

42Crunch API Protection

Runtime API Security Built on DevSecOps Principles

Introduction

Today, APIs are the primary target for cyberattacks. While API vulnerabilities originate across many layers of the technical stack, from infrastructure misconfigurations to coding bugs or supply chain flaws, they are ultimately exploited through the API transaction. This makes the transaction not just a point of exposure, but also the most effective choke point for defense. 42Crunch addresses this critical need by delivering runtime service-level protection through its micro-firewall technology, purpose-built for the dynamic nature of modern APIs.

DevSecOps in Action

The 42Crunch micro-firewall is configured from a hardened OpenAPI definition, or API contract, that defines the API runtime behavior, including allowed data and required security controls. The API firewall ensures that runtime behavior strictly aligns with the developer's intent by enforcing the contract. As the API evolves, runtime protection automatically adapts, maintaining a continuous feedback loop between development, security, and production. With 42Crunch, API security scales effortlessly with DevOps, maintaining robust protection throughout rapid release cycles and constant API changes.



Runtime API protection aligned with agile API development

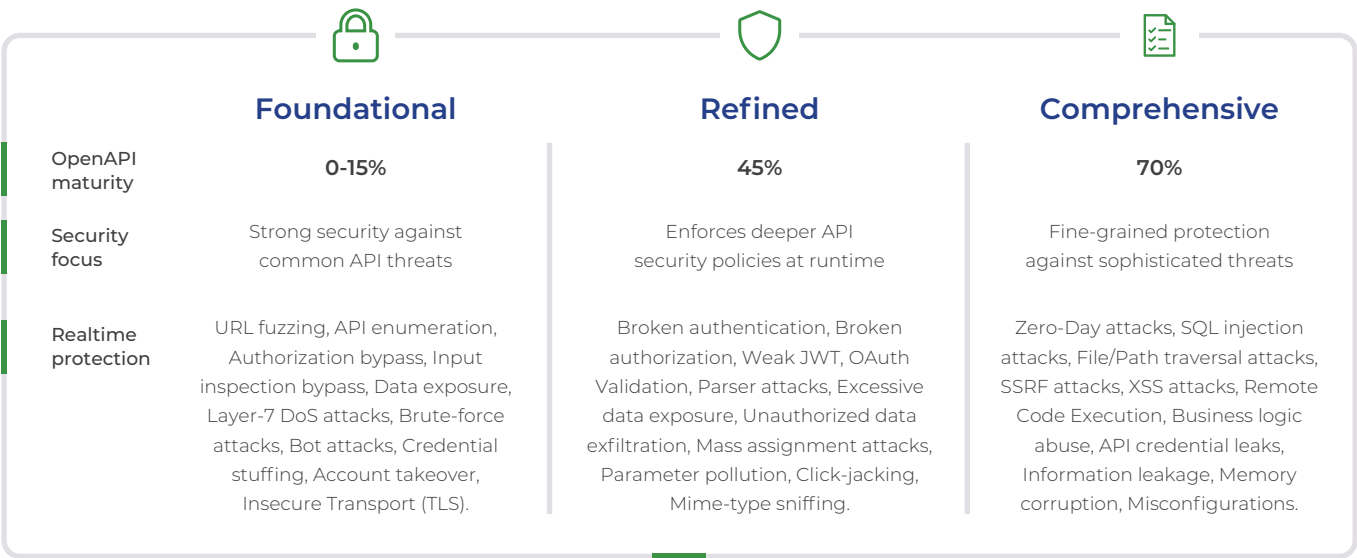
An Iterative Approach to API Security

Deploy protection where it matters most. The 42Crunch API micro-firewall secures APIs individually, enabling teams to prioritize high-value services and scale protection at their own pace. Start small, iterate fast, and strengthen protection continuously without slowing service delivery.

Immediate Value at Any OpenAPI Maturity Level

Get instant protection whether your API contracts are basic or fully detailed. Low-maturity specs benefit from baseline protections, while hardened contracts unlock advanced defenses like authentication, JWT validation, and strict schema enforcement.

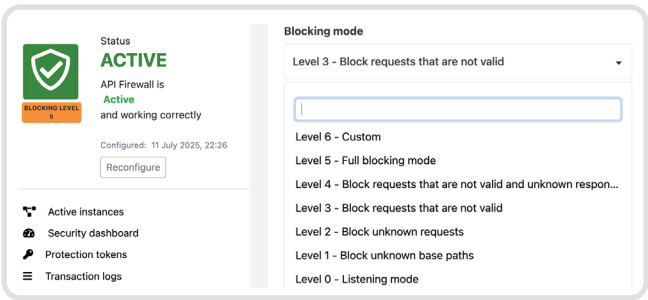
As shown, protection evolves with the maturity of your API specs, from initial creation through hardening the API contract. The tighter the contract, the stronger the security, all without making backend code changes.



Stronger runtime protections as OpenAPI maturity increases

Customized Blocking Levels

42Crunch API Protection also delivers up to seven granular blocking levels. This flexibility empowers teams to gradually adjust runtime enforcement as confidence in the API and its contract grows, enabling progressive hardening without risking service disruption.



Flexible Deployment for Modern Architectures

42Crunch API micro-firewall is designed for seamless deployment in cloud-native and containerized environments. It is typically deployed as a sidecar proxy, sitting alongside the API or microservice it protects. This model enables **fine-grained, per-service protection** against both north-south traffic (external-to-internal) and east-west traffic (service-to-service), enforcing consistent security policies close to the workload, and scaling horizontally with your API infrastructure.

Wire-Speed API Security with Minimal Overhead

42Crunch API micro-firewall is written in highly optimized C language and purpose-built for efficient API content inspection. Unlike traditional firewalls and API gateways that rely on external databases or policy engines at runtime, 42Crunch embeds all whitelist-based validation rules, derived from the hardened API contract, directly inside the micro-firewall runtime. This eliminates costly API lookups and context switching, resulting in **extremely low per-request overhead**.

With average latencies around 1-3ms, 42Crunch micro-firewall is orders of magnitude faster than conventional runtime security tools, making it **the only viable option for real-time API content inspection and protection**.

42Crunch API Protection – Real-Time Security for Modern APIs

APIs are now the top target for cyberattacks, with the API transaction being the most effective point for defense. 42Crunch delivers real-time, service-level protection through micro-firewalls generated directly from your API contracts. This DevSecOps-aligned approach ensures security scales automatically with each API update, without slowing development.

Whatever the maturity of your API specs, 42Crunch provides immediate and effective protection, with flexible blocking modes that enable progressive hardening. Designed for cloud-native architectures, the micro-firewall deploys as a sidecar with wire-speed performance and minimal latency.

**Protect your APIs
where it matters most.**



Learn more or request a demo at 42Crunch.com