AppSentinels Helped a US Online Marketplace Find the Blind SSRF Its AI Red-Teamer Could Not Reach

How a US online marketplace's existing security tools tested a workflow for weeks and still missed the blind SSRF sitting several steps inside it until a two-week AppSentinels proof of concept found it.

EXECUTIVE SUMMARY

An online marketplace based in the U.S. already ran a dedicated API discovery and AI-based red-teaming product, plus a separate bot and runtime defense tool, and still could not be sure nothing was getting through. Their AI red-teamer tested endpoints one at a time. It had no way to string calls together into the multi-step sequences an attacker would actually use, and that was exactly where their exposure lived.

In a two-week proof of concept, AppSentinels found out what the incumbent stack had missed: a confirmed blind SSRF, several broken object-level authorization flaws, an unauthenticated endpoint leaking profile data, a NoSQL injection, and a reflected XSS. The engagement closed on schedule and moved into commercial discussion.

The Challenge: A blind SSRF that lived several steps into a workflow

The vulnerable parameter was a nested image URL on a product-comparables endpoint, reachable only after a specific sequence of prior calls. Hitting the endpoint directly did not expose it. It returned nothing to an attacker either: no error, no content, no timing signal. That combination is exactly why it had survived.

01 Blind SSRF
Reachable only through a nested parameter, several steps into a multi-step workflow.

02 Broken object level authorization (BOLA)
Multiple cases where one user's identifier could be substituted to reach another user's object, found only by chaining calls.

03 Broken authentication
An API reachable with a partner key but no user token, returning profile information including personal data.

04 NoSQL injection
Malformed input reaching the data layer and returning database errors that expose what to try next.

05 Reflected XSS
Confirmed in testing and blocked at runtime within the same engagement.

> **"We already had API testing running. What we did not have was anything that could string calls together the way an attacker would, and that turned out to be exactly where the finding was."**
>
> — Application Security Leader, US online marketplace

The Solution

API Discovery

2,400 APIs discovered in under 24 hours, including 60 with no authentication and 1,100 carrying sensitive data, against an inventory the team believed was already complete.

Automated Workflow-Aware Testing

2,577 tests built automatically from observed traffic, no scripts written, re-run as the APIs changed, checking whether valid calls chained together into something the application never intended.

End-to-End Exploit Validation

Chained the calls to reach the vulnerable state, planted a callback in the nested parameter, and confirmed the hit via out-of-band DNS. Reproduced on demand at the customer's request.

45 min	2,577	2 weeks
from deployment to live traffic	tests auto-generated, no scripts written	for the entire proof of concept

Business Outcomes

- **Reproducible Blind SSRF**
  Found the flaw the incumbent AI red-teamer had missed, proven by out-of-band callback and reproducible on demand.
- **Risk-Ranked API Inventory**
  Surfaced 60 unauthenticated APIs and 1,100 carrying sensitive data against an inventory the team believed was already complete.
- **Reduced Manual Testing Effort**
  Generated and re-ran thousands of tests automatically as the API surface changed, with no scripts written.
- **Broader Risk Detection**
  Surfaced BOLA, broken authentication, NoSQL injection, and reflected XSS inside an environment already covered by dedicated API security tooling.
- **Faster Pilot-to-Purchase Path**
  Closed the two-week proof of concept and moved directly into commercial discussion.

About AppSentinels

AppSentinels is the Business Logic Security platform for modern applications. Built around the Business Logic Graph, it delivers continuous discovery, automated stateful red-teaming, and runtime protection across AI agents, MCP servers, APIs, and the workflows that connect them. First-generation API security tools inventoried endpoints; AppSentinels secures the logic behind them, the layer where breaches happen.