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.

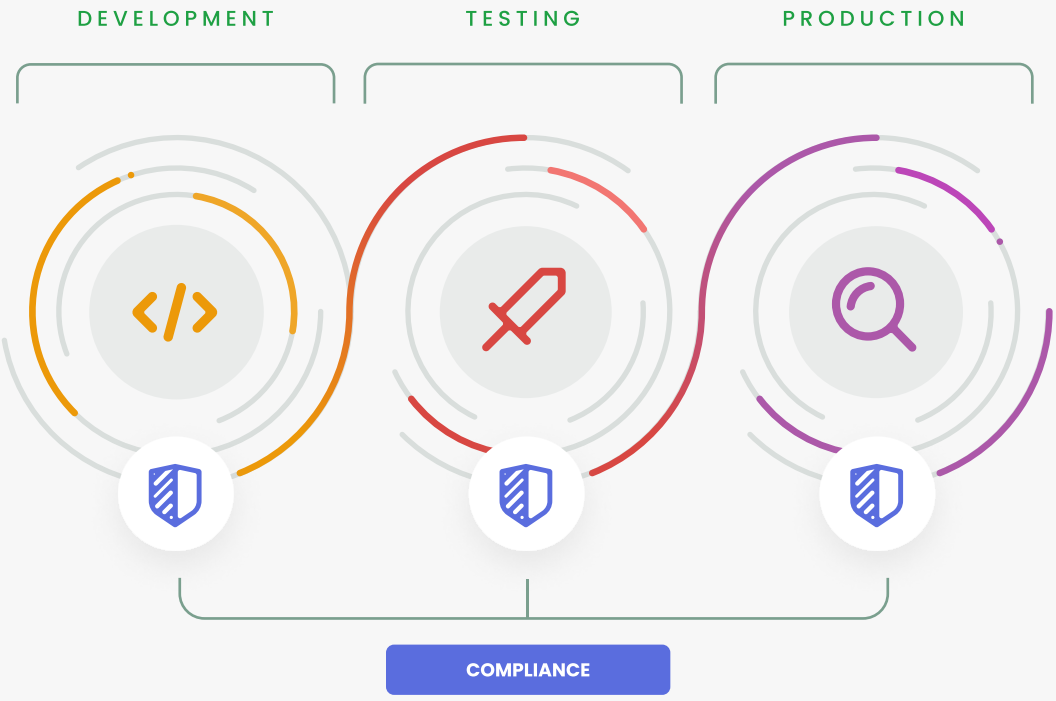
Microservice-based architeture changed the attack surface and security needs adapt accordingly. Attackers are aware of this and are attacking the new architecture, while defenders are struggling to keep up.

“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 iterative feedback throughout the lifecycle ensuring a constantly improving API security model.



Wib's full lifecycle API security platform enables you to safely accelerate your business by discovering blindspots, identifying and remediating vulnerabilities and blocking API attacks - from development to production.

Key Capabilities

Eliminate Blindspots

Categorize API information:

- Inventory APIs
- Internet/External
- Shadow and Zombie APIs
- Authentication methods
- Automatic documentation
- Dynamic API Profiling
- Business Impact
- API Risk Management
- Compliance Frameworks
- Data Flows

Threat Analysis

Automated AI-based detection:

- Data Leaks
- Malicious Activity
- Misconfigurations
- API Versioning
- Data Policy Violations
- OWASP API Top 10/CVEs
- Context-based vulnerabilities
- Establish a baseline for each API
- Compile API activity into an attacker timeline

Remediate

Stop attacks and fix vulnerabilities in real-time:

- Suggest remediation to remove found vulnerability
- Actionable Insights
- Remediation ownership
- Remediation Feedback Loop
- Integrate with daily workflows (ticketing, SIEMs, etc)

Logic Testing

Active API testing in pre-production and production environments:

- Continusly run smart attacks to identify issues
- Execute thousands of API attack variants.
- Validate found issues.
- Test OWASP API Top 10 business logic.
- Integrate into existing CI/CD pipelines.
- On-demand deployment.