

? Why API Security?

In recent years, business has changed and companies have been forced to increase their speed of delivery and changes to their applications. This resulted in **change of application architecture** – from monolithic (slow, complex to upgrade) to microservice-based architectures. Microservice-based architecture **changed the attack surface** and security needs adapt accordingly. Attackers are aware of this and are attacking the new architecture, while defenders are struggling to keep up.

“Gartner predicts 2022” stated that **API attacks are the #1 attack vector**, and at Wib we believe ‘Your Defense Should be Informed By The Offense. If you don’t have an API security program, you aren’t defending against the #1 attack vector today.

Full Lifecycle API Security Platform

The only way to fully secure your APIs is to **protect APIs throughout the entire software development lifecycle**. Some vulnerabilities can only be identified at the code level, some can be caught by testing with smart simulations, and others can only be discovered by monitoring APIs in real time, setting a baseline of expected behaviour and detecting anomalies.

Wib’s platform works in synergy, to provide **feedback loop throughout the lifecycle** ensuring a constantly improving API security model.

