FireCompass Launches AI Agents for Autonomous Web and API Penetration Testing With Freemium Access

Start in minutes and validate exploitable paths across web apps, APIs, and external infrastructure.

BOSTON, MA, UNITED STATES, February 5, 2026 /EINPresswire.com/ -- FireCompass today announced the launch of Explorer, a credit-based freemium model designed to make proof-based web and API penetration testing easy to start, evaluate, and expand. The new "FireCompass Explorer" experience gives security teams immediate, self-serve access to FireCompass's AI-powered Autonomous Pen Testing (Infrastructure + Web App + API), so they can validate real attack paths with evidence, not just alerts.

Attackers move faster than periodic security testing cycles. Traditional approaches often cover a limited portion of assets and struggle to confirm exploitability, driving noise, delays, and missed attack paths. FireCompass was built to close that gap with continuous discovery, multi-stage attack simulation, and validation that prioritizes what is actually exploitable.

"Teams shouldn't need weeks of calls and procurement cycles to conduct a penetration test," said Bikash Barai, Founder and CEO of FireCompass. "With credit-based freemium access, security teams can start in minutes, run real penetration tests safely, and review evidence-backed results."

What's Included in "Start Free"
-Explorer (Free • Self-serve).
-Includes $2,000 in one-time credits.
-Designed for fast time-to-value: onboard targets, run tests, and review findings in the portal.
You can access it here: https://firecompass.com/start-trial/

For enterprise teams that want structured outcomes, guided onboarding, and a time-bound evaluation, FireCompass also offers a white-glove pilot with $5,000 to $10,000 in one-time credits.

What Teams Can Validate With Free Credits
With the new freemium access, teams can evaluate FireCompass across core workflows, including:
-Autonomous Web and API penetration testing, including both authenticated and

unauthenticated testing.
-Continuous Automated Red Teaming (CART) using automated multi-stage attack trees and playbooks (available in enterprise pilots).
-Attack Surface Discovery to align testing coverage with real-world exposure and discover shadow assets.

Why This Matters
FireCompass is designed to reduce noise and prioritize action by validating exploitability and mapping attack paths, including multi-stage attack chains. This approach assures near-zero false positives, attack-path-based prioritization, and stronger ROI compared to traditional security testing.

Availability
Credit-based freemium access is available starting today. Explorer is self-serve. Optional enterprise onboarding capacity is limited and scheduled.
Access is provided to verified enterprise users to ensure safe, authorized use.

About FireCompass
FireCompass is an agentic AI platform for automated penetration testing, red teaming, and attack surface management. It covers the full stack across web apps, APIs, cloud, and infrastructure. It discovers shadow assets and validates risk through safe exploitation and multi-stage attack path analysis across external and internal environments. FireCompass delivers evidence-backed results with near-zero false positives, prioritizing what is actually exploitable. It can run fully autonomously or with expert-in-the-loop validation. FireCompass is trusted by Fortune 500 enterprises and recognized by Gartner, GigaOm, and IDC.

Priyanka Aash
FireCompass Technologies Inc
+1 650-248-4625
priyanka.aash@firecompass.com
