STACKHAWK

Customer Success Story

Pharmacy Benefits Optimizer Expands Security Coverage While Increasing Development Velocity

- Enhanced Visibility
- 3x More Scans, Zero Slowdown
- Continuous, Automated Testing

Use Case
Modernize and Scale Security Testing

Industry
HealthTech

Employees
+800

Developers
50

Location
USA

When outdated security tools slowed development, this leading pharmacy benefits optimizer turned to StackHawk. With automated, developer-friendly testing embedded in their workflows, the company increased scan volume 3x, expanded coverage, and accelerated secure releases across its growing platform.

A leading pharmacy benefits optimizer experienced several security challenges before implementing StackHawk. Their application security (AppSec) team was struggling to keep up with how fast development was moving, leading to gaps in vulnerability detection and remediation. Their previous legacy security tool presented roadblocks—slow scan times, difficulty integrating into developer workflows, and a lack of developer-friendly remediation tools all hindered productivity. Operating and competing in the healthcare industry means the company must deliver value fast while also keeping sensitive customer data (PHI) safe, making the need for a better solution urgent.

> I don't have to analyze the scans except for false positives, so I can work with the devs to get those fixed. Other than that, it's in the devs' court.
>
> **Cloud Engineer**

The Problem

Challenges with slow legacy tools that couldn't keep up with development. The lack of seamless integration and developer-friendly remediation hindered vulnerability detection and remediation, making security a bottleneck.

The Solution

Adopting a shift-left approach with StackHawk's automated, developer-friendly solution and integrating it within existing workflows to enable proactive security testing.

The Result

Security scans increased from 50-60 to nearly 200 per week, while security testing expanded from a few applications to over 40. Developers took ownership of security, reducing bottlenecks and accelerating software release cycles without compromising security.