ApiFort

Safeguarding Connections, Securing Futures:
APIFORT is Your API Security Solution

Sales Overview

1. APIs & API Security
2. Market Details
3. What is APIFORT?
4. APIFORT’s Key Features
5. What is inside APIFORT?

Introduction to APIs and API Security

APIs (Application Programming Interfaces) serve as the bridge between different software applications, allowing them to communicate and interact with each other.

API security refers to the practices, measures, and technologies implemented to protect APIs from unauthorized access, data breaches, and other security threats.

5 Major API Incidents in 2025

- **DeepSeek**: A misconfigured backend API exposed over 1 million chat records and API keys.
- **Volkswagen Connected Services**: A Broken Object Level Authorization (BOLA) vulnerability allowed users to access data from vehicles they did not own.
- **Salesloft – Drift**: Stolen OAuth credentials were abused through Salesloft APIs to access Salesforce customer data.
- **McHire (McDonald's)**: Weak administrative access controls and IDOR vulnerabilities led to the exposure of job applicant data.
- **HPE OneView**: An unauthenticated REST API vulnerability enabled remote code execution (RCE) and was added to CISA's list of actively exploited vulnerabilities.

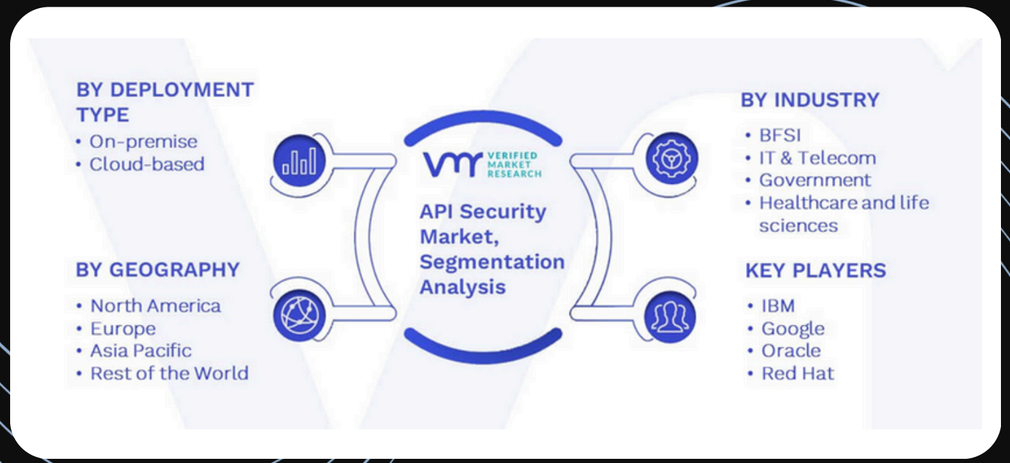
Market Research

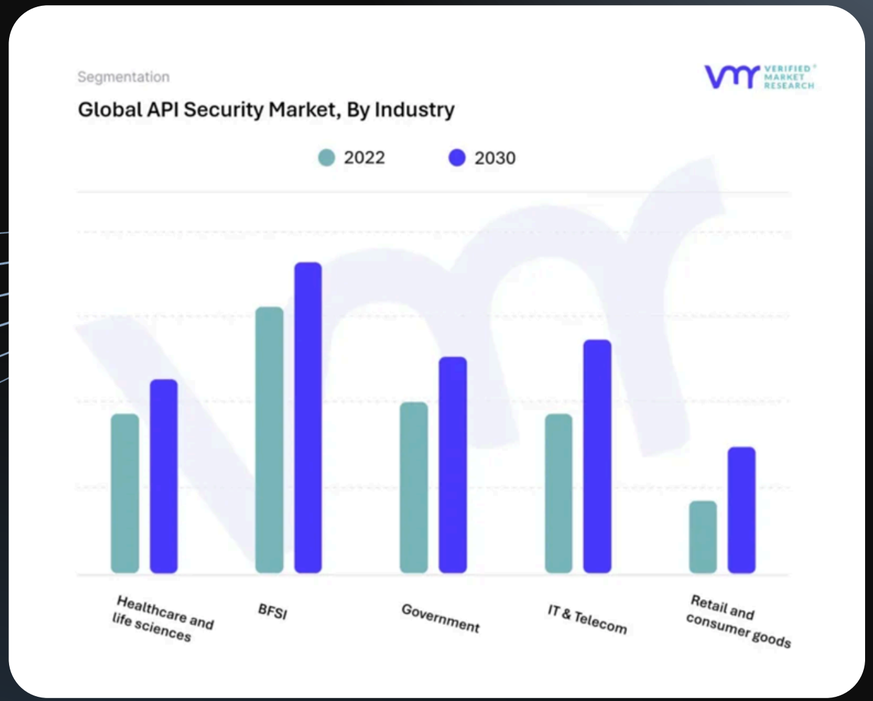
According to Virtue Market Research, The Global API Security Market was valued at USD 30.59 Billion.

It is expected to reach a market size of USD 47.85 Billion by the end of 2030.

The market is projected to grow at a CAGR of 6.6% during the forecast period 2024-2030.

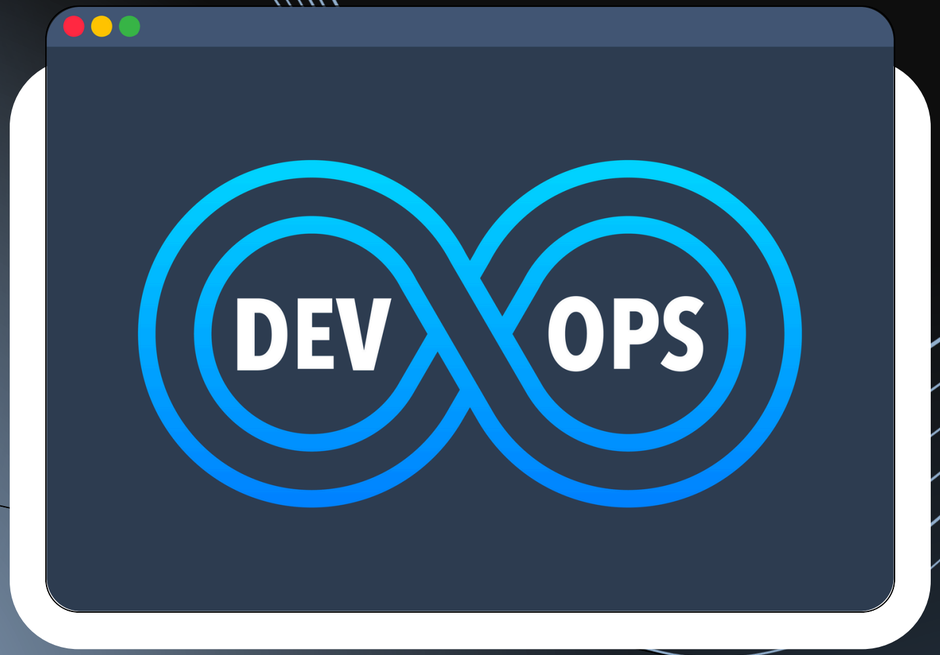
Market Share

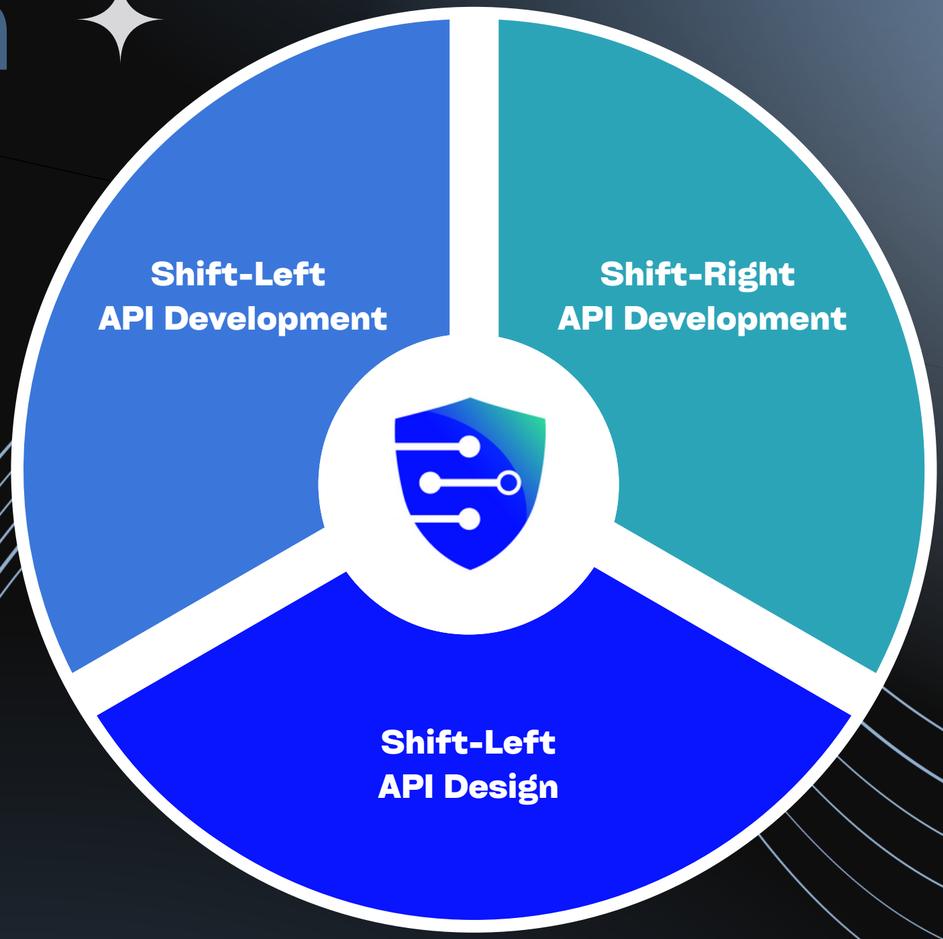




Source: www.verifiedmarketresearch.com/product/api-security-market/

Market Ecosystem





What is ApiFort?

APIFORT is an advanced cybersecurity solution designed to safeguard APIs against a wide range of security threats and vulnerabilities.

APIFORT protects modern web applications, microservices, and APIs in cloud, on-premises, and hybrid environments.

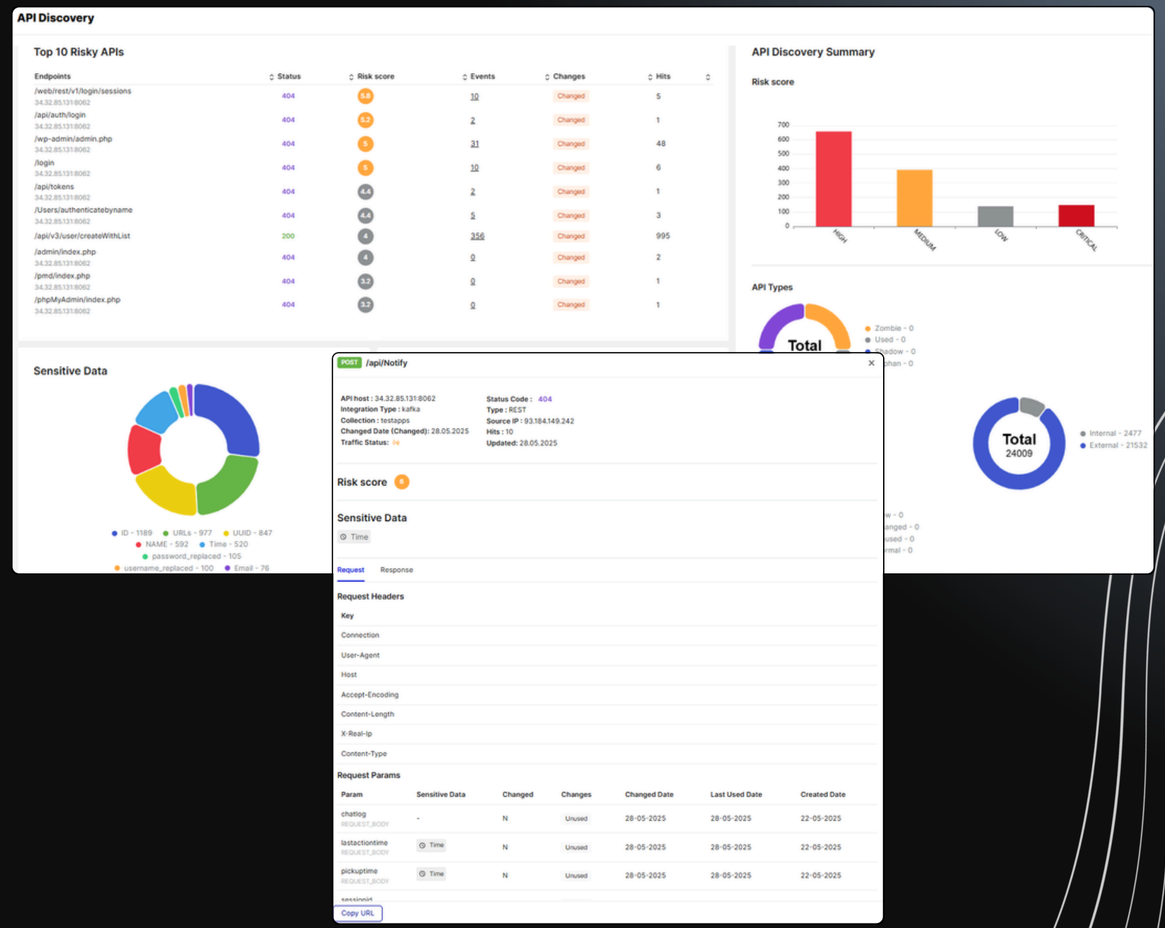
Key Features of ApiFort

- API Discovery
- Real-time API Attack Detection
- Detect Changes in APIs
- Vulnerability Detection
- Up-to-date API Inventory
- Sensitive Data Detection
- API OWASP Top 10
- Enhanced Integrations

What is inside ApiFort?

Discovery

discover APIs and Endpoints with all the details



Enhanced API Inventory

Regenerate API Specifications from Real-Time Application Traffic

Real-Time API Traffic

Capture the traffic of APIS with multiple integrations such as F5, NGINX, GoReplay, Kong

Empower Security Strategy with Comprehensive API Risk Score

Evaluate Usage, Data Types, and Internal/External Access

API Data Classification

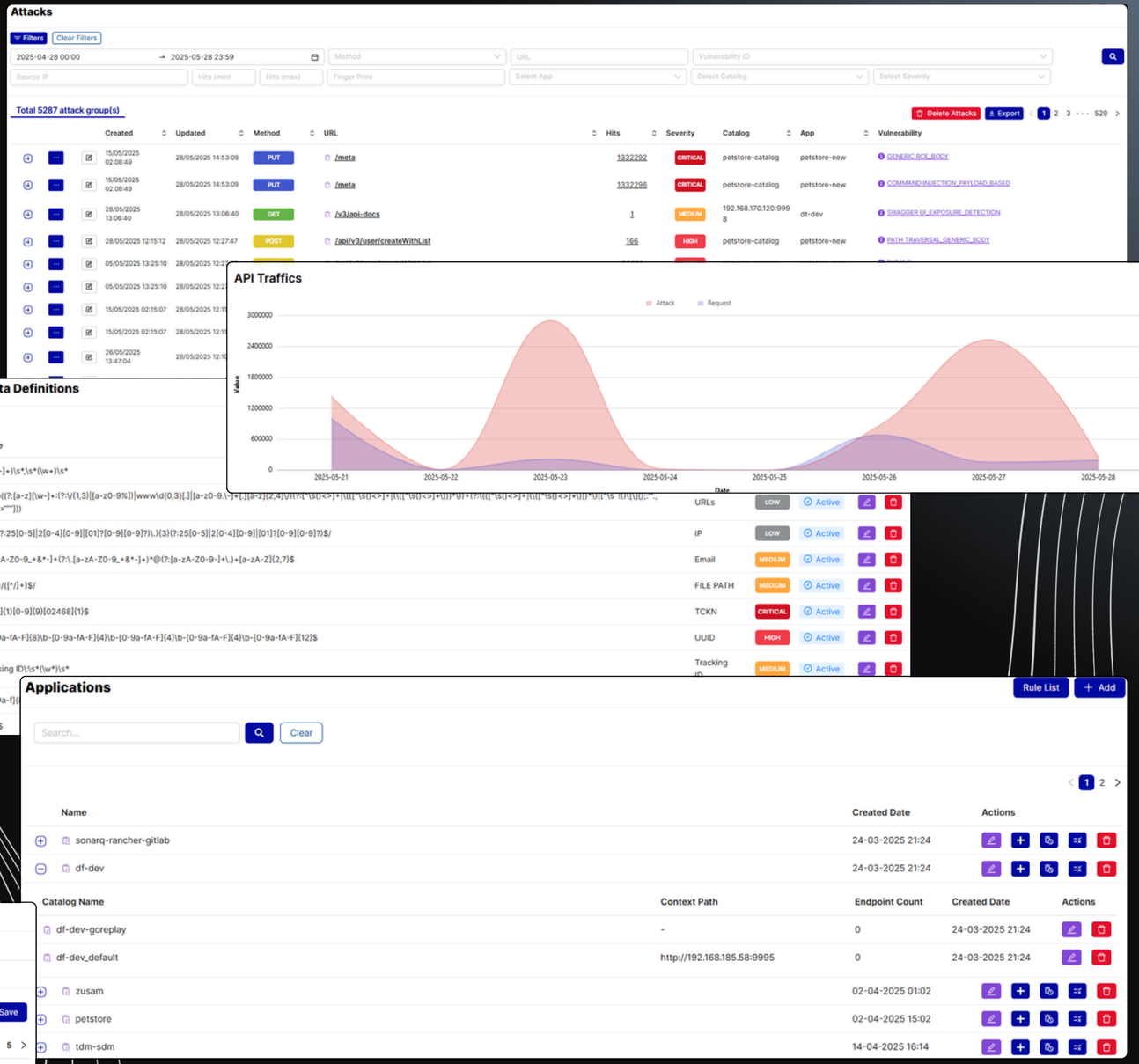
- Detect and Identify Sensitive Data as Personal, Financial, and Credentials
- Internal/External Classification

Informed with API Drift Tracking

Receive Alerts for New APIs or applications, and view changes

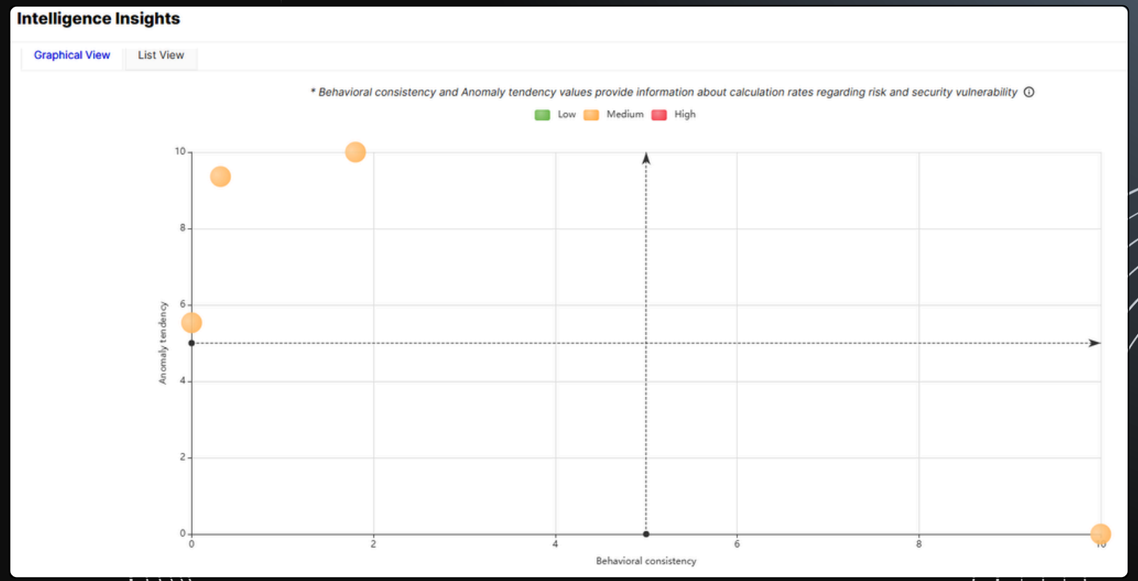
Detection

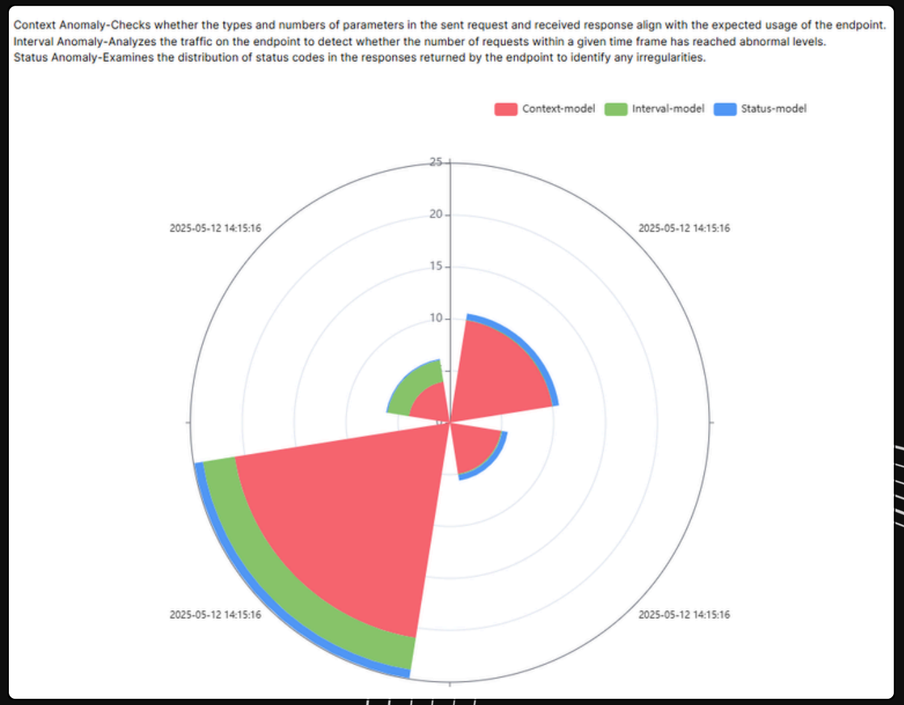
- list and filter all the Events with their details as Method, Hits, Risk score, Severity etc.
- view API Traffic, Attack Types and Vulnerabilities
- manage Applications & Collections
- manage Sensitive Data Definitions
- manage Parameters & Rules
- add Swagger URL or Collection File

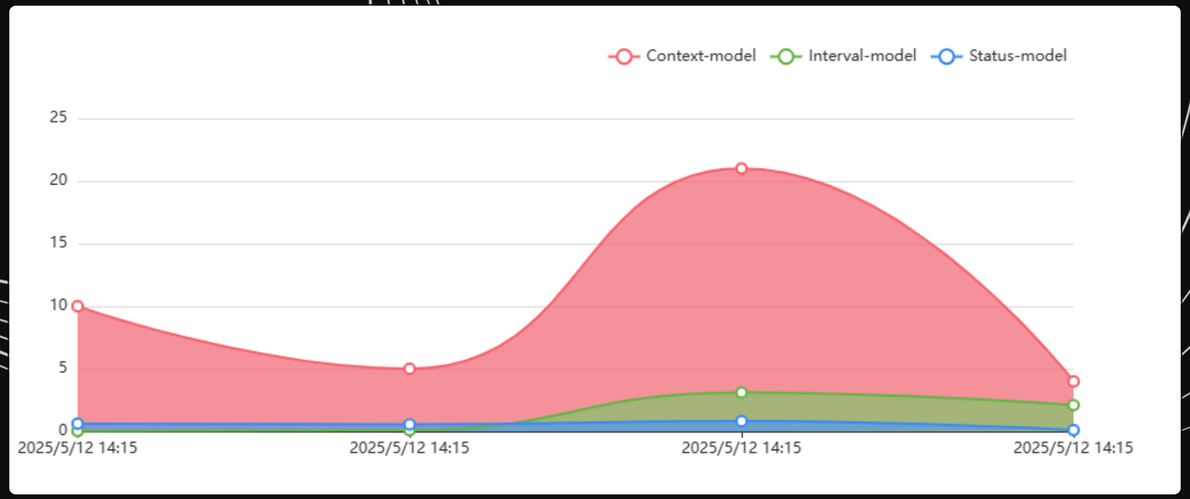


Intelligence Insights

- secures APIs using artificial intelligence
- aims to ensure security by learning the usage behavior of APIs instead of adding traditional rules
- detects uses that are outside general patterns and behaviors that could be malicious.







Integration Capabilities

Streamline Collaboration Across Teams: Easily Integrate API Security with Your Current DevOps and Security Tools!

DevOps Tools

Coming soon with CLI support

- Atlassian OpsGenie
- Jenkins
- Azure DevOps

Universal Integration

- General WebHooks
- Public APIs
- Atlassian Jira
- FluentD
- Logstash

SOAR

- Splunk Phantom — In Testing
- Cortex XSOAR — In Development

SIEM

- Splunk SIEM — In Testing
- Sumo Logic SIEM
- IBM QRadar SIEM

Messengers

- Slack
- MS Teams

Comparison Matrix

	on-premise	on-premise	cloud
Features	ApiFort	wallarm	wallarm
Attack categorization based on OWASP API Top 10	✅	✅	✅
Customer-Defined Signatures	✅	✅	✅
Micro Brute Force Detection	✅	✅	✅
BOLA (Broken Object Level Authorization) Protection	✅	✅	❌
Credential Stuffing Detection	✅	✅	✅
Vulnerability Analysis	✅	❌	✅
API Specification Comparison and Zombie/Shadow API Detection	✅	✅	✅
Customizable Sensitive Data Detection	✅	✅	✅
Customizable Sensitive Data Masking	✅	✅	✅

Comparison Matrix

	on-premise	on-premise	cloud
Features	ApiFort	wallarm	wallarm
API Risk Scoring	✅	❌	❌
API Discovery	✅	❌	✅
API Signature Change Detection	✅	✅	✅
SIEM/SOAR Integrations	✅	✅	✅
SSO (Single Sign-On) Support	✅	❌	❌
Role-Based Access Control (RBAC)	✅	❌	❌
Multi-tenant	✅	✅	✅
False positive marking	✅	✅	✅
Multi-Focused Dashboards	✅	✅	✅
AI-Based Anomaly Detection	✅	❌	❌

Comparison Matrix

	on-premise	on-premise	cloud
Features	ApiFort	wallarm	wallarm
Cloud Provider Traffic Support (AWS, Azure, GCP)	✗	✗	✓
Various API Traffic Capture Methods (F5, Nginx, Mirror, Direct, etc.)	✓	✓	✓
Processing REST, SOAP, and GraphQL APIs	✓	✓	✓
API Vulnerability Scanner	✓	✗	✓
In-Line Traffic Support	✗	✓	✓
WAF Features	✗	✗	✓
API Abuse Prevention	✗	✗	✓
In-Line Virtual Patching	✗	✗	✓
IP Whitelisting, Blacklisting, and Greylisiting	✗	✗	✓
API Session Management	✓	✗	✓

ApiFort

ApiStrike

Meet ApiStrike!

ApiStrike is a powerful API scan module designed to help organizations proactively identify and address potential vulnerabilities in their APIs.

How ApiStrike Secures Your APIs?

Identifies APIs

Detects APIs using Swagger URL/file options across different environments.

01

Customizable Security Scans

Enforces predefined rules while allowing users to modify existing ones or add new rules.

02

Reveals Vulnerabilities

Highlights critical weaknesses in your endpoints.

03

Enhances Security Early

Enables fixes before deployment for a safer API lifecycle.

04

ApiFort

ApiStrike

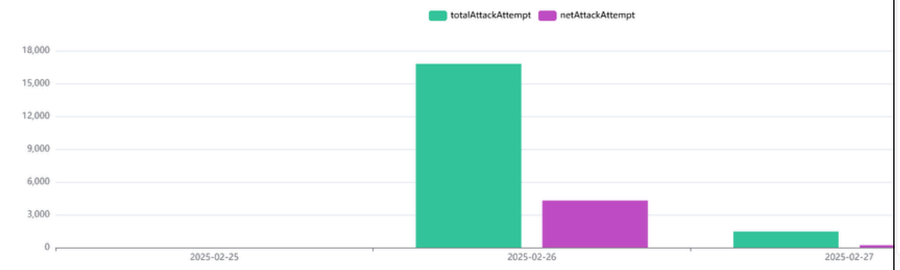
2024-11-30 → 2025-02-28

39 Projects Total: 39

3.918 APIs Total: 3918

384 Rules Total: 384

Daily Attack Attempts -- Last 3 Days



Test Status

Scheduled - 0

Running - 0

All Run Test Count: 90

Authentication

Authenticated - 351

Not authenticated - 2955

Methods

DELETE
GET
POST
PUT

Test Details

7155 Attack Attempts

Vulnerability Seve

LOW: 0 MEDIUM: 0 HIGH: 25

Vulnerabilities | Attack Attempts | Endpoints

Method | URL | Vulnerability Category | Severity

Method	URL	Category	Severity	Actions
DELETE	http://34.32.50.251:9090/api/user/STRING	Cross-Origin Resource Sharing (CORS)	HIGH	
PUT	http://34.32.50.251:9090/api/user/STRING		HIGH	
GET	http://34.32.50.251:9090/api/user/STRING		HIGH	
GET	http://34.32.50.251:9090/api/user/logout		HIGH	
GET	http://34.32.50.251:9090/api/user/login		HIGH	
POST	http://34.32.50.251:9090/api/user/createWithList		HIGH	

Most Frequent Vulnerabilities

Vulnerability Type	Count
CORS MISCONFIGURATION INVALID ORIGIN	604
HSTS SECURITY DETECTION	494
IDOR ATTACK URL BASED	179
IDOR ATTACK PAYLOAD BASED	109
DESCRIPTIVE ERROR MESSAGE INVALID PAYLOAD	11
PII SENSITIVE DATA LEAK	10

Swagger URL/File Actions

deneme You can save the Swagger URL or file for this project.

Swagger URL | Collection File

Swagger URL Ex: http://11.12.13.14:8080/v3/api-docs

API Endpoint

Save

PUT http://34.32.50.251:9090/api/pet

Request URL

PUT - http://34.32.50.251:9090/api/pet

Query Params

-

Secure

Secure

Request Headers

Key	Value
Content-Type	application/json

Request Body


```
{
  id: 10
  name: "doggie"
  category: {
    id: 1
    name: "Dogs"
  }
  photoUrls: [
    0: "string"
  ]
  tags: [
    0: {
      id: 0
      name: "string"
    }
  ]
  status: "available"
}
```

Local Power, Global Vision

Apifort is an API security platform developed in Türkiye with 100% local technology.

Full Compliance with Regulations and KVKK

Local infrastructure simplifies regulatory compliance.

Local Support and Service

Fast response, effective communication without language barriers, and sustainable service quality.

Flexible Development and Organization-Specific Adaptation

Quick response to changing needs, customizable architecture.

Data Security

All data is hosted domestically; external dependency and data leakage risks are minimized.

Accelerated Delivery – From Procurement to Project Launch

Seamless installation, integration, and support without delays.

Thank You

For your time and attention.