42Crunch vs Legacy WAF

Extend protection beyond the edge with 42Crunch's automated API Security Platform

"65% of organizations experienced successful application-layer attacks that bypassed their existing web application firewall (WAF)."

"Managing legacy WAF deployments is complex and time-consuming, requiring an average of 2.5 security administrators who spend 45 hours per week processing WAF alerts, plus an additional 16 hours per week writing new rules to enhance WAF security."

Ponemon Institute: The State of Web Application Firewalls

Out with the Old, in with the New

WAFs were built for a specific purpose: protect web applications. Web applications architecture has evolved over the past years to use APIs as their back-ends -- instead of legacy application servers. APIs are now the entry point into your enterprise, exposing data and processes from your core enterprise applications. The other major change is the externalization of some of this data and processes to public cloud and SaaS applications. An application today is typically constructed of up 5 to 10 APIs accessing internal and external systems.

While WAFs are capable of filtering HTTP traffic and understand the protocol, they do not understand APIs. In order to properly protect APIs, you need to understand API specific protocols and standards. Using a legacy WAF to protect APIs entails defining a lot of specific rules to avoid false positives, which is a manual process that makes it hard to scale with the constant API changes.

This makes legacy WAF solutions costly and time consuming to maintain, incapable of detecting or preventing attacks that exploit the vulnerabilities unique to APIs, and unable to scale within complex modern day infrastructures.

Protect Your APIs with 42Crunch

The 42Crunch platform provides a set of integrated tools to easily secure your entire API infrastructure by building security into the OpenAPI contract, and enforcing those policies throughout the entire API lifecycle. By delivering security as code you enable a seamless DevSecOps experience, allowing innovation at the speed of business without sacrificing security.

Capabilities	42Crunch	WAF
API Native	●	—
Default Security Model	allowlist	denylist
Developer Driven Security	●	—
Configuration Base	OpenAPI produced by developers	Rules - standard and fee-based
Firewall Configuration per API	Automatic from OpenAPI	Manual from custom rules
Kubernetes Native	●	—
Cloud Native	●	⊙
Platform Agnostic	●	—
Multi-Cloud Support	●	—
Microservices Support	●	—
Latency	Microseconds	?

Deliver API Security by Design with 42Crunch

- **API Native:** Addresses natively APIs' unique security requirements across data validation, authentication, authorization, confidentiality and integrity.
- **Positive Security Model:** The API Contract is the core of the security configuration, allowing to automatically enforce traffic inbound and outbound.
- **Integrate into CI/CD:** Push your OpenAPI definition to your CI/CD pipeline and automatically audit, scan and protect your API.
- **Platform Agnostic Micro API Firewall:** Thanks to its low footprint, 42Crunch micro API Firewall can be deployed at scale on any container orchestrator such as Kubernetes, Amazon ECS or Red Hat OpenShift.
- **Intuitive User Interface:** The intuitive interface makes it easy to get started on day one, and provides real-time Security dashboards with actionable data.
- **Designed for DevSecOps:** Enables a seamless DevSecOps experience from development to deployment through automation.