Wie bekomme APIs so sicher wie möglich

Wie binde ich Sicherheit in den API Lebenszyklus ein und welche tools helfen mir dabei. Ein Blick aus Sicht der API Entwickler und der Security Teams

Axel Grosse

Email: axel@matanga.io
LinkedIn: https://www.linkedin.com/in/axelgrosse/

Gartner

Widespread use of APIs without an overarching API strategy leads to governance challenges, security and compliance risks, and failure to deliver meaningful business outcomes

Strategic Planning Assumptions

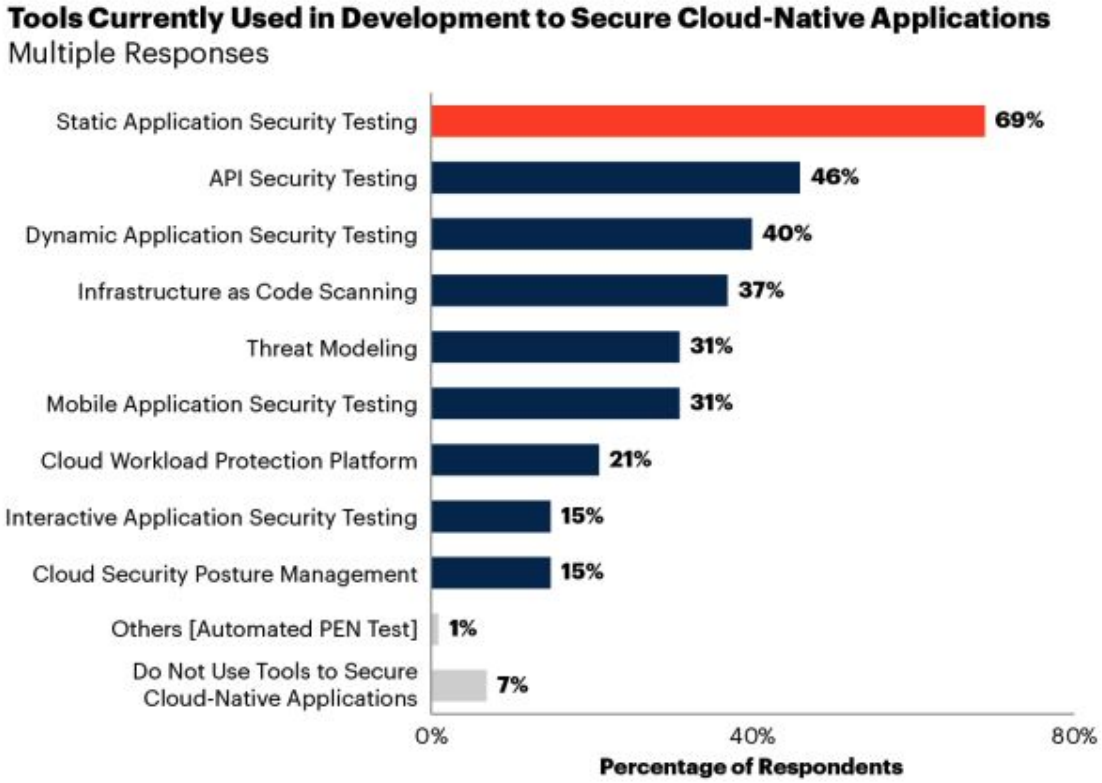
By **2024**, API abuses and related data breaches will nearly double.

By **2025**, more than 80% of organizations will identify themselves to have implemented advanced or expert level API strategies.

By **2025,** more than 75% of organizations will directly or indirectly monetize APIs.

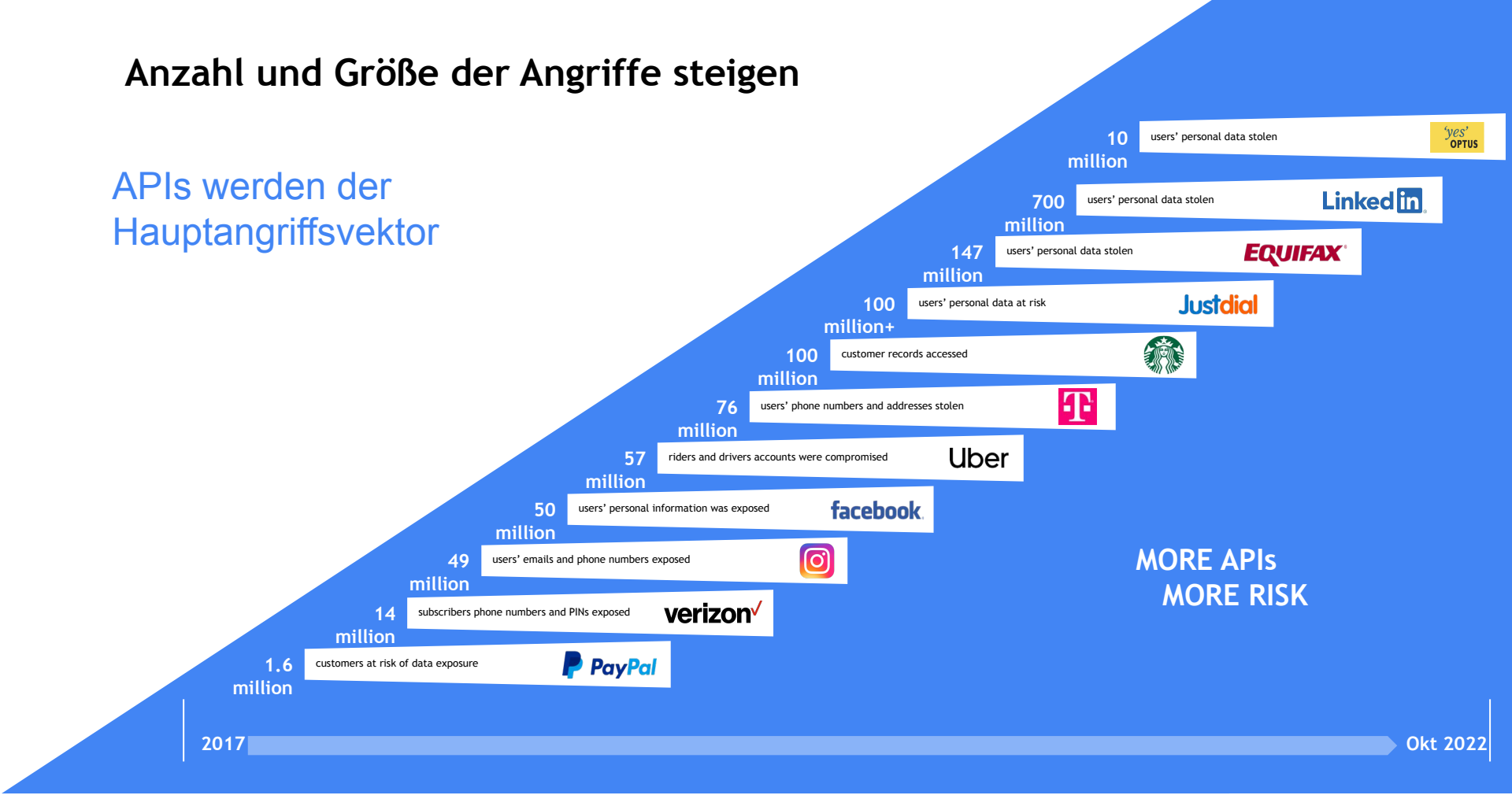
Figure 2: DevSecOps Tools in Development to Secure Cloud-Native Applications

Gartner



Anzahl und Größe der Angriffe steigen

APIs werden der Hauptangriffsvektor



Optus: Telekom in Australien

Sicherheitslücke

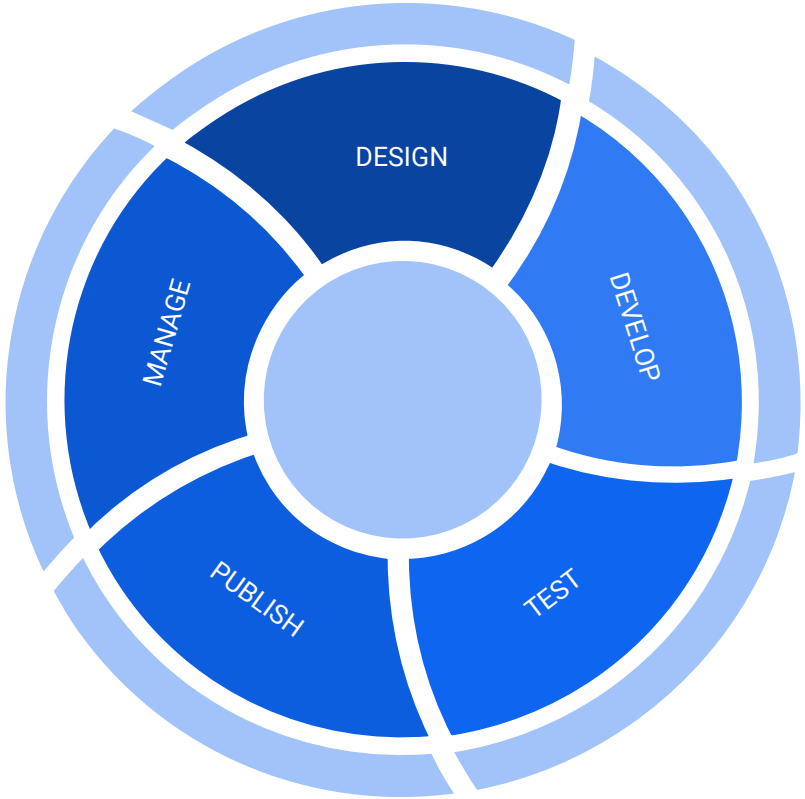
- Public API ohne Authentifizierung
- PII Daten unverschlüsselt
  - Pass/Führerschein Nr
  - Adresse
  - Geburtsdatum
  - TelefonNr
- Nutzennummer waren seriell in der URL

Einordnung

- 10 Millionen Datensätze entspricht ca. 40% der Bevölkerung Australiens
- Mit den Daten lässt sich sehr einfach **Identitätsdiebstahl** erstellen.
- **Folgeeffekte** des Datendiebstahls sind schon sichtbar (nach einem Monat)

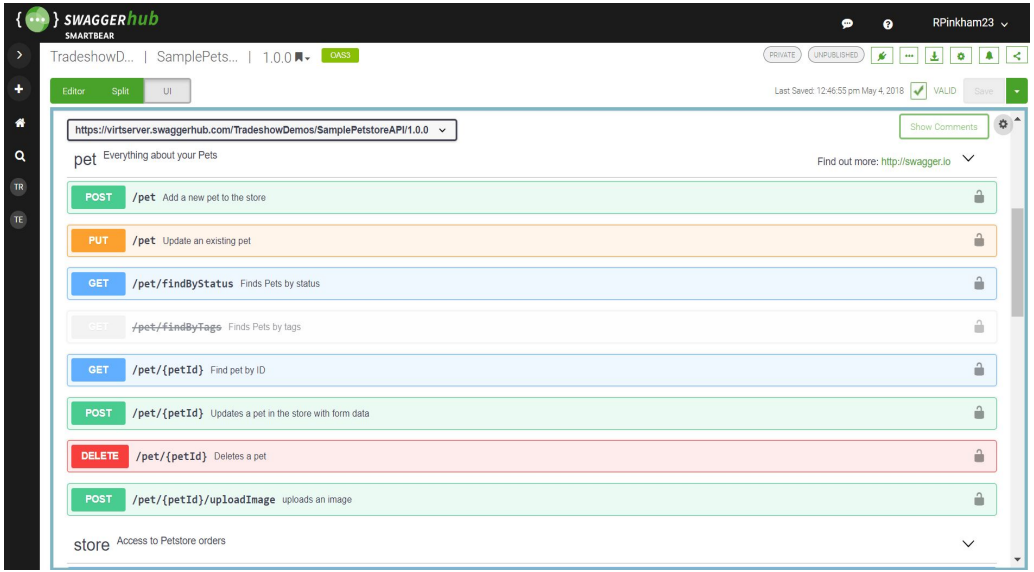
source: https://www.upguard.com/blog/how-did-the-optus-data-breach-happen

API Lifecycle



APIs sind ein leichtes Ziel

- Sie sind einfach zu finden
- Sie sind gut dokumentiert
- Angriffe lassen sich leicht automatisieren
- Es gibt super Werkzeuge um die Angriffe zu automatisieren.



2019

#	OWASP API Top 10 Vulnerabilities
1	Broken Object Level Authorization
2	Broken User Authentication
3	Excessive Data Exposure
4	Lack of Resources & Rate Limiting
5	Broken Function Level Authorization
6	Mass Assignment
7	Security Misconfiguration
8	Injection
9	Improper Assets Management
10	Insufficient Logging & Monitoring

2023

	OWASP API top 10
1	Broken Object Level Authorization
2	Broken Authentication
3	Broken Object Property Level Authorization
4	Unrestricted Resource Consumption
5	Broken Function Level Authorization
6	Unrestricted Access to Sensitive Business Flows
7	Server Side Request Forgery
8	Security Misconfiguration
9	Improper Inventory Management
10	Unsafe Consumption of APIs

Die Vorteile eines Positive Security Model

POSITIVE SECURITY MODEL

- **DENY ALL**
- Allowed data types strong defined and enforce in OAS mode
- Data format can be precisely defined
- Operations can be fully specified too

- **Only allow data conforming to specification — anything else is an error**
- **Only allows “known good”**

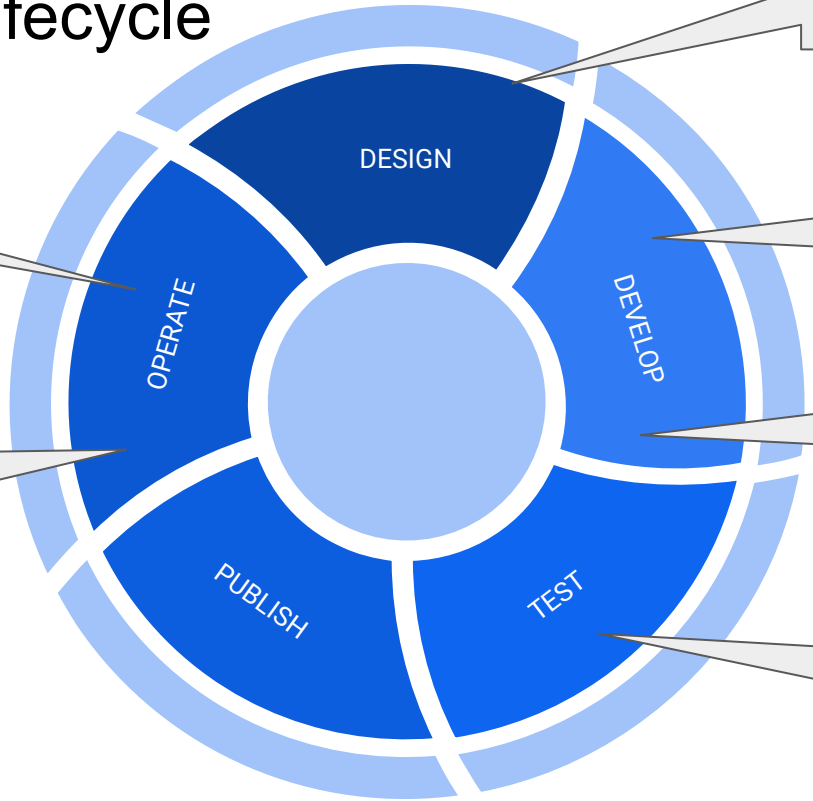
VS.

NEGATIVE SECURITY MODEL

- **ALLOW ALL**
- Attempts to interpret data based on the runtime context i.e., Javascript, HTML
- Attempt to block what shouldn’t be present in a given context
- Can easily be subverted with encoding, etc.
- AI will be able to understand the protection

- **Attempts to block “known bad”**

SECURE API Lifecycle



Check OpenAPI Spec file for possible flaws

Check Service behaviour Does it conform ?

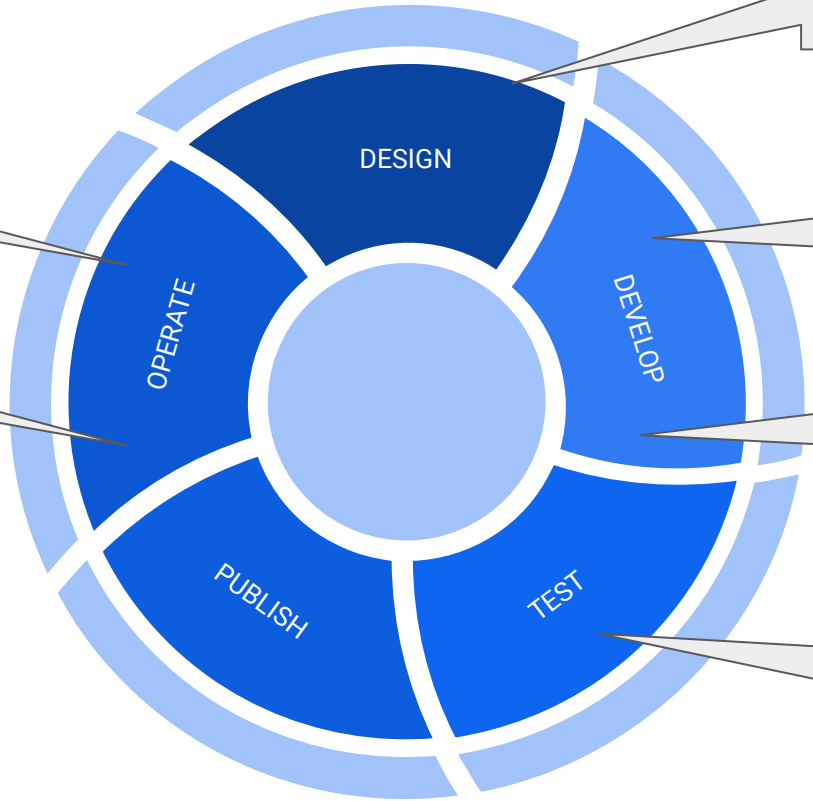
Scan Code for vulnerabilities and bad libs

Test as usual for functional and integration

Protect at runtime API Gateway / API Firewall

Monitor behaviour and detect abuse

SECURE API Lifecycle Tools



42Crunch Audit

42Crunch Scan

SonarCube, Veracode, Checkmarx, etc.

Snyk, Veracode, Checkmarx, etc.

Noname, Salt, Broadcom, Axway, Google, AWS, Azure

42Crunch, Kong, Tyk, Broadcom, Axway, Google, AWS, Azure

API Security testing tool example

THE DEVELOPER FIRST API SECURITY PLATFORM

SECURITY MANAGEMENT & GOVERNANCE

Visibility & control of security policy enforcement throughout API lifecycle for security teams.

API AUDIT

Lock down your API's definitions to reduce the attack surface and remove potential security gaps.

API SCAN

Dynamic runtime testing of your API to ensure compliance with API Contracts.

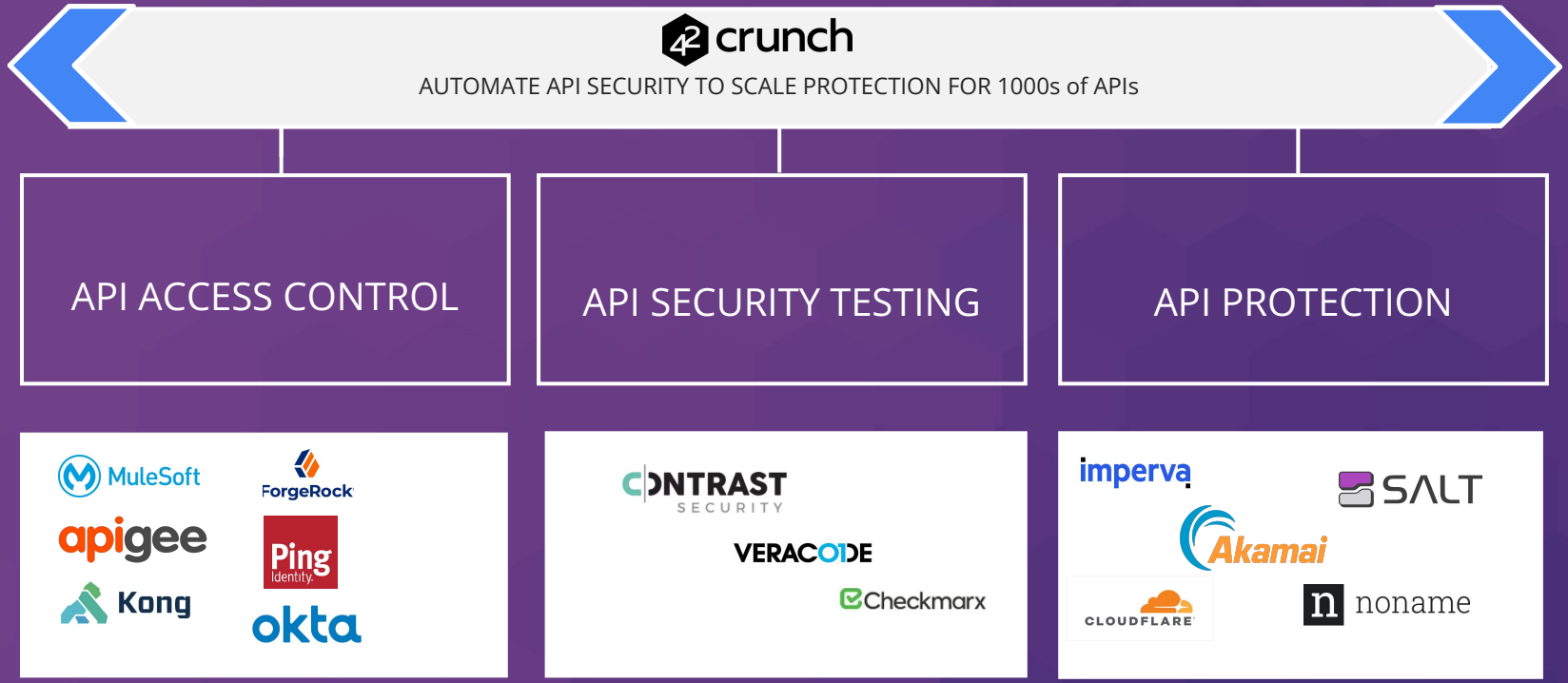
API PROTECT

Protect each API with an API micro-firewall to distinguish legitimate traffic from malicious API attacks.

INTEGRATED ACROSS API LIFECYCLE

Continuous security enforcement across IDE, CI/CD and at runtime.

API SECURITY LANDSCAPE



Gartner

API Security: Protect your APIs from Attacks & Data Breaches

Contact

Axel Grosse

Email: axel@matanga.io

LinkedIn: https://www.linkedin.com/in/axelgrosse/