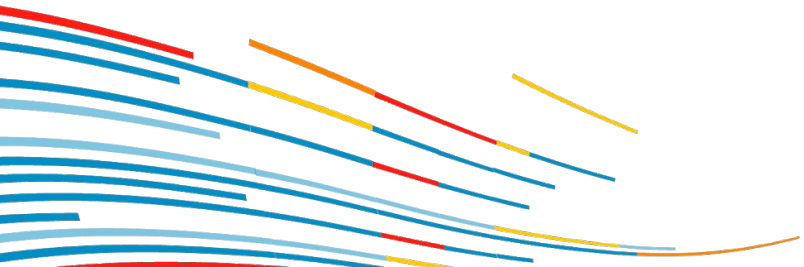
IMVISION

How enterprises secure their APIs

The only platform to protect your APIs across the entire lifecycle (even the ones you don't know about).

Imvision API Security Platform enables you to proactively get ahead of the growing challenges of APIs with automated protections across the lifecycle, at any scale.

By analyzing the unique API dialogue to learn the application's behavior, Imvision helps security teams go beyond rules and find unknown vulnerabilities, prevent functional attacks, and automatically shift-left to simulate attacks that outsmart attackers.



Ford

As a leading automotive company, **Ford Motor Company** uses APIs extensively to enable new client experiences, while improving collaboration with its network of integrated business partners.

Partnering with Imvision, Ford was able to enhance protection of sensitive client data and key functionalities across their infrastructure.

Raiffeisen Bank International

As an international banking group, **Raiffeisen Bank International** is continuously investing in API development to enable digital experiences and to meet Open Banking standards.

Partnering with Imvision, RBI was able to gain visibility into its APIs and accelerate API security maturity while complying with regulations.

NTT docomo

As the prominent mobile operator in Japan, **NTT Docomo** manages an extensive international network of business partners, generating more than 20 billion monthly transactions.

Partnering with Imvision, NTT Docomo was able to extend enforcement at scale, improving service while keeping service disruptions to a minimum

IMVISION

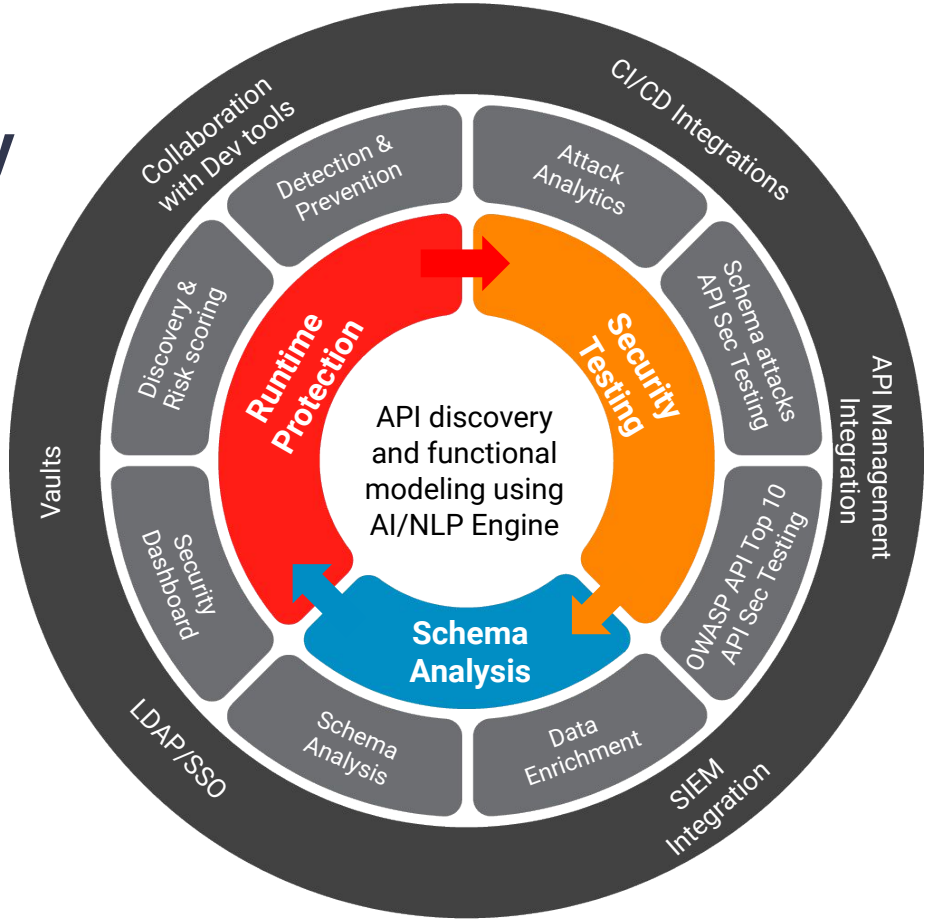
“Runtime to Code” API Security

The ideal shift-left platform to protect your APIs

Deep functional modelling
Uncover the API functionality using NLP-based AI to model complex data relations.

Accelerate remediation
Understand anomalies faster and in the context of the business logic.

<0.001% false positives
Detect behavior sequences attempting to manipulate the logic - at any scale.



Context-aware protection ● Easy to deploy & scale ● Data-driven visibility

IMVISION

Why enterprises choose Imvision

Context-aware protection based on the API functionality	Minimize falses using NLP for 'Meaningful Anomaly' detection	Proactive security from production back to code
IMVISION	IMVISION	IMVISION
Users are protected from API abuse through data-driven modeling of the API's business logic, including mapping user behavior patterns, flow, and complex data relationships.	Users can avoid false positives by focusing on meaningful anomalies, the specific behavior sequences that attempt to intentionally manipulate the API business logic.	Based on the learned logic, security teams can shift-left to simulate attacks and outsmart attackers, going beyond rules and known signatures to find unknown vulnerabilities.
Other API security platforms	**Other API security platforms**	**Other API security platforms**
Focus on monitoring the API traffic and user behavior.	Use a statistical approach to establish traffic baselines and detect anomalies.	Provide protections only during runtime, not

IMVISION

Imvision vs. other API security solutions

	IMVISION	Other API security platforms
Automated API discovery	✓	✓
PI/PII and sensitive data detection	✓	✓
Runtime anomaly detection	✓	✓
Agentless deployment, on-prem or cloud	✓	✓
Context-aware detection	✓	✓
User behavior analysis	✓	✓
Adaptive endpoint-level risk scoring	✓	✗
Attack analytics and incident classification	✓	✗
Automated remediation recommendations	✓	✗
Business Logic Automated Security Testing	✓	✗
Schema analysis and enforcement	✓	✗
Auto/semi-automatic runtime prevention	✓	✗