



AWESOME CUSTOMER SUCCESS STORY

LATAM Financial Giant Secures Modern Microservices with StackHawk

BACKGROUND

A leading financial institution in Latin America was up against a new regulatory mandate across the LATAM region, emphasizing the critical need for DAST. Their previous reliance on infrequent, external penetration testing proved to be inadequate. The process was too slow to keep pace with development cycles, lacked the depth to uncover vulnerabilities in their complex microservices architecture, and provided security feedback to their developers too late in the development process. The company needed a solution that could provide comprehensive, continuous security testing that could scale.

Financial Services

Use Case

Securing Modern Microservices

Industry

Financial Services

Employees

+100,000

Location

LATAM



We went from slow, manual pen testing to automated, near-instant feedback in our pipeline, truly shifting left and securing our modern infrastructure at scale. StackHawk didn't just sell us a tool, they became our security partners, helping us understand our attack surface better than ever before.

- DevOps Engineer



THE PROBLEM

The financial institution's outdated security testing was too slow and inadequate for their complex microservices, failing to protect from breaches and meet new regulatory mandates.



THE SOLUTION

They implemented StackHawk's automated DAST platform, integrating it into their Azure pipelines for continuous, comprehensive security testing.



THE RESULT

StackHawk drastically reduced scan times, provided near-instant feedback to developers, and enhanced the security team's understanding of their application infrastructure.

CHOOSING A SOLUTION

Automated DAST at Scale

The company required a solution that could be integrated into its Azure pipelines and existing developer workflows. Its goal was to automate DAST testing in its pipelines, stop code progression when vulnerabilities were found, and help developers resolve bugs with as little disruption to their workflow as possible. This was a tall order, but StackHawk was the clear choice for the job after evaluating a handful of legacy tools.

Comprehensive Microservices Testing

The company's supermodern microservices infrastructure demands a DAST solution capable of thoroughly testing individual services and their interactions.

StackHawk's modern platform was built to automate security testing across all API types and services proactively. It enables the company to uncover unexpected data interactions and potential vulnerabilities with specific key input values for API requests, identify vulnerabilities unique to their application's architecture and business logic, and remediate any issues uncovered before bad actors can exploit them.

Responsive and Reliable Support

The company was particularly impressed with StackHawk's commitment to providing exceptional customer support. They found great value in weekly calls and having direct access to a dedicated success representative and Solutions Architect from StackHawk. The StackHawk team went above and beyond by providing a translator on every call and ensuring all onboarding documentation was translated into Spanish. Even emails were thoughtfully translated, making communication effective and demonstrating a genuine dedication to being a partner in the company's success. After experiencing a lack of responsiveness from a previous security vendor when they needed help the most, this level of personalized support was a key factor in the customer's decision to choose StackHawk.

EXPERIENCE WITH STACKHAWK

Lightning-Fast Scan Times

The company's average scan time has been reduced to less than one minute, enabling continuous testing (up to 12 scans per day!) and providing developers with security feedback almost immediately.

Tighter Feedback Loops

The near-instantaneous feedback provided by StackHawk empowers the developers to address security vulnerabilities early in the development lifecycle, reducing the cost and effort of remediation and enhancing overall security posture.

Enhanced Application Infrastructure Knowledge

By implementing StackHawk, the company's security team gained a deeper understanding of its application and API infrastructure. They now have a clear picture of which applications to prioritize for testing and can maintain a comprehensive view of their overall attack surface and coverage.



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