APIsec

Find API vulnerabilities before they get to production.

APIsec provides the industry’s only 100% automated and continuous API security testing platform that eliminates the need for expensive, infrequent, manual pen-testing. APIsec produces certified and on-demand penetration testing reports required by the compliance standards, enabling enterprises to stay compliant at all times — at a fraction of cost.

APIsec pressure-tests the entire API before it gets into production where hackers can access sensitive data and functionality. Run APIsec tests on your APIs at any stage of the development cycle to identify critical flaws in API logic to ensure no endpoints can be exploited.

- **Continuous Security —** Continuous testing that keeps up with development.
- **Automated Testing —** Automated test creation ensures APIs are fully examined.
- **Complete Coverage —** Tests every endpoint and method against OWASP risks.
- **Speed —** Executes complete API test suites in minutes.
- **Integrated —** Integrates with orchestration, API platforms and ticketing.
- **Zero Touch —** No agents, no source-code access, nothing inline.

SEISMIC

Our customers ask us what we are doing to protect their sensitive data on Seismic, and once they see what we have done with APIsec, their confidence in us grows.

Tim Dzierzek, VP Info Security

slimstock

As we looked towards building our API focused products we were at a cross-road; do we build API security validations ourselves or do we leverage external companies. APIsec impressed us with what they were able to do quickly and the price to value ratio was incredible.

Daan Majoor, CTO

4 USE CASES FOR SECURING YOUR API

- Web & Mobile app API
- Public/External API
- Microservices/ Container API
- Privacy and Compliance

The challenges of securing APIs

Coverage

APIs are highly complex applications with myriad functions, all interoperating to deliver business objectives. Testing frameworks must cover the entire surface area of APIs, exercising every possible feature against all API threat types.

Scale

API can be made up of dozens or hundreds of separate endpoints, each supporting 3 – 5 different methods. Then add the myriad API threat vectors. Comprehensive testing can easily require thousands of unique attack playbooks.

Speed

APIs can change daily as Developers release new functionality, fix bugs, update logic, and more. Security assessments cannot get in the way and delay product releases. So testing needs to operate at Developer speed.

How It Works

1 — Learn your API

All APIsec needs to learn your API is a list of endpoints and methods. Or give us an OpenAPI spec, Swagger, Postman collection, etc. Or integrate directly into your API platform

2 — Create tests

APIsec automatically creates thousands of attack playbooks to test every corner of your API. The playbooks address the entire OWASP API Security Top 10 and more, giving you complete coverage.

3 — Run attacks

APIsec runs playbooks against your APIs to make sure there are no loopholes for hackers. We can run these in test/staging or production.

4 — Find vulnerabilities

The APIsec playbooks are designed to find the trickiest vulnerabilities — business logic flaws, not just standard security issues. We'll find any loopholes and integrate issues into your ticketing systems.

Sign Up for a free APIsec Pen-Test against your own API

Sign Up

The test provides 10X coverage of manual pen-testing, and includes a certified Pen-Test Report.

Getting started is easy. We just need a few pieces of information from you:

- URL for your API (pre-production or production)
- API spec file (OpenAPI, Swagger, RAML, Postman, etc.)
- 2 – 3 User accounts and credentials (used for testing)

That's it. Once we have everything you'll get a report in 24 hours.