



APIs In The Technology Industry



Solution Brief



Industry Overview

APIs play a significant role in technology companies and their products. Customers use APIs almost every time they use an app like Facebook, Google, or Amazon, to send an instant message, or check the weather on their phones. Furthermore, major tech companies such as Google, Amazon, and Twitter offer their own APIs to accelerate product development. But the risks are equally significant.

Risks

API calls are used in practically every line of code. They help programmers construct their products faster and more efficiently, enabling flexibility and simplifying design. However, the increased use of APIs has resulted in a significantly expanded attack surface as there are many entry points to an organization's network.

Many risks have ensued, including:

- Data extraction through breaches in the API system
- Impacted performance of the API server, resulting in DoS
- Fraudulent usage of users' data

Full Lifecycle Overview

APIs undergo a constant cycle of creation and updates. The best way to protect them is by establishing an iterative feedback loop between each stage, to secure the APIs across their entire lifecycle. You need an API Security solution that provides a suite of integrated tools to easily secure your entire API lifecycle, through development, testing, and production.

Our Solution

Technology firms' API-driven development models can increase penetration risks if controls do not keep pace with change. A feedback loop between every stage of the SDLC can help to ensure protection at production and continuously improve security by removing vulnerabilities in code.

The process of overseeing an API's whole life cycle, from planning through retirement, serves as a foundation for digital strategy, ecosystem development, and API management. Your API requires a full lifecycle security solution.

Wib offers a full lifecycle protection for your APIs.

- Development stage: We support API code analysis to analyze APIs and client code to detect API threats and vulnerabilities as soon as possible.
- Testing stage: We offer an API attack simulator to test and improve your APIs, protect them from threats, and fix vulnerabilities by simulating API attacks before they go live.
- Production stage: We include API message inspection capabilities and an API compliance defender.
 - API Message Inspection analyzes each API call to establish a baseline of usual behavior and detect any activity that deviates from it.
 - API Compliance Defender identifies and solves compliance breaches and security issues through in real time.