CASE STUDY

Leading Insurer

Automates API Security and Compliance Across Partner Ecosystem

Overview of the Problem

As one of the world's largest insurers, this company operates across a complex, globally distributed digital environment. APIs are at the core of the insurer's digital strategy—powering everything from customer portals and mobile apps to broker platforms and third-party integrations with banks and partners.

However, with this API-driven model came growing challenges for the insurance giant's security and development teams:

- **Complex Partner Ecosystem**: APIs were being consumed and integrated by a wide network of partners, brokers, and reinsurers—each with varying levels of security maturity and integration practices.
- **Regulatory Compliance Pressure**: Insurance companies operate under stringent regulatory oversight (GDPR, NAIC, COPPA, Solvency II, local data protection laws), requiring strict access controls, data minimization, and auditability across all systems—including third-party-exposed APIs.
- **Manual and Fragmented API Security**: Traditional perimeter security controls weren't sufficient for API-specific threats. Security reviews and governance enforcement were mostly manual, difficult to scale, and inconsistently applied across development teams and external integrations.
- **Exposure to OWASP API Top 10 Risks**: Without centralized control, APIs were exposed to common threats such as Broken Object Level Authorization (BOLA), Excessive Data Exposure, Security Misconfigurations, and Improper Asset Management.

The insurer needed a solution that could **automate API security** across the entire lifecycle, **enforce governance policies**, and ensure **regulatory compliance across internal and external teams**—without slowing innovation or partner onboarding.

Industry:

Insurance

Key Impacts:

- **API Governance across team of 700 Developers**
- **Proactive security enforcement for 1300 APIs**
- **API lifecycle risk & compliance management**

The Solution: 42Crunch API Security Platform

The insurer implemented the 42Crunch API Security Platform to automate API security enforcement across its global insurance ecosystem.

Key components of the solution included:

- **Security-by-Design**: 42Crunch integrated into the CI/CD pipelines and developer IDE toolchains, enabling automated OpenAPI contract scans. This identified vulnerabilities related to the OWASP API Top 10 before APIs were released—allowing developers to fix issues early and consistently.
- **Policy-Driven Governance**: The Insurer used 42Crunch's policy-as-code capabilities to define strict, standardized API security requirements—such as authentication schemes, data exposure limits, and schema validation rules. These policies were automatically enforced across all business units and external partners.
- **Runtime API Protection**: Using 42Crunch's micro API firewall, the insurer deployed dynamic security protections in production, blocking malformed requests and unauthorized access attempts—without requiring manual rule-writing or maintenance.
- **Visibility and Compliance Reporting**: The platform provided centralized dashboards and audit trails, giving the compliance and security teams complete visibility into API security posture, policy violations, and regulatory readiness.

> Insurance CIOs who intend to exploit the potential of open APIs must adopt a continuous approach to API security.
>
> **Gartner Report: 5 Best Practices for Insurance CIOs**

The Benefits

By adopting 42Crunch, the insurance company achieved significant improvements in security, governance, and regulatory compliance:

- **End-to-End Automation**: API security checks were embedded into the development process, drastically reducing manual effort and speeding time-to-market.
- **Enforced Governance at Scale**: Consistent security policies were applied across thousands of APIs, regardless of whether they were internal or integrated via partners and brokers.
- **Improved Regulatory Readiness**: Audit logs, risk scoring, and policy enforcement helped meet GDPR, Solvency II, and other data protection mandates with confidence.
- **Stronger Ecosystem Security**: APIs consumed by brokers and partners were protected by uniform controls, reducing risk across the extended enterprise.
- **Reduced API Risk Exposure**: With OWASP API Top 10 threats proactively mitigated, improved its cyber resilience while maintaining agility in a fast-paced industry.

Conclusion

With 42Crunch, this insurance company successfully implemented a secure-by-design, compliant-by-default API security model—enabling innovation and ecosystem connectivity without compromising on security, regulatory or governance frameworks.