



1 Hello,
2 we are "Aikido",
3 your all-in-one software
4 security platform.

5

6

7

8 ↪ aikido.dev

The Pains

Time-heavy

Finding the right tools to cover all the areas, languages, and infrastructures requires a lot of time.

Noisy

Tons of false positives & notifications overload.

Unwieldy

Confusing UI & fighter jet cockpit with computer science degree needed.

Pricy

Costs a shitload of money.

8-in-1 Security Coverage

Sure, you can juggle between multiple security tools with confusing pricing models. Tools that will overload you with irrelevant alerts & false positives.



Or you could get Aikido

4

The Solution



1

8 tools in 1

2

Noise massively reduced

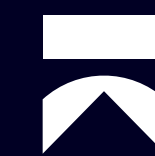
3

UI & UX is stellar

4

Price is not ridiculous

5



5

1

8 tools in 1 platform

1



Cloud posture management

Detects cloud infrastructure risks across major cloud providers.

2



Open source dependency scanning

Scans & monitors the open source dependencies in your codebase for known vulnerabilities and risks.

3



Secrets detection

Scours your source code for API keys, passwords, certificates, encryption keys, etc...

4



Static code analysis

Scans your source code for security risks before an issue can be merged.

New

5



Infrastructure as code scanning

Scans Terraform, CloudFormation & Kubernetes infrastructure-as-code for misconfigurations.

6



Container scanning

Scans your container OS for packages with security issues.

7



Surface monitoring

Monitors exposed surfaces for issues like SSL compliance & DNS takeover attack risks.

8



Open source license management

Export your open source licenses with one click and monitor non-reputable or problematic licenses.

6 2 Noise massively reduced

Only get alerts  that matter to **you**.

your environment.

your risk tolerance.



Deduplication

Groups related issues so you can quickly solve as many issues as possible.



Auto-Triage

Analyzes & monitors your codebase and infrastructure to automatically filter out issues that don't affect you.











Custom Rules

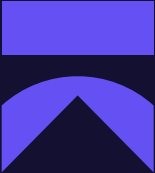
Set up custom rules to filter out the irrelevant paths, packages etc. You'll still get alerted when there's a critical issue.

4 Price is not ridiculous

Competition

-  Open source dependency scanning \$\$\$
-  Open source license reporting \$\$\$
-  Secrets detection \$\$\$
-  Surface monitoring \$\$\$
-  Static code analysis \$\$\$
-  Cloud posture management \$\$\$
-  Infrastructure as Code Scanning \$\$\$
-  Container scanning \$\$\$

Aikido



Flat fee,
no hidden charges.

Pro **€249**

Enterprise **€999**

Aikido integrates with your

git     , clouds    ,

CI/CDs    , languages     

   , compliance systems   ,

issue trackers    , IM   .

We're **Product-led**

Starter

€0

- ✓ Up to 20 repos & 1 cloud
- ✓ Basic CI integrations
- ✓ Task management integrations

Pro

€249 /m

- ✓ Up to 200 repos & clouds
- ✓ Full CI integrations
- ✓ User groups
- ✓ Compliance suite integrations

Enterprise

€999 /m

- ✓ Unlimited repos & clouds
- ✓ Public API
- ✓ Audit logs & reporting
- ✓ Feature branch scanning

11

Our great customers

 Showpad,  OTA Insight,  Officient,
 Cake.app,  Journey.io, and  Apideck

Value

Save Time

- ✓ Auto-triaging / ignoring
- ✓ Buying, configuring & maintaining multiple tools
- ✓ Assigning easily

Sell More

- ✓ We help you get SOC2 & ISO compliant
- ✓ We'll get you through security reviews faster

Save Costs

- ✓ We'll help you postpone the hiring of security engineer, or further building out that team.

Founded by

Product



Amber Rucker,



Roeland Delrue,

Revenue & Ops

Marketing



Felix Garriau &



Willem Delbare.

Tech

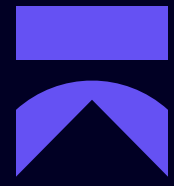
Mission

To simplify software security for developers who have other shit they would rather be doing.

Sounds exciting?

[Scan your repos for free](#)

[Schedule a meeting](#)



1

2





3

↳ aikido.dev

Annex

Aikido Security vs. Competitors












				
Open source dependency scanning	✓	✓	✓	✓
Cloud posture management	✓	✗	✓	✓
Secrets detection	✓	Enterprise only	✗	✗
Open-source license reporting	✓	✗	✓	Cloud only
Static code analysis	✓	Enterprise only	✗	✗
Surface monitoring	✓	✗	✗	✗
Container scanning	✓	✗	✓	✗
Infrastructure scanning	✓	✗	✗	✗

Example Findings







The dashboard displays a list of security findings. A dropdown menu is open over the 'Type' column, listing various issue categories. The findings table includes columns for Name, Severity, Location, Age, Status, and Assignee.

Type	Name	Severity	Location	Age	Status	Assignee
OS Dependencies	Django - Old version allo /	Critical	poetry.lock	20 h	New	
Cloud posture	Load balancer allows inv in alb.tf and ecs.tf	High	Production	5 h	To Do	
Exposed secrets	GCP api key secret expo in billing.yaml	High	marketing.py	2 m	PR Open	Bert
SAST	Using Pickle can lead to remote code execution in data_processor.py	High		10 d	PR Open	Bert
Surface monitoring	Outdated MySQL version is no longer supported in Dockerfile	Medium	docker image	3 d	PR Open	Roeland
Infrastructure as code	Subdomain at risk of takeover help.domain.com	Medium		15 d	Task Open	Roeland
	Root account should have MFA enabled /	Medium	aws Staging	2 m	Task Open	Amber
	8 exposed secrets	Low	RepoName	3 days	Solved	

Example Findings

Type	Name
	Django - Old version allows SQL injection /
	Load balancer allows invalid HTTP headers in alb.tf and ecs.tf
	GCP api key secret exposed in billing.yaml
	Using Pickle can lead to remote code execution in data_processor.py
	Outdated MySQL version is no longer supported in Dockerfile
	Subdomain at risk of takeover help.domain.com
	Root account should have MFA enabled /
	8 exposed secrets within openai.json, name.json and x others
	loader-utils Abuse of javascript's prototype API possible (prototype pollution)

Show issue type

-  OS Dependencies
-  Cloud posture
-  Exposed secrets
-  SAST
-  Surface monitoring
-  Infrastructure as code

We're compliant

We're implementing security best practices aligned with the highest standards.



SOC 2

Compliant



27001

Implementing

FAQ's

¹ Does Aikido ever store your code?

In short: Aikido does not store your code after analysis has taken place. Some of the analysis jobs such as SAST or Secrets Detection require a git clone operation. Below we talk about the technical measures we take to ensure your code is protected:

- We perform risky actions such as git clones in a fresh docker container for each repository. After analysis, the data is wiped and the docker container is terminated.
- For Github, no refresh or access tokens are ever stored in our database. We use the new GitHub Apps which do not require this. Even a database breach of Aikido itself would not result in your GitHub code being downloadable.
- By default, our integrations require a very minimal read-only scope. Only if you enable special features such as Autofix Pull Requests will Aikido request write accesses.
- Aikido has SOC2 Type 2 certification. A report is available upon request. That means we adhere to several organizational and technical policies by default.
- Aikido runs on AWS, mainly in the EU-west-1 region in Ireland. That means all processing and storage will stay in that location.

² Does Aikido make changes to my codebase?

We can't & won't, this is guaranteed by read-only access.

FAQ's

3 What happens to my data?

We clone the repositories inside of temporary environments (such as docker containers unique to you). Those containers are disposed of, after analysis. The duration of the test and scans themselves take about 1-5 mins. By default, all the clones and containers are then auto-removed after that, always, every time, for every customer. This process repeats every 24 hours, to provide continuous monitoring.

4 How can I trust Aikido?

We're doing everything we can to be fully secure & compliant. Aikido has been examined to attest that its system and the suitability of the design of controls meets the AICPA's SOC 2 Type II requirements. Next to that we are implementing ISO 27001 compliance standards. Visit our Trust page to learn more about our security practices.

5 When does Aikido scan?

Aikido monitors your security by scanning for new vulnerabilities every 24 hours, and upon every PR merge. Whenever you like you can trigger a manual rescan directly in the app.

Process to ensure code security



Select repos
of your choice



Temporary clones are secured
in isolated containers



Scans are being
performed in 1-3 minutes



Containers get
destroyed

The whole process takes 5 minutes in total and repeats every 24 hours.