42Crunch + API Management

Protect your APIs from code to production allowing innovation at the speed of business without sacrificing security

The Growing Threat Landscape

The new wave of modern technology has led to a rapid adoption and proliferation of APIs – expanding organizations attack surfaces exponentially. What use to be 5-10 APIs has become hundreds or even thousands, and they all need to be properly documented, managed and secured – all while keeping up with the demand of innovation. If the right tools aren't in place, it's easy for security to get over-looked and improperly implemented – leaving your organization wide open for sophisticated API attacks.

Gartner predicts that "by 2022, API abuses will be the most frequent attack vector resulting in data breaches for enterprise web applications."

API Management Platforms are becoming a foundational part of organization's API programs because they provide tools to make the design, deployment, security and maintenance of APIs easier and more efficient. Though they do offer some necessary security functionality such as OAuth and rate limiting – that is not enough to fully protect against sophisticated attacks directly targeting APIs.

42Crunch and API Management are Better Together

42Crunch compliments API Management Platforms by adding a deeper level of security functionality to ensure that API programs are not only effectively managed but also stay secure from code to production.

With 42Crunch, security can be easily defined in OpenAPI contracts, tested for bad behavior, and protected by a micro API firewall with the click of a button – ensuring unparalleled protection across the entire API lifecycle.

Better Together	API Mgmt	42Crunch
Developer Portal	●	
OAuth Key Mgmt	●	
API Call Transformation & Orchestration	●	
API Security Audit at Design and Implementation		●
Contract Conformance Testing		●
API Contract Enforcement		●

42Crunch Platform Features

Actionable Security Insights: Reports contain specific information on each issue and the overall score so developers and security know exactly what needs to be fixed and why any particular issue is bad.

Contract Conformance: All API definitions are tested in a pre-production environment to make sure that the API contracts are followed by the implementation.

Micro API Firewall: Protection module adds the super-efficient component that enforces the API security with sub-millisecond overhead.

Positive Security Model: Lock down API definitions to only allow calls and responses that follow them. This automatically protects against edge cases and also potential unknown vulnerabilities in the implementation stack.

Centralized Management: Centrally manage policy requirements, have them evaluated and enforced across entire API lifecycle.

Seamless Integration: Integrate right into developer tools, including integrated developer environments (IDEs) and continuous integration / continuous delivery (CI/CD) pipelines to reduce risks, provide more visibility, and deliver more secure code - faster.

ABOUT 42CRUNCH

42Crunch bridges the gap between API development and security teams with a simple, automated platform that provides auditing, live endpoint scanning, and micro API firewall protection. Unlike other solutions on the market, 42Crunch Platform empowers development, security, and operations teams with a set of integrated tools to easily build security into the foundation of the API, and enforce those policies throughout the API lifecycle. By delivering security as code, you enable a seamless DevSecOps experience, allowing innovation at the speed of business without sacrificing integrity.

Visit 42crunch.com to learn more.