42crunch | axway

# UPGRADE API SECURITY
## for Axway API Management

**42CRUNCH HAS THE UNIQUE CAPABILITY** TO FEED TRULY SECURITY TESTED APIs INTO THE API MANAGEMENT LIFECYCLE.

42Crunch implements a proactive approach to API security by certifying at design time the Swagger/OAS files used to build the security policies for the API Gateway to protect APIs at runtime.

API Gateways have provided the platform for the explosion in the adoption of APIs over the past decade. The flipside of this success has been the rise of API attacks which now represent the most-frequent attack vector for data breaches of enterprise web applications. The Axway API Gateway offers a good set of capabilities for role-based access control, traffic throttling and verification of content, but that is not enough in today's world. It requires an approach that starts at the beginning of the API lifecycle and automates it until it hits production. 42Crunch integrates with Axway to upgrade its API management offering, with a robust set of security testing and governance capabilities, enabling full end-to-end API security.
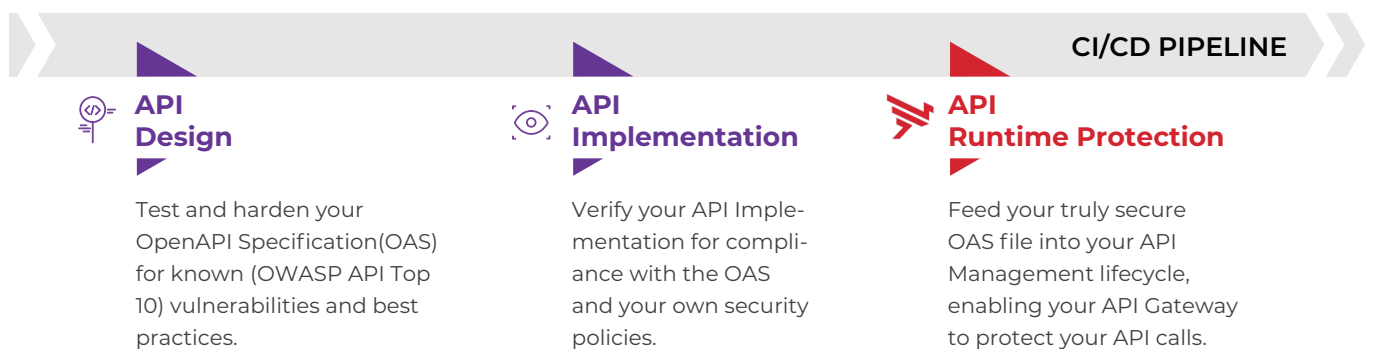
## RUNTIME PROTECTION
### AXWAY

· Integrate with Identity Management systems to protect against unauthenticated and unauthorized access
· JSON Threat protection
· Schema validation
· Threat protection through REGEX
· Rate limiting

## DESIGN TIME SECURITY GOVERNANCE **42CRUNCH**

· Detect potential security vulnerabilities from design time through analysis of OpenAPI/Swagger files
· Build secured JSON schemas which can be used effectively in the schema validation policies inside the Axway API Gateway
· Automatically test APIs' conformance to the specifications
· Test security resilience of the APIs as part of continuous integration
· Deliver security certified OAS files into the API Manager and the API Gateway

## AUTOMATE YOUR SECURE API LIFECYCLE

**CI/CD PIPELINE**

### API Design

Test and harden your OpenAPI Specification(OAS) for known (OWASP API Top 10) vulnerabilities and best practices.

### API Implementation

Verify your API Implementation for compliance with the OAS and your own security policies.

### API Runtime Protection

Feed your truly secure OAS file into your API Management lifecycle, enabling your API Gateway to protect your API calls.

# AUTOMATING API SECURITY WITH 42CRUNCH

Leveraging 42Crunch, Axway admins reduce manual tasks and automate security into the API workflow in order to get secure code quickly out the door and into production. Following the steps below, Axway admins can focus on driving API utilization in the API Marketplace.

## HOW DOES 42CRUNCH
## ENHANCE YOUR API MANAGEMENT SOLUTION

**01**   42Crunch audits your OAS files for known OWASP Top 10 vulnerabilities and provides remediation help inside the developer's IDEs.

**02**   42Crunch scans the API implementation continuously against the contract, detecting drifts and implementation security issues.

**03**   Approved OAS file is used in Axway's API Manager to create a backend API in the repository using the API Manager REST API for API Repository.

**04**   Utilizing the API Manager REST API for Proxy Registration the predefined security rules inside the API Gateway can be assigned while creating the frontend API.

**05**   All the above steps should be automated using your preferred CI/CD tools to promote the secured API from design through the environments to production.