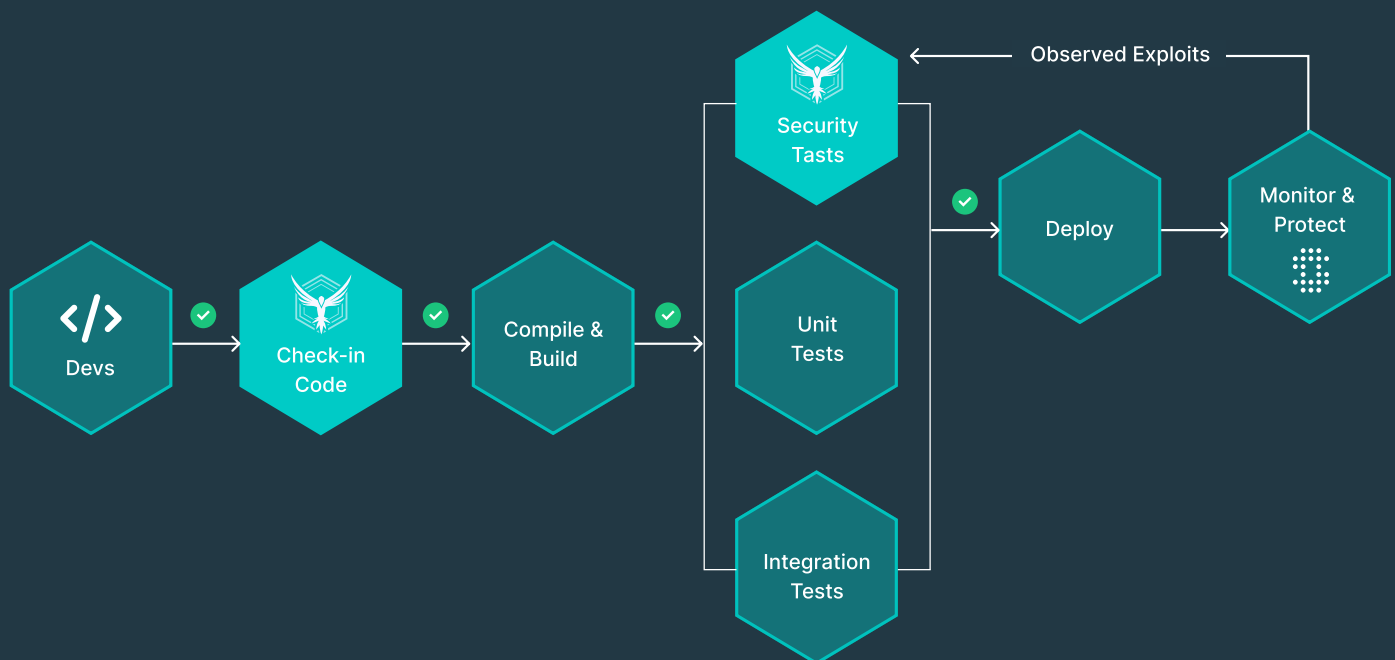










## Partnering to deliver best-of-breed API security with the most trusted solutions in the market.

StackHawk's developer-focused approach to automating API security testing and Salt's deep API adaptive intelligence gives organizations the option to deploy best of breed technologies to monitor, find, and fix security vulnerabilities as they look to improve their security posture. Together, StackHawk and Salt offer the most comprehensive approach to API Security.



## Benefits of StackHawk and Salt together:

- 
**Automate API Security Testing** - Find and fix security vulnerabilities faster across your CI/CD systems with flexible testing architectures (run locally or on any CI/CD system)
- 
**Optimize for Developers** - Integrate with common developer workflows to enable faster fixes, scalability and adoption while reducing friction to deploy secure code
- 
**Modern API Coverage** - Test your APIs prior to deployment to ensure secure builds with complete coverage for gRPC, GraphQL, SOAP and REST
- 
**Understand your API Attack Surface** - Gain clarity into your API attack surface utilizing StackHawk security tests on APIs surfaced by Salt
- 
**Act 'As If'** - Mimic realistic attack scenarios by leveraging data from your production traffic to enhance the accuracy and authenticity of your security tests
- 
**Break down silos between Security and Development** - Feed real time threat intelligence into product tests to ensure software resiliency in an evolving threat landscape

## Why StackHawk for API and Application Security Testing

StackHawk was built to bridge the trust gap between AppSec and Developers to deliver more secure software faster. The company's deliberate approach to developer-focused API Security Testing, helps organizations improve their security posture by eliminating operational inefficiencies, accelerating security-tested releases, and managing risk appropriately.

To learn more, visit [www.stackhawk.com](http://www.stackhawk.com)