STACKHAWK

Customer Data Platform Achieves 95% API Coverage

BACKGROUND

This customer is a leading customer data platform (CDP) that helps global enterprises unlock the full value of their data. They enable businesses to unify and activate customer insights at scale, meaning they operate in a high-stakes environment with complex systems and sensitive information flowing through a massive web of APIs.

Before integrating StackHawk into their ecosystem, the security team was struggling with some familiar yet frustrating challenges. Rapid API development was moving faster than their ability to test thoroughly, and false positives were drowning both security and engineering teams. They lacked clear visibility into their attack surface, and the vulnerability management process had become time-consuming and prone to errors.

In short, they needed a better way to test APIs, reduce noise, and stay ahead of vulnerabilities without playing constant catch-up.

> *With StackHawk, security doesn't slow us down—it helps us move faster with confidence.*
>
> - Staff Security Engineer

Information Technology

Use Case
Automating and Scaling API Security

Industry
Information Technology

Employees
+550

Location
USA

THE PROBLEM

The team struggled with limited visibility into their expanding API attack surface, high false positives, and a manual, inefficient vulnerability management process that couldn't keep up with development.

THE SOLUTION

They adopted StackHawk for its seamless integrations, automated API discovery, AI-driven testing accuracy, and organization-wide policy management—enabling scalable, developer-friendly security testing.

THE RESULT

They now have 95% of APIs under test, reduced false positives, and streamlined security workflows across 15 applications—transforming security from a bottleneck into a competitive advantage.

CHOOSING A SOLUTION

They weren't just looking for another tool, they needed a trusted security partner that could meet their technical complexity and velocity head-on.

Integration was a big deal. StackHawk easily connected with their existing toolchain, making it simple to map applications to code repositories and send scan results to existing developer workflows. It felt less like bolting on another layer and more like extending what they already had.

Even better, StackHawk delivered features that actually moved the needle: automated API discovery, customization options for fewer false positives, and flexible policy management that worked at an organizational level. Bonus points for the Backstage plugin, which brings security directly into the developer portal.

It wasn't just about ticking boxes. StackHawk proved it could scale with them, support their DevSecOps goals, and bring order to a chaotic security landscape.

EXPERIENCE WITH STACKHAWK

Since adopting StackHawk, the company has transitioned from a reactive to a proactive approach to application security.

They've successfully scaled their security testing across 15+ applications without adding unnecessary overhead. Today, 95% of their APIs are under active testing with StackHawk, offering a level of visibility and control that was previously out of reach. They know what's in their attack surface, what's vulnerable, and where to focus—no more security blind spots.

The team has also seen a noticeable drop in false positives, which means developers are spending less time chasing ghosts and more time building. StackHawk's automation and policy tools have turned once-manual processes into efficient, repeatable workflows.

> *The ability to bring visibility to all the APIs in our systems so we can make informed decisions on what to test and how frequently has been extremely valuable.*

- Staff Security Engineer

STACKHAWK

Learn how to Ship Secure Software Faster at **www.stackhawk.com**