CASE STUDY

Global Investment Bank

Scales API Security and Compliance with 42Crunch

Overview of the Problem

A global leader in investment banking and financial services relies heavily on APIs to power digital platforms, automate trading systems, enable partner integrations, and deliver real-time financial services. The rapid expansion of APIs—spanning internal teams, external partners, and mobile applications—created a sprawling and dynamic attack surface.

Security and development faced several interrelated challenges:

- **Rapid API Growth**: With thousands of APIs deployed across business units, manual security reviews could not keep pace with the development velocity.
- **Regulatory Pressure**: As a systemically important financial institution this bank is subject to strict regulatory compliance standards (e.g., SOX, FFIEC, NYDFS), requiring demonstrable control over data access and secure API design.
- **Fragmented Security Governance**: API security ownership was scattered across teams, making it difficult to enforce consistent controls and track adherence to corporate security policies.
- **OWASP API Top 10 Risks**: APIs were susceptible to common vulnerabilities like broken object-level authorization, excessive data exposure, and security misconfigurations—exacerbated by inconsistent documentation and lack of centralized testing.

The investment bank needed an enterprise-grade solution that could automate API security, enforce policy compliance, and scale protections across its entire API footprint—without slowing down development.

Industry:

Banking

Key Impacts:

- Scale API security governance across 200 developers and 1,000 APIs
- Automation of security scanning reducing costly manual intervention
- Assisted regulatory compliance with full API-based data protection

The Solution: 42Crunch API Security Platform

The 42Crunch API Security platform was selected to transform the bank's approach to API protection—from reactive and manual to automated, continuous, and policy-driven.

Key capabilities leveraged:

- **Automated API Security Audits**: 42Crunch integrated with IDE and CI/CD pipelines, performing real-time OpenAPI contract analysis to detect vulnerabilities like BOLA, injection flaws, and misconfigurations. This enabled developers to fix issues early and meet security requirements before deployment.
- **Security-as-Code Governance**: The bank used 42Crunch to define and enforce consistent security policies across thousands of APIs. Teams could codify requirements such as authentication methods, data exposure rules, and schema validation—ensuring every API adhered to organizational standards and regulatory mandates.
- **Runtime Protection at Scale**: Using 42Crunch's dynamic API firewall, the investment bank deployed schema-driven protection to production APIs, blocking malicious payloads and enforcing strict schema validation without requiring manual tuning or rules.
- **Centralized Visibility and Reporting**: The platform provided a unified dashboard for security and compliance teams to track API posture, audit activity, and demonstrate adherence to OWASP Top 10 and regulatory controls.

> Banks need to adapt to the new reality that any vulnerable API, flawed DevOp cycle, or malicious activity can result in a breach. Although many financial institutions are aware of the need for API security to support their new corporate reality, they do not really know how to approach it…
>
> Podcast with
>
> **Sandy Carielli**
>
> VP, Principal Analyst, Forrester

The Benefits

Some of the key transformative benefits derived from deploying 42Crunch include:

- **Scalable Security Automation**: Thousands of APIs were continuously audited and protected without increasing headcount or slowing delivery pipelines.
- **Compliance Confidence**: Security controls were demonstrable, auditable, and aligned with financial regulations, supporting both internal audit and external oversight requirements.
- **Shift Left Enablement**: Developers received early, actionable feedback within existing tools, reducing costly late-stage fixes and improving code quality.
- **Consistent Governance**: Security policies were codified and enforced enterprise-wide, reducing variability and ensuring every API met baseline controls.
- **Reduced Risk Exposure**: By proactively mitigating OWASP API Top 10 risks, the bank strengthened its defense against API-based attacks and data breaches.

Conclusion

By implementing 42Crunch this global investment bank successfully operationalized a secure-by-design API strategy. The platform allowed the firm to scale API security, automate compliance enforcement, and embed governance into every stage of the API lifecycle—all without compromising speed, agility, or innovation.