IMVISION TECHNOLOGIES

Protect Your Business Against API Threats

The next big wave of Cyber-Attacks are targeting APIs resulting in Data breaches, Account Takeovers and Fraud

Gartner *"By 2022, **API abuses** will move from an infrequent to the **most-frequent attack vector**, resulting in data breaches"*

API Gateway

WAF

xSAT

Gartner *"Protecting web APIs with **general purpose application security** solutions alone continues to be ineffective"*

ImVision's API Anomaly Management Platform (AMP) is a Cutting Edge AI-based "API-Specific" Security solution

AMP analyzes API calls and self learns the business logic through patented AI-powered Natural Language Processing (NLP) technology, then detects anomalies and blocks attacks.

Security values

- ✓ Data driven API discovery & risk scoring
- ✓ Protects against sophisticated API business logic and business process attacks
- ✓ Early detection and prevention - before any damage occurs
- ✓ Self explanatory dashboard with easy to understand explanations

Operational values

- ✓ Full automation – zero human tuning
- ✓ 0.0001% False Positive Rate
- ✓ Automatic prevention

Utilizing NLP to uncover API's business logic

Natural Language based text is strongly characterized by structural features, for example: a word's meaning is highly dependent on its neighboring words, preceding sentences can affect the meaning of the current sentence.
APIs show similar attributes to natural language based text :

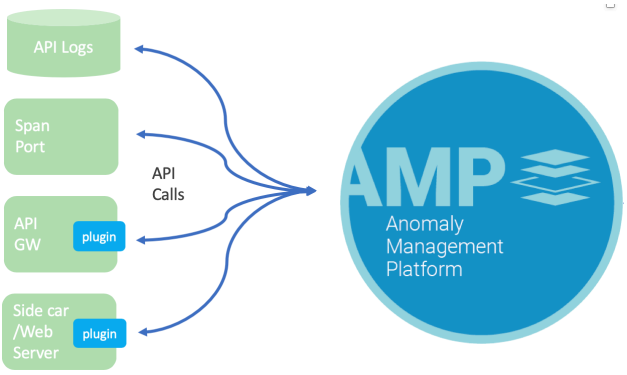
- API data is structured in layers of hierarchy, and there are dependencies between the elements in different layers of the hierarchy
- API calls are sequential in nature, and there are dependencies between elements in the sequence
- API uses vocabulary from a human language (e.g. English) and syntax from API type (e.g. REST/JSON)

imVision leverages 1000s of man-years invested in research of NLP for analysis of the API language and usage patterns to achieve:

- Automatic learning of API functional usage pattern
- Meaning inference from API call/call flow to model the API business logics
- Automatic detection of anomalies that impact application functionality

Seamless integration into the service

Using a wide-set of plugins, API AMP integrates seamlessly into any service architecture, regardless of API architecture (centralized or distributed), API use-case (internal or external) and the API GW



imVision is a market leader in API security solutions, its API Anomaly Management Platform (AAMP) is commercially deployed worldwide, including Fortune Global 500 customers, analyzing 10B API calls per month, 700+ B2B 3rd party partners for over 100m end users.

The inherent lack of API security and their proprietary nature makes them a prime target for the next big wave of cyber attacks. The Open Web Application Security Project (OWASP) defines a dedicated Top 10 for API Security threats, where the majority of API threats are caused by logical failures at the application layer

imVision enables service providers to protect their operations against API-driven attack such as data breaches, account takeover, fraud and application level denial of service.

imVision's patented technology uses automated learning of the "API Language" to build in-depth, granular behavioral models of data content, context and business logic and enforce them in real time. The Anomaly Management Platform (AMP) identifies and reacts to suspicious behavior on APIs, providing a unique advantage in mitigating attacks on APIs.