is dedicated to keeping the web safe from cyberattacks. Feroot cyber-defense platform combines behavior-based intrusion detection with data access controls to prevent digital skimming threats, provides actionable insights, and enables organizations to simplify web security operations. Feroot analyzes activities of a countless number of JavaScript security events daily, enabling real-time detections of Magecart-skimming attacks and other threats to help organizations’ ensure the safety of their data on the web.

Ivan Tsarynny
Feroot
+1 408-692-6429
[email us here](#)

Together at Last

Introducing Feroot PageGuard and Inspector to defend your business from Magecart-style web skimming attacks

Feroot extends your web security operations to the client-side. PageGuard security engine uses browser-level sandbox isolation technology to control access of third-party JavaScript code to sensitive data. It gives you granular control over which third-party scripts are allowed to be loaded on each web page, blocks unwanted side-loaded scripts, and protects sensitive form fields from unauthorized data access.

EASY IMPLEMENTATION

Activate PageGuard Now

Feroot PageGuard and Inspector defend your business from Magecart-style digital e-skimming attacks

This press release can be viewed online at: <http://www.einpresswire.com>

Disclaimer: If you have any questions regarding information in this press release please contact the company listed in the press release. Please do not contact EIN Presswire. We will be unable to assist you with your inquiry. EIN Presswire disclaims any content contained in these releases. © 1995-2019 IPD Group, Inc. All Right Reserved.