

API Governance

Retaining Oversight of Your API Security

API Governance as it specifically relates to an API security context can be defined as the governance process that ensures APIs are designed, developed, tested, and protected in compliance with an organization's security process. Traditionally Web Application Firewalls and API Gateway solutions have been used as the enforcers of API security, however, as the volume and complexity of API deployments has grown over time, these solutions are patently not fit for purpose.

Key Principles of API Governance in a security context:

- Ensuring your APIs are consistent i.e., use standard patterns for authentication and authorization
- Standard processes are adhered to for the development of new APIs
- Data privacy and compliance requirements are adhered to via the enforcement of managed API security policies
- A process is observed for APIs at their end-of-life to eliminate insecure zombie APIs

How 42Crunch Helps

The 42Crunch API security platform ensures that API development adheres to the mandated security policy, and gives application security teams full visibility and control of the process.

42Crunch's Security Quality Gate feature enables appsec teams to customize the enforcement of compliance and standards as developers code. The Data Dictionary feature lets administrators define a dictionary of formats for developers to use as they code APIs.

Additionally our SIEM integrations also actively monitor and report on API endpoints in real time.



Knowing that any developer changes will be caught early to prevent contract breaking or straying from the OAS allows us to focus on all the other aspects of our API lifecycle."

Gartner
Peer Insights™

