wib

APIs in the E-commerce Industry

Solution Brief

Overview

To build a solid foundation for your E-commerce firm, you need to use APIs for much of your business, including your shipping and logistics. E-commerce fulfillment APIs can help organizations automate, coordinate, manage, and streamline their operations with features including order fulfillment, courier management, invoicing, tracking, and confirmation alerts. But the risks are equally significant.

Risks

API calls are an element of 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 APIs across their entire lifecycle. Therefore, 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

E-commerce models can increase penetration risks if controls do not keep pace with change. A feedback loop between every Software Development Lifecycle (SDLC) stage can help 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. Therefore, your API requires a complete lifecycle security solution across development, testing, and production as well.

Wib offers 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 in real-time.