DATASHEET

API Threat Protection

Runtime Content Validation and Threat Detection

Despite taking steps to improve security at API design and development time, your APIs will inevitably still come under attack in production. A defense-in-depth approach is the foundation of risk reduction — regardless of how well designed your APIs are, they will still be attacked by persistent and skilled adversaries. Despite the best efforts of traditional web application firewalls and API gateways, runtime attacks on APIs continue to breach these defenses with increasing financial costs and brand reputational damage. This suggests the need for a dedicated API protection mechanism at runtime.

Key Elements of Secure API Protection Include:

- JWT validation
- Secure transport options
- Brute force protection
- Invalid path or operation access · Rejection of invalid request data · Filtering of response data
- Protection logs should be ingested into standard SIEM/SOC platforms to ensure visibility of API security operations at a pan-organizational level.

> 42Crunch's ability to secure both the CI/CD pipeline & the runtime environment makes it a compelling candidate for any API security project.
>
> **Rick Turner, Principal Analyst.**
>
> OMDIA

How 42Crunch Helps

The 42Crunch API Protect service is an API micro-firewall that enforces at runtime the API-specific security policy as defined in the API contract, on all incoming as well as outgoing transactions. Transactions that do not conform to the OpenAPI definition are automatically blocked. It can be used to protect both north-south and east-west traffic and as it can deployed from the CI/CD pipeline it will automatically reconfigure each time the API changes. In microservice deployments, API Protect is deployed separately with each instance of the microservice, so rate limiting is also enforced separately on each instance.