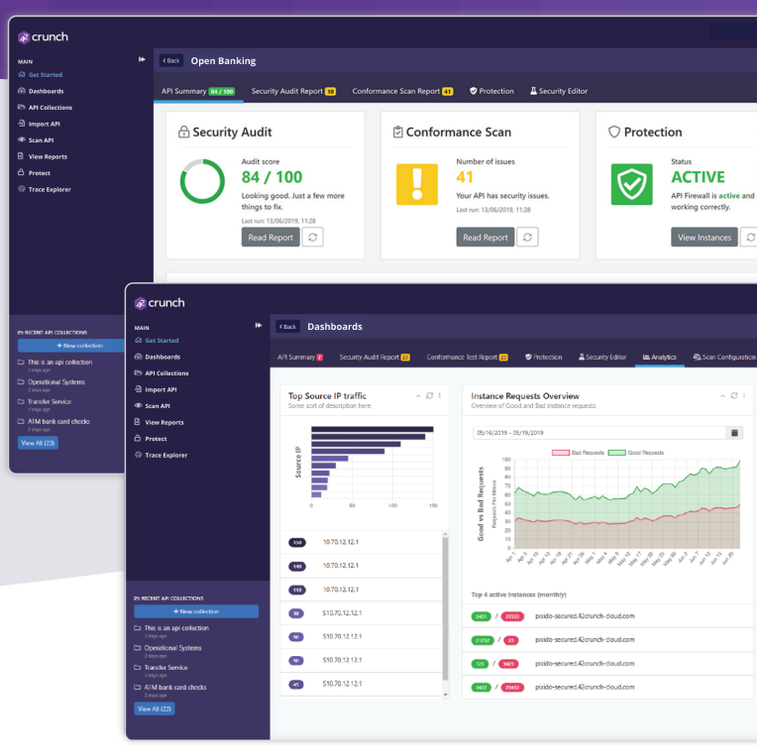
DATASHEET

Automate API Security Testing & Threat Protection

The only API security platform to proactively test, fix and protect your APIs from development to runtime



Enterprises deploy 42Crunch to navigate the challenge of enforcing API security across a complex landscape of distributed development teams and multiple technical architectures.

42Crunch automates the enforcement of API security policies and standards across these development and security ecosystems. We help security take back control of API Governance and give development the tools they need to build safer APIs.

DELIVERING VALUE TO SECURITY & DEVELOPMENT TEAMS

Governance & Compliance

42Crunch brings API semantic, code hygiene and data definition compliance to all APIs. Security teams now gain oversight and governance of the policy enforcement throughout the API lifecycle.

Automate Manual Tasks

Security audit and scanning become automated checks ensuring that insecure code never makes it to the master branch and production deployment. Runtime protection policies are automatically redeployed with each API change.

Security by Design

Empower your developers to implement security as code in their workflow. 42Crunch is embedded in IDEs, code repositories & CI/CD environments.

Remove False Positives

Traditional solutions generate an unacceptable volume of false positives. Eliminate noise and only see the issues that actually matter and need to be fixed.

Accelerate API Delivery

Security is never the bottleneck. Enable your developers to focus on high value work to improve and accelerate the delivery of secure world-class APIs.

Scale Protection

Eliminate friction between development and security teams and automate protection to ensure that your API security program has unlimited scale.

PLATFORM CAPABILITIES

42Crunch is uniquely designed to enable a collaborative DevSecOps approach to API security. All teams: Application Security, API architects, Developers, QA, and Operations – get a shared view of API security, its shared definition, and a shared understanding of what needs to be done to enable security at scale. Core services include:

API Governance

- Discover and catalog APIs automatically
- Automate building of API Contracts from traffic and other sources
- Integrated with development repositories

API Security Testing & Vulnerability Detection

- Empower developers with security tools with no false positives
- Instantly calculate APIs security score against 300+ checks
- Automate security fuzzing from API contracts
- Deploy within any open source or commercial CI/CD

Security Governance & Compliance

- Standardized, secured API contracts
- Centrally managed security compliance rules
- Centrally managed runtime security policies

Runtime API Threat Protection

- Automated configuration from API Contracts, with no manual rules.
- Detect & block shadow /zombie APIs as well as API-specific attacks
- Standard, deployment-agnostic policies, working with any API Gateway
- Connect to your favorite SIEM for combined threat intelligence

Integrated into Developer & AppSec Workflows

Continuous API security enforcement from design through production.

API GOVERNANCE

The success of an enterprise's API security strategy depends on ensuring that the APIs are designed, developed, tested and protected in compliance with its security policies. A robust API governance framework ensures that these various stages comply with the organizational methodologies. Companies successfully use 42Crunch to automatically discover and catalog APIs at runtime and designtime, through traffic monitoring and integrations with development repositories, such as GitHub. Companies can automate the building of API Contracts in adherence to OpenAPI/Swagger specifications to ensure a standardized approach to design is adopted across the enterprise.

SECURITY GOVERNANCE AND COMPLIANCE

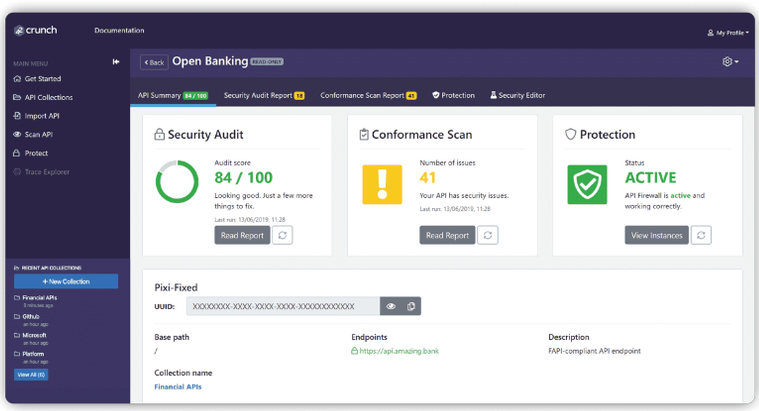
The 42Crunch platform helps API security governance and compliance teams trust, but verify the work of development teams. It offers risk officers a centralized view of API contract workflows across distributed development teams to help consolidate security design and enforcement efforts at all stages of the API lifecycle. Leveraging the platform's advanced security quality gates features, security teams configure, customize and automate the enforcement of security policies from design to runtime.

42Crunch also offers deployment-agnostic policies that work out of the box with many existing API gateways. Combining 42Crunch's API design and run-time security controls with security incident and event management (SIEM) solutions offers enterprises an holistic view of their API security program and gives them the confidence to roll out their API-driven initiatives at scale.

API SECURITY TESTING AND VULNERABILITY DETECTION

Companies use 42Crunch to continuously scan for API contract misconfigurations and vulnerabilities at both testing time and runtime. 42Crunch detects OWASP API Security Top 10 issues early in the API lifecycle and rejects unexpected requests at runtime.

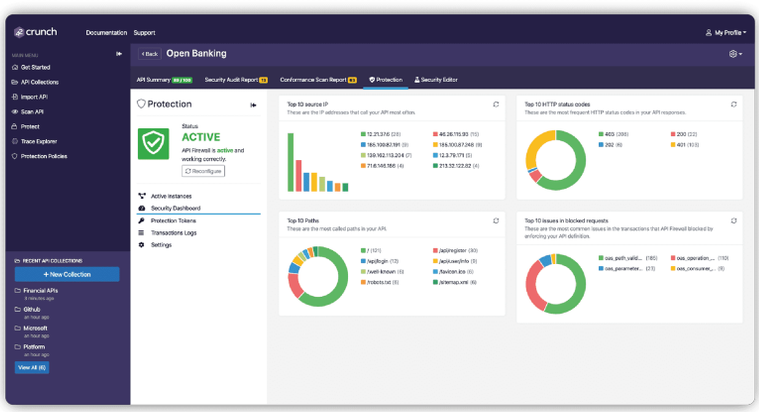
42Crunch delivers API security from design to production. We empower developers to remediate quickly and test often with tooling that resides within their existing platforms and workflows. These tools run inside the leading Integrated Development Environments (IDE) and provides instant security scoring (300+ checks) for prioritization and remediation advice at design-time to help developers build the best API contracts possible.



RUNTIME API THREAT PROTECTION

A defense-in-depth approach is the foundation of risk reduction. In addition to implementing API design-time security testing and detection capabilities, enterprises also need to protect their APIs via dedicated API protection mechanisms at runtime.

With 42Crunch, enterprises remove the need for manual rule writing by automating the configuration of API protection directly from the CI/CD. Using this proactive positive security approach, 42Crunch detects & blocks shadow /zombie APIs as well as API-specific attacks and unlike traditional WAF-based solutions, distinguishes API attacks from legitimate API content traffic.



DEPLOYMENT AND INTEGRATION

Leverage the power of your Security and Development Ecosystem

Depending on your needs, the 42Crunch API Security platform can be rapidly deployed on SaaS or on-premises. By offering a wide range of integrations with core design and runtime platforms, 42Crunch enables companies to easily and quickly implement their API security across the enterprise landscape.

Category	Product
IDE Design time API security	VSCode, Intellij, Eclipse
CI/CD Runtime API security configuration	GitHub Actions, Bitbucket, Visual Studio, Bamboo, Jenkins, Gitlab, Sonarqube, Tekton
API Gateway Enhance your API security	Azure, Google Apigee, Kong, Axway, WSO2
Runtime Containers Deployment flexibility	Kubernetes, Amazon ECS, Red Hat OpenShift
Security Incident & Event Management Simplify monitoring of API threats	Microsoft Azure Sentinel, Splunk

63% of C-Suite executives reported an API security breach in the last 12 months

Google Market Survey Report API Security: Latest Insights & Key Trends 2022

ABOUT 42CRUNCH

42Crunch enables a standardized approach to securing APIs that automates the enforcement of API security compliance across distributed development and security ecosystems. Our API security testing and protection services are used by Fortune 500 enterprises and over 1 million developers worldwide. The 42Crunch API security platform empowers developers to build security from the IDE into the API pipeline and gives application security teams control of security policy enforcement from the CI/CD across the entire API lifecycle. This seamless DevSecOps approach to API security reduces governance costs and accelerates the delivery of secure APIs.

OPENAPI INITIATIVE

ISO 27001

OWASP®

Member of Microsoft Intelligent Security Association

Microsoft