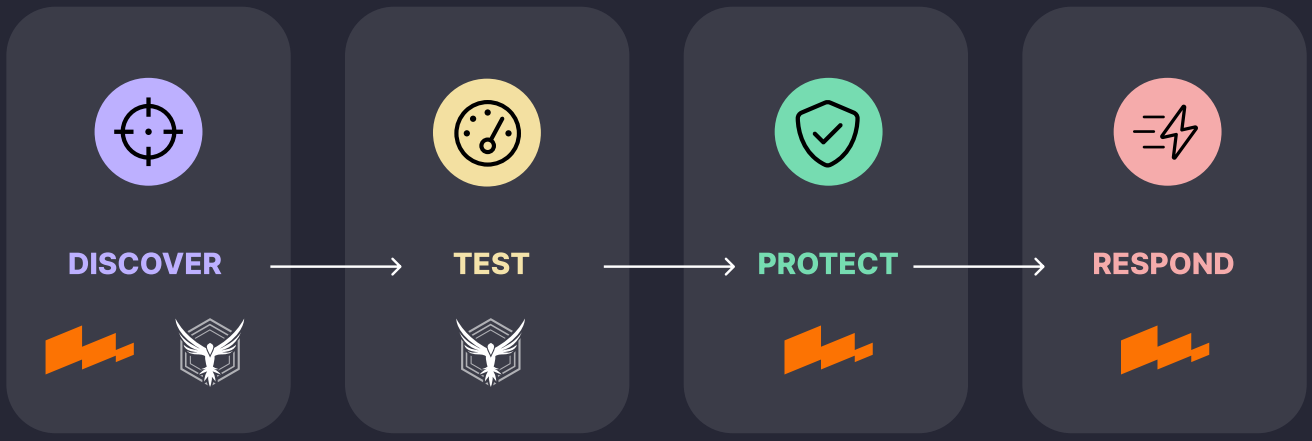
STACKHAWK | wallarm

Integrate Continuous API Security with StackHawk and Wallarm

The integration of StackHawk and Wallarm offers a straightforward, automated solution for maintaining API security. Wallarm's real-time endpoint inventory generates OpenAPI specifications, while StackHawk's DAST uses those specs to run continuous security tests. This integration enables AppSec and development teams to stay ahead of potential threats and ensure protection as APIs evolve.

Key Benefits

- **Automated OpenAPI Generation:** Wallarm's continuously creates OpenAPI specifications, keeping an accurate inventory of API endpoints.
- **Comprehensive API Security Testing:** StackHawk leverages OpenAPI specs for security scans based on real data, improving test coverage.
- **Early Vulnerability Detection:** StackHawk flags security vulnerabilities quickly, helping teams remediate issues before they reach production.
- **Scalable API Security:** Combined insights from Wallarm and StackHawk ensure security scales as API environments grow.



STACKHAWK | wallarm

Getting Started with the StackHawk and Wallarm Integration

If new to StackHawk, signup for a free 14-day trial at https://auth.stackhawk.com/signup

Step 1: Generate the OpenAPI Specification in Wallarm

1. **Open API Discovery:** In Wallarm's Console, navigate to the API Discovery section to view your endpoints.
2. **Filter Endpoints:** Apply filters to focus on specific endpoints, like those handling sensitive data.
3. **Export OpenAPI Spec:**
   - Export the OpenAPI spec as a `swagger.json` file to capture all endpoints.

Step 2: Configure StackHawk for Testing

1. **Add OpenAPI Spec to StackHawk:** Save the swagger.json file in your project directory and reference it in your `stackhawk.yml` file

```
app:
openapi: "path/to/swagger.json"
```

1. **Set Testing Parameters:** Adjust settings in `stackhawk.yml` to define scan parameters and specify any endpoints to include or exclude.
2. **Run the Security Scan:** Begin scanning your API endpoints, and receive detailed reports on any vulnerabilities detected.

Step 3: Review and Address Findings

1. **Review Reports:** Use StackHawk's insights to identify security vulnerabilities across your endpoints.
2. **Prioritize Fixes:** Focus on remediating high-risk vulnerabilities early in development to maintain a secure environment.

Get Started Today!

Together, StackHawk and Wallarm offer an automated approach for continuous API security as threats evolve.

Get started with a free-14 day trial at www.StackHawk.com
Book a demo of Wallarm at www.Wallarm.com

To learn more, visit www.stackhawk.com