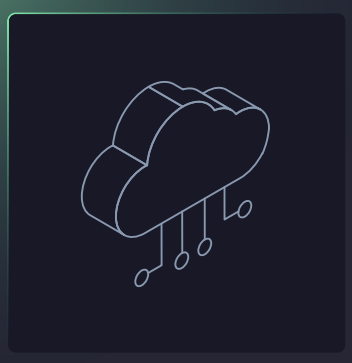
STACKHAWK

Customer Success Story

Cybersecurity Leader Moves from 4-Hour Scans to Fast, Confident Releases

- Scans Cut from Hours to Minutes
- Seamless On-Prem GitLab Integration
- Real-Time Vulnerability Visibility



Use Case
Accelerating Secure Development Cycles

Industry
Information Technology

Employees
+790

Location
USA

A leader in digital identity and anti-fraud solutions, delivering secure, seamless customer experiences through innovative technology, struggled to maintain their application security posture as their product suite continued to expand.

They were faced with slow and cumbersome security scans by legacy solutions that took between 1.5 to 4 hours, significantly delaying development cycles. Configuring scans, especially for SOAP APIs, was complicated, slowing down teams and leaving security gaps. The company also found itself limited by a lack of visibility into their security posture, with no clear insights into application vulnerabilities or coverage. On top of that, integrating security scans within their existing on-premises GitLab installation required frequent manual adjustments, consuming valuable development resources.

When legacy security tools slowed development with multi-hour scans and limited visibility, this digital identity and anti-fraud leader turned to StackHawk. With fast, developer-friendly DAST integrated into their on-prem GitLab pipelines, the company reduced scan times from hours to minutes, streamlined SOAP API testing, and gained real-time insight into their application security posture.

The Problem

The company struggled with slow, 1.5 to 4-hour security scans, complex SOAP configurations, and limited visibility into vulnerabilities, causing delays and draining developer resources.

The Solution

They adopted StackHawk for its fast, developer-first DAST capabilities, clear feedback on configurations, and seamless integration with on-prem GitLab, including support for SOAP APIs and custom environments.

The Result

StackHawk dramatically cut scan times, enabled proactive vulnerability management, and empowered both security and development teams with automated CI/CD workflows and increased visibility into their security posture.