IMVISION

Extending from your API Gateway to Full Lifecycle API Security

Enhance API visibility, protection and remediation

Most enterprises today manage APIs and integrations using one or more API Management (APIM) platforms. These platforms commonly provide some security features through the API Gateway, such as authentication, access control, throttling and custom policies. While these are important protections, they are not enough to protect APIs - especially those you don't know about. The Imvision platform can integrate with your APIM platform to enhance API visibility, protection and remediation:

Visibility: Gain visibility across the board and deeply understand the business logic behind your APIs:

- API traffic analysis auto-inventories all endpoints, and methods - even those not in the APIM platform.
- Automatic detection and classification of PII and sensitive data exposure.
- Scan endpoints for dormant APIs using advanced fuzzing techniques.
- Learn the API's unique business logic and functionality using NLP-based algorithms.
- Model complex data relationships, consumer behaviors, flows, and usage patterns.
- Granular risk scoring of endpoints based on API characteristics, sensitive data, severity, and anomalies.

Protection: Embed dedicated security controls through the API lifecycle and protect the business logic:

- Use NLP to detect only 'meaningful anomalies', resulting in a false-positive rate of <0.0001%.
- Expand detection to cover OWASP API Top-10 and API abuses/business logic attacks.
- Simulate business logic attacks based on the behavior models learned during runtime.
- Identify security issues during development by analyzing the API specification for flaws.
- Verify API schema matches actual development and surface discrepancies.

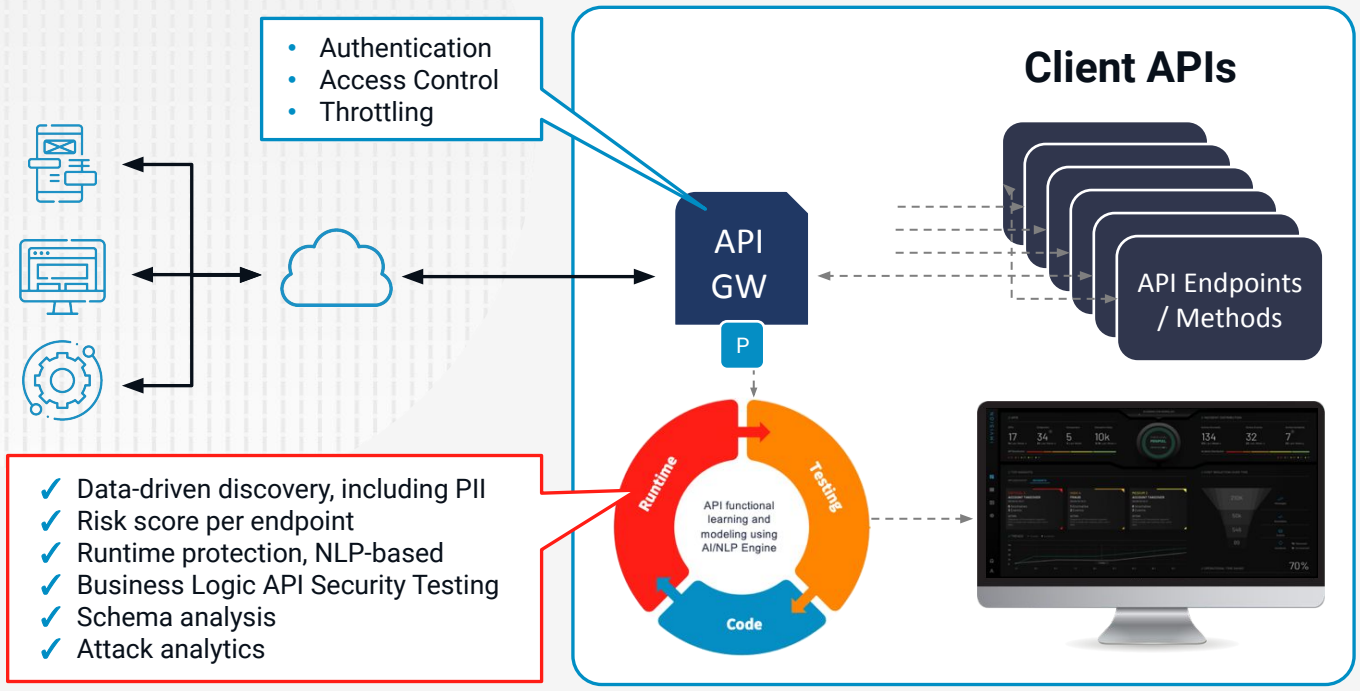
Remediation: Enhance API security posture and reduce risk by prioritizing and accelerating remediation:

- Reduce analyst workload and accelerate remediation through dedicated attack analytics.
- Automated clustering and classifying of anomalies according to common attack vectors.
- Gain detailed remediation recommendations using NLP-based algorithms.
- Provide developers with full forensic support to investigate, reproduce and fix flaws.

Seamless Integration: Deploy once, secure always

Dedicated OOTB plugins connect to your API data across all your cloud services, no agents or network configurations are required. Imvision seamlessly connects with the leading API gateways, load balancers, sidecars, reverse proxies, span ports – whatever it takes to integrate with your existing architecture.

	Inventory of APIs, endpoints and methods	Automatic detection of PII and sensitive data	Granular risk scoring of API endpoints
API Discovery	API Gateway		
	Imvision		
	Authentication, access control and rate-limiting	OWASP API-10 and API business logic abuses	Meaningful anomaly detection, <0.0001% FPs
Runtime Protection	API Gateway		
	Imvision		
	Analyze the API schema for flaws during design	Verify API specification matches development	Simulate business logic attacks automatically
Security Testing	API Gateway		
	Imvision		
	Detect anomalies in API transactions data	Automated clustering of anomalies by incidents	Get detailed remediation recommendations
Attack Analytics	API Gateway		
	Imvision		



IMVISION

For more information or to schedule a demo:
www.imvision.ai | info@imvision.ai | Follow us on