

Wib Fusion Platform

Holistic API security across code,
testing and production.

The Wib API Security Platform is a comprehensive, holistic solution for securing APIs across an organization's entire ecosystem. It utilizes a comprehensive, multi-lens approach, powered by Wib's proprietary Fusion Engine, to assess the security posture of APIs, minimize risk, and quickly address cybersecurity incidents throughout the entire development process - from code to testing and production - further enabling incident response and vulnerability management via the Wib Security Center.

Why is API security important?

Microservice architectures are becoming increasingly popular as organizations undergo digital transformation and move away from monolithic systems. Such architectures rely on APIs to enable communication and data exchange, making them a common target for cyberattack. If not properly defended, APIs can expose the organization's assets and flows to potential "logic attacks", which manipulate the intended functionality of the API itself to gain unauthorized access to company resources. Traditional application security tools are insufficient against these types of attacks, unable to understand the underlying logic of an application, leaving existing security programs completely blind to the API attack surface.



Wib Fusion Engine

A multi-lens approach

At the heart of the Wib API Security Platform is the Fusion Engine, which unifies all the data generated by the core traffic, code analysis and testing engines into a single source of truth for an automatically updated API Inventory, leveraging this data to create security insights using a multi-lens approach. Through this approach, the Wib API Security Platform is uniquely equipped to optimize defense against API logic attacks, where traditional rule base detection will fail.

What are API logic attacks?

API logic attacks differ from traditional cyberattacks focused on technical vulnerabilities, as they specifically target the intended functionality of the API itself – specifically the logic through which APIs process activities. API logic attacks aim to exploit the capabilities and features of APIs to gain unauthorized access to sensitive information/systems, disrupt operations or steal valuable resources. This may involve manipulation of input parameters, tampering with back-end systems, bypassing security controls and other tactics. It's important for organizations to be aware of these types of attacks and take steps to protect their APIs and systems.

The traffic engine collects customer API traffic, identifies APIs, hostnames, and API endpoints, and detects security incidents – all in real time. It enables multiple types of traffic collection, depending on the organization's network architecture, such as:

- Traffic mirroring (AWS/Azure)
- Agent-based (Windows/Linux)
- Wasm or Plugin (Gloo Edge/Istio/NGINX)
- Sidecar (K8s)
- Dedicated API gateway (Envoy)

The code analysis engine uses static code analysis to scan customer repositories and detect API endpoints and logic vulnerabilities. It directly integrates with source code management (SCM) providers such as GitHub, Bitbucket and GitLab and supports the following programming languages and frameworks:

Language	Frameworks/Libraries
Java	Spring 3/4/5/Boot, JavaEE, JAX-RS
C#	.NET core 3.1 -> 6 (any version in between)
OAS (Swagger/OpenAPI), RAML	

The crawler serves as an independent data source, providing insights on APIs that may not be visible through other means. The crawler provides detection of the following:

- Web applications and their APIs.
- Domains and sub-domains.
- Verified Shadow APIs that are not found in the source code or gateways.
- Third-party APIs consumed by web applications.
- External APIs.
- Sensitive data that is internet facing.

The testing engine is used to validate vulnerabilities that have been found, and the fixes that have been implemented to remediate or patch them.

Wib Fusion Discovery

Automated API inventory continuously updated in real-time

Automation virtually eliminates the time it takes for developers to write and maintain API documentation by autonomously updating content and simplifying some tasks. Wib API Inventory also brings consistency to documentation to provide a similar user experience for all APIs, while security teams get the necessary visibility and 'single source of truth' of the API estate, so they know what they need to secure.

The API estate inventory is a complete inventory of an organization's APIs, along with their associated Open API specification.

- Full endpoint schema including URL, query, header, and body parameters.
- Endpoint schema responses.
- Detection of sensitive data.

The risk scorecard determines the risk level of each API by evaluating the likelihood and impact of an attack.

Likelihood parameters include:	Impact parameters include:
What is the authentication and encryption strength?	What kind and amount of sensitive data detected?
Are there any HTTP methods restrictions?	What is the business context of the endpoint?
Has an authorization mechanism been implemented?	Do the endpoints have DB accessibility?
Has rate limiting been implemented?	
What is the endpoint issues state?	
Were any anomalies detected on the EP?	
What is the endpoint direction (external/internal)?	

API snapshots allow SecOps teams to investigate security incidents and vulnerabilities detected by evaluating APIs at their development stage by:

- Detecting any API code changes
- Tracking commits history
- Determining API ownership.

Wib Fusion Defense



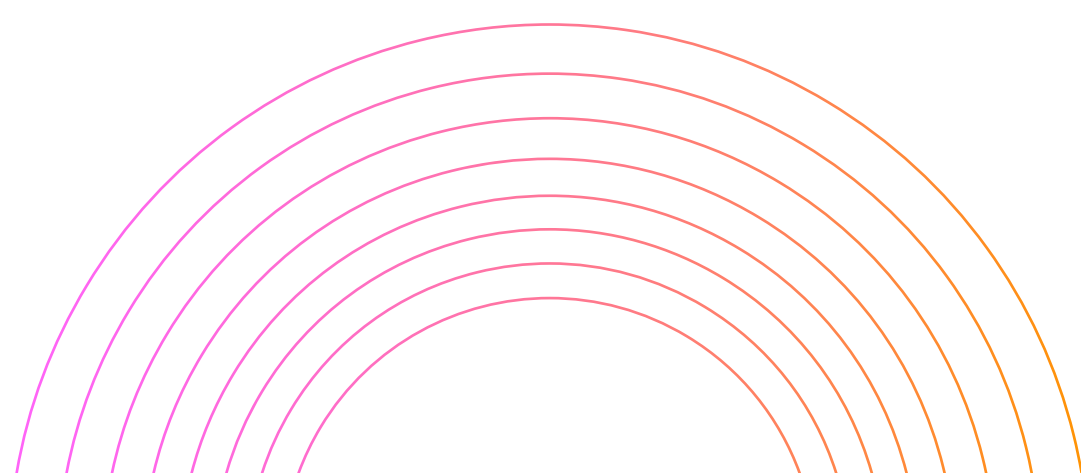
Comprehensive management of end-to-end API security

Fusion Defense, the security layer of the platform includes features for incident response, vulnerability management, and WAF rule creation, all designed to help organizations protect their APIs from potential threats.

Manage and respond to API security incidents.

- Incident detection by actor, path or general target.
- Affected assets and business impact.
- Complete forensics including incident/event timeline and call activity.
- Immediate response mitigation with recommended blocking rule creation.
- Incident validation (using the API testing engine).
- Related vulnerabilities (if a known vulnerability was exploited).
- Blocking performance.

Manage and remediate API vulnerabilities.

- Detection of OWASP API Security Top 10.
 - Detection by path/vulnerability type.
 - Virtual patching via WAF.
 - Vulnerability validation (using the API testing engine).
 - Related incidents.
 - Patching performance.
 - Ticket-based tracking – to track remediation progress and recovery.
 - Validation fix (using the API testing engine to test if a fix was implemented).
- 

Platform Deployment and Integration

Seamless, flexible, best practice

The Wib API Security Platform can be rapidly deployed on SaaS or on-premises, depending on the organization's needs and compliance requirements, and integrates seamlessly with existing security workflows (including the following) to incorporate into existing security processes and systems.

- Notification services: Email, Slack.
- SIEM systems: QRadar, Splunk.
- Ticketing providers: Jira, Monday.
- Vulnerability management: Rapid7.
- Web application firewalls: Imperva, Akamai, F5.
- Traffic management solutions: Envoy, Gloo Edge, Istio, Kong, NGINX.

Gartner guidelines

Wib API Security Platform follows Gartner guidelines for API protection, including API visibility, posture management, runtime protection, and API pen testing. By utilizing this comprehensive approach, organizations can effectively defend against API-based attacks and protect their critical assets.

Wib's API Penetration Testing as a Service

TPCI has released updated guidance concerning API security, both in version 4.0 of the new PCI Data Security Standards (DSS), where both controls and testing are required to cover APIs and attacks on business logic (sections 6.2.4, 6.4.1, and 11.4). In addition their new secure software standard (section 2.1) just released in December 2022 lays out specific language around API security.

Wib's industry's first API Penetration Testing as a Service program specifically designed to cover both:

FFIEC (2021) and PCI DSS (2022) requirements for API security.