IMVISION

Holistic API Security Platform

Automatically discover, test, and protect your APIs and sensitive data.

No coding, network configuration, or documentation needed.

Securing APIs is a daunting responsibility. APIs are spreading like wildfire across organizations: running on multiple clouds, developed by different teams, serving more and more consumers. APIs promise many benefits, but at the same time, many companies struggle to develop secure APIs.

Since each API is different, it is not sufficient to protect them using policies or tests based on known vulnerabilities. More and more functional attacks are being executed, such that target the specific functionality of an API, exploiting its unique business logic vulnerabilities. APIs are becoming the most frequent attack vector, while existing security solutions and API gateways remain insufficient.

Imvision helps security leaders to scale up their API security. Forget about poorly documented APIs, endless security configurations and lack of security awareness across the organization. Using Imvision's API Security Platform, security leaders can easily protect all their APIs, without falling behind development cycles or leaving exposed vulnerabilities to chance.

Trusted by

Ford · Raiffeisen BANK · 浦发银行 SPD BANK · NTT docomo

The ultimate API security advantage

Full Visibility

Poor visibility invites security breaches. Imvision provides you with the visibility you need to improve your API security posture and align teams, by discovering all APIs and mapping behaviors and flows across your endpoints. Keep track of sensitive data and rogue APIs, and gain a deep understanding of your consumers. Bye-bye blind spots!

Context-Aware Protection

Analyst fatigue is not a myth. Imvision helps you make sure your team remains razor-sharp and focused on what really matters, using behavior modeling to detect and prevent breaches automatically, while keeping false positives to a minimum through continuous learning and reinforcing model decisions. Stay fresh and alert.

Swift Remediation

Ultimately, API vulnerabilities are bugs. Imvision supports developers and security analysts in quickly drilling down into security incidents, reviewing relevant logs, identifying root causes, reproducing bugs, and getting a detailed recommendation of what needs to be fixed. Remediate more, investigate less.

Proactive Testing

The best defense is a good offense. Imvision makes it easy to take a proactive approach to security when it comes to APIs, by automating vulnerability testing based on learned logic. Test as frequently as needed to keep up with the API development cycle and business demands. Open up only when you are secure.

Easy Deployment

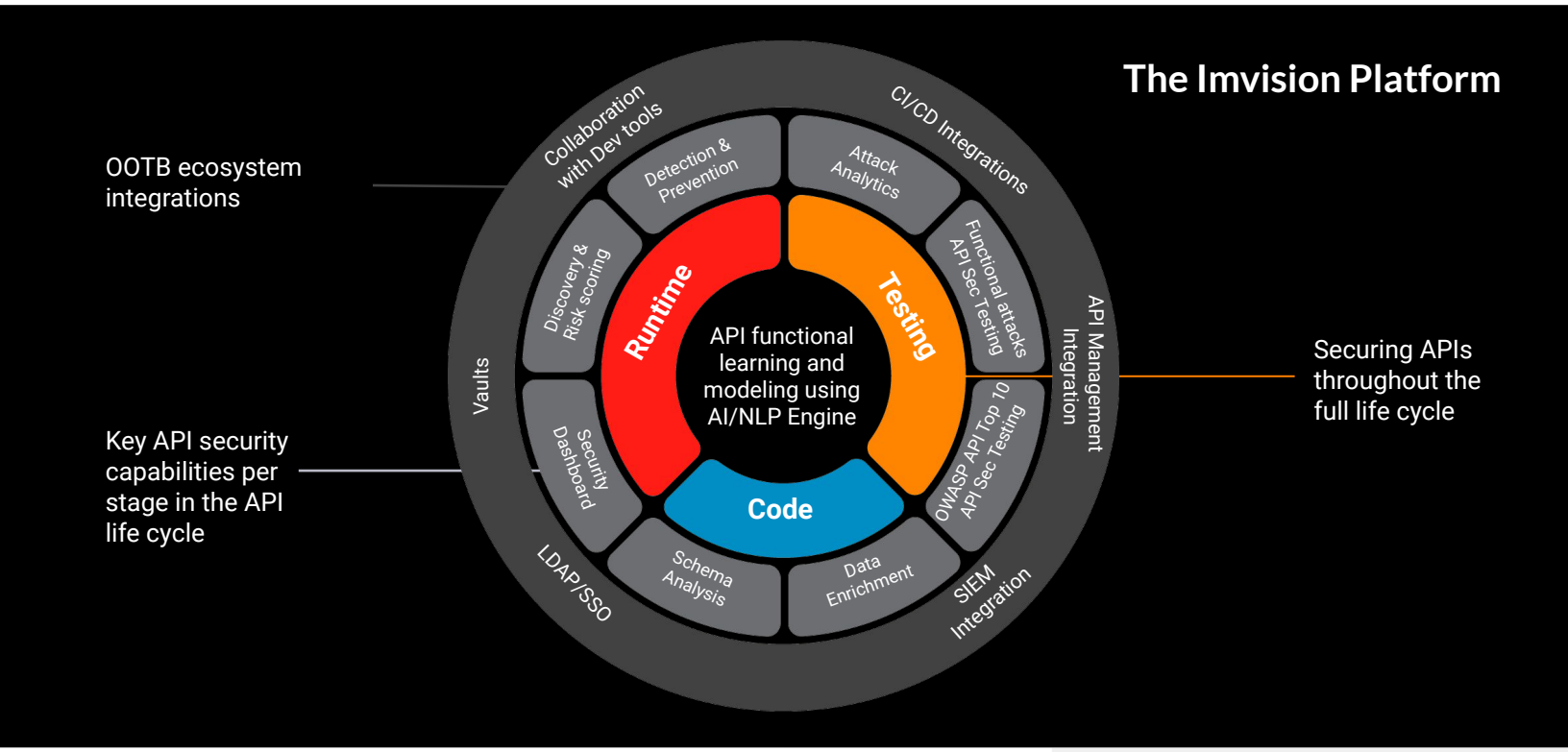
Forget about agents or network changes. Imvision's platform is locally installed on your network using a wide range of plugins. The platform runs a set of docker containers orchestrated by Kubernetes, allowing for service scalability and ease of onboarding. And don't worry - the data never leaves your network.

"By 2022, API abuses will move from an infrequent to the most-frequent attack vector"

Gartner

A holistic approach to API security

Proactively get ahead of the growing challenges of APIs with automated protections at all stages of the API lifecycle. Imvision's API Security Platform supports all cloud infrastructures and platforms, uses advanced NLP-based algorithms to preserve high level of accuracy for detection and prevention at scale, and generates the visibility needed to raise organization-wide awareness to API security.



Data-driven discovery, PI/PII detection & risk scoring

Gain full visibility into all internal and external APIs, uncovering methods and endpoints that expose sensitive data, analyzing consumer patterns, and continuously calculating endpoint risk.

The risk is calculated based on API characteristics, detected anomalies, and severity level, allowing security analysts to prioritize endpoints based on their individual business risk level.

API specifications analysis & attack simulation testing

Proactively identify potential vulnerabilities and accelerate secure development by analyzing the API specification for security issues and by generating simulated attacks based on the business logic. The platform uses learned behavioral models to automatically test beyond the schema and provide developers with full forensic support to reproduce and fix flaws.

Natural Language Processing (NLP) based analysis of API data

- ✓ < 0.001% false positives rate
- ✓ Automatic sensitive data detection
- ✓ Detect meaningful anomalies in the context of the business logic

Out of the box integration with all the platforms and tools you love

- ✓ Dev CI/CD pipeline tools
- ✓ Security team analysis tools
- ✓ Cloud service platforms
- ✓ API management software

Runtime anomaly detection & auto-prevention

The platform discovers and learns every API's unique complex relationships of data objects to monitor, detect, alert, and block abnormal behaviors that impact the API business logic.

The behavior modeling uses NLP to detect meaningful anomalies and minimize false-positives, allowing security professionals to focus on what really matters and reduce analyst fatigue.

Attack analytics & mitigation recommendations

Self-explanatory descriptions of malicious actions are automatically generated by aggregating and classifying anomalies into incidents matching common attack types. The attack analytics enable rapid and effective countermeasures, highlighting insights for the different teams - Executive team, security analysts and developers - delivering remediation recommendations and reporting.

Full compliance and protection against the OWASP API Top-10

- ✓ Broken Object Level Authorization
- ✓ Broken User Authentication
- ✓ Excessive Data Exposure
- ✓ Lack of Resources & Rate Limiting
- ✓ Broken Function Level Authorization
- ✓ Mass Assignment
- ✓ Security Misconfiguration
- ✓ Injection
- ✓ Improper Assets Management
- ✓ Insufficient Logging & Monitoring

Imvision API security

With Imvision, enterprises can accelerate their digital transformation by making sure that every API is individually protected and every API call is scrutinized – no matter how many there are. That means that every interaction between people, businesses, and machines can be trusted.

Imvision's platform detects breaches by analyzing each API's unique dialogue, understanding the application's behavior, and modeling complex relationships within the data. This allows it to highlight business logic issues so that they can be corrected before breaches take place.