CASE STUDY

Enabled Global Telco

to Automate and Scale API Security Across Thousands of Endpoints

Overview of the Problem

This global telecommunications leader manages an extensive digital ecosystem comprising thousands of APIs that power its customer-facing services, internal systems, and partner integrations.

With the proliferation of APIs came a growing risk surface—threat actors increasingly targeting APIs with sophisticated attacks outlined in the OWASP API Security Top 10.

The telco's security and development teams faced three critical challenges:

- **Lack of API Security Governance** – APIs were developed and deployed across distributed teams in different timezones, often with inconsistent security controls and documentation, making it difficult to enforce security standards uniformly.
- **Manual and Siloed Processes** – Security reviews were often manual and time-consuming, slowing down DevOps pipelines and introducing bottlenecks.
- **Scalability of Protection** – Traditional perimeter-based defenses including web application firewalls, could not effectively scale or detect complex logic flaws, broken object-level authorization, or excessive data exposure in API endpoints.

With thousands of APIs to manage and increasingly rapid development cycles, the telco needed a solution that could automate and scale security enforcement without hindering innovation.

Industry:

Telecommunications

Key Impacts:

- Full security governance across 20,000 APIs
- 6,000 developers in globally distributed teams using platform
- Runtime threat protection for complete API inventory
- Seamless integration to existing SIEM

The Solution: 42Crunch API Security Platform

The telco adopted the 42Crunch API Security platform to embed security directly into its API development lifecycle and enforce consistent protections across all APIs—at scale.

Key components of the solution included:

- **Automated API Contract Security Testing** – 42Crunch integrated directly into the telco's software development lifecycle at the IDE and CI/CD pipelines, enabling automated OpenAPI contract analysis that scored APIs against OWASP API Top 10 vulnerabilities such as Broken Object Level Authorization (BOLA) and Mass Assignment. This testing provided instant feedback to developers and prevented insecure APIs from reaching production.
- **Centralized API Security Governance** – With a single-pane-of-glass view of the API security governance landscape, the telco's security teams could monitor the API risk posture, and security scores across business units. This visibility enabled the global enforcement of API security policies without micro-managing each team.
- **Runtime Protection at Scale** – 42Crunch's lightweight micro-API firewall provided context aware, schema-based protection against attacks like injection, data leaks, and denial-of-service at runtime—automatically generated from validated API definitions. This ensured APIs were protected in production without needing hand-written security rules.

> Securing telecom infrastructure comes with a set of functional requirements to support massive scale. Cybersecurity vendor 42Crunch is shown to effectively support these scaling requirements for API security in the context of telecom usage.
>
> **Dr. Edward Amoroso**
>
> Founder & CEO TAG,
> Former CISO AT&T

The Benefits

Implementing 42Crunch delivered measurable benefits:

- **Massive Scale, Reduced Overhead** – With over 20,000 APIs, manual security was no longer feasible. 42Crunch's automation enabled security to scale in lockstep with API growth, without increasing resource demands. Cost reduction was achieved for application security testing tasks engaged by red and blue teams.
- **Shift Left Security** – Over 6,000 developers in distributed teams, received immediate static and dynamic testing feedback within their IDEs and CI/CD pipelines, fixing issues earlier and reducing rework and vulnerabilities in production.
- **Reduced Risk of API Breaches** – By addressing the OWASP API Top 10 at both design-time and runtime, the telecomm's provider drastically reduced its API attack surface and improved compliance with internal and regulatory standards.
- **Corporate wide Compliance** - Compliance objectives were achieved via adoption of API standards and governance of all API-based services.
- **Faster Time-to-Market** – By automating reviews and enforcement, security no longer blocked releases. Teams could deliver faster with the confidence that APIs met corporate security benchmarks.

Conclusion

With 42Crunch, this global telecommunications company was able to transition from reactive, fragmented API security to a proactive, automated, and scalable model. The platform empowered both security and development teams to collaborate more effectively while addressing the unique risks posed by modern APIs—helping the company stay secure in an increasingly connected world.