ApiFort

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

Gartner
Peer Insights™

4.3 / 5 on Gartner Peer Insights
(based on early customer reviews)

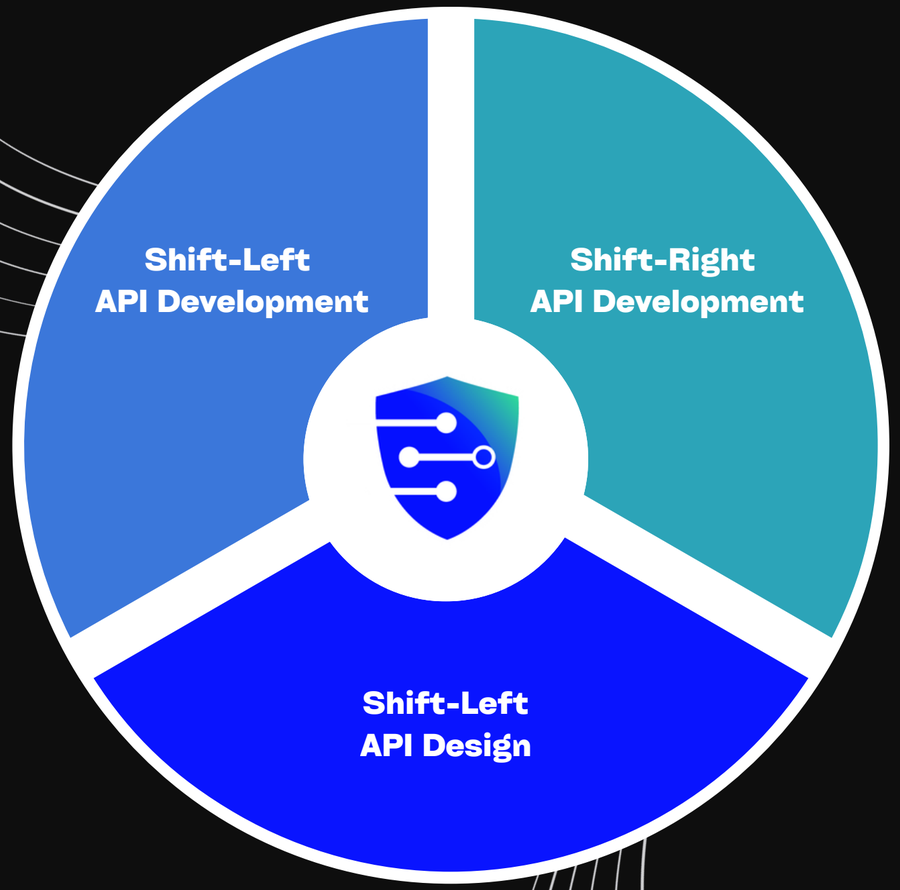
Introduction to APIs and API Security

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.

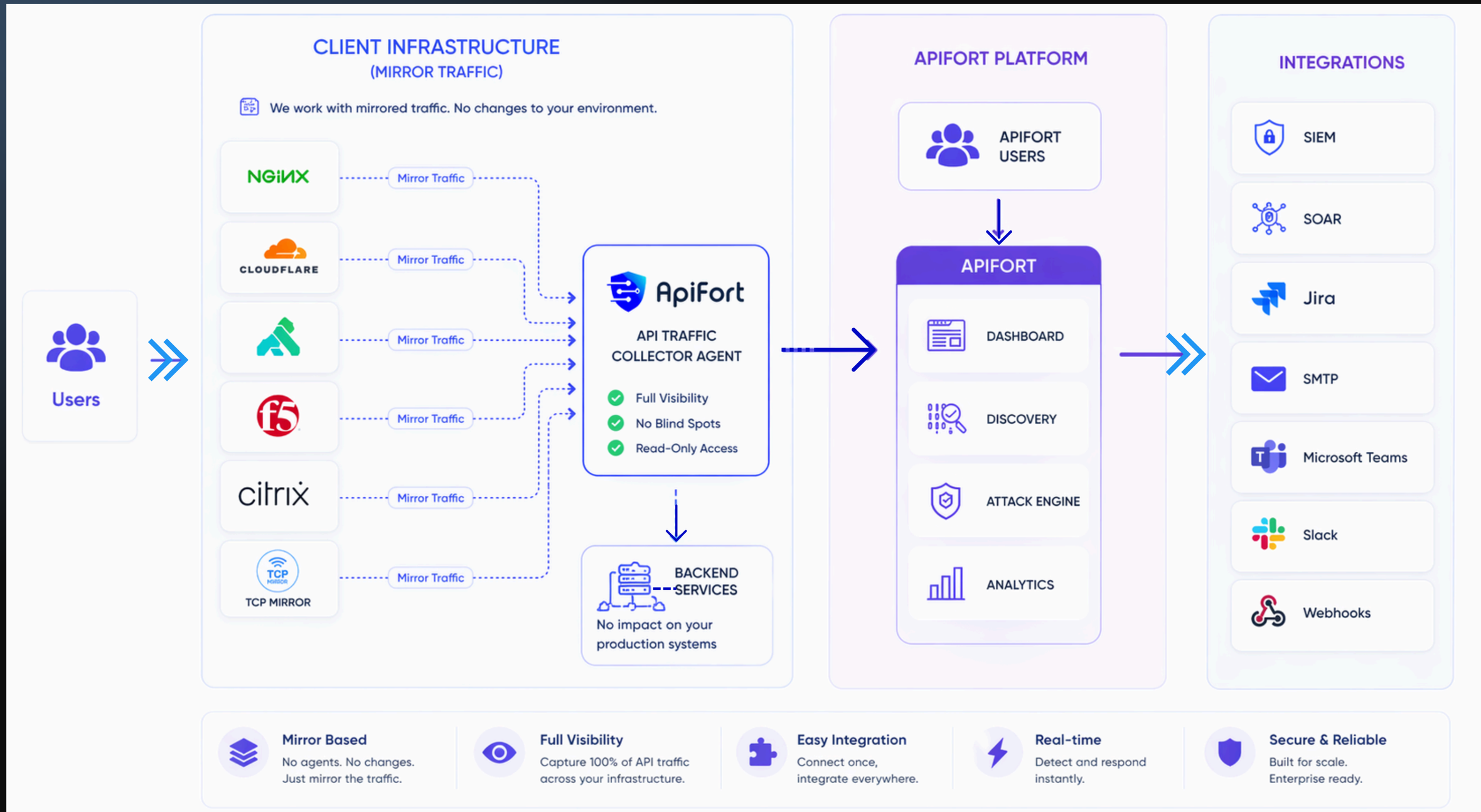


What is ApiFort?

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.

DEV OPS


CLIENT INFRASTRUCTURE
(MIRROR TRAFFIC)
We work with mirrored traffic. No changes to your environment.
Users
NGINX
CLOUDFLARE
citrix
TCP MIRROR
Mirror Traffic
Mirror Traffic
Mirror Traffic
Mirror Traffic
Mirror Traffic
Mirror Traffic
ApiFort
API TRAFFIC COLLECTOR AGENT
Full Visibility
No Blind Spots
Read-Only Access
BACKEND SERVICES
No impact on your production systems
APIFORT PLATFORM
APIFORT USERS
APIFORT
DASHBOARD
DISCOVERY
ATTACK ENGINE
ANALYTICS
INTEGRATIONS
SIEM
SOAR
Jira
SMTP
Microsoft Teams
Slack
Webhooks
Mirror Based
No agents. No changes. Just mirror the traffic.
Full Visibility
Capture 100% of API traffic across your infrastructure.
Easy Integration
Connect once, integrate everywhere.
Real-time
Detect and respond instantly.
Secure & Reliable
Built for scale. Enterprise ready.

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

Discovery

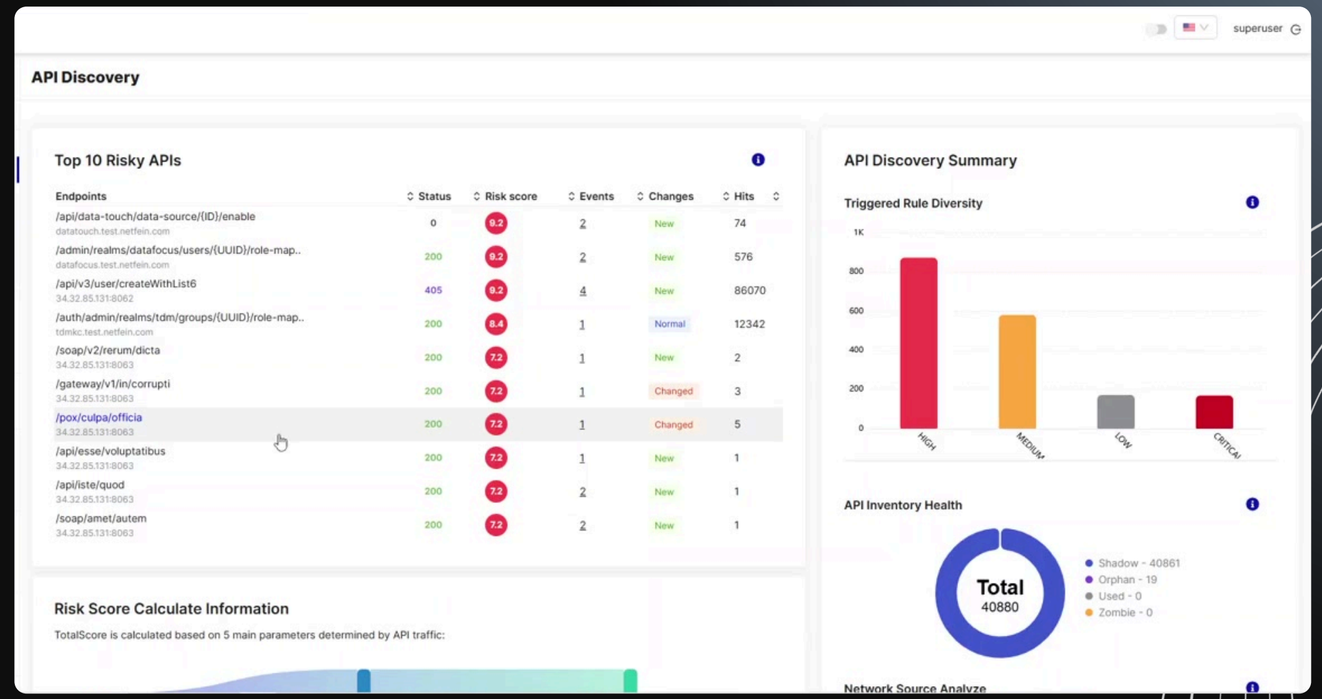
discover APIs and Endpoints with all the details

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

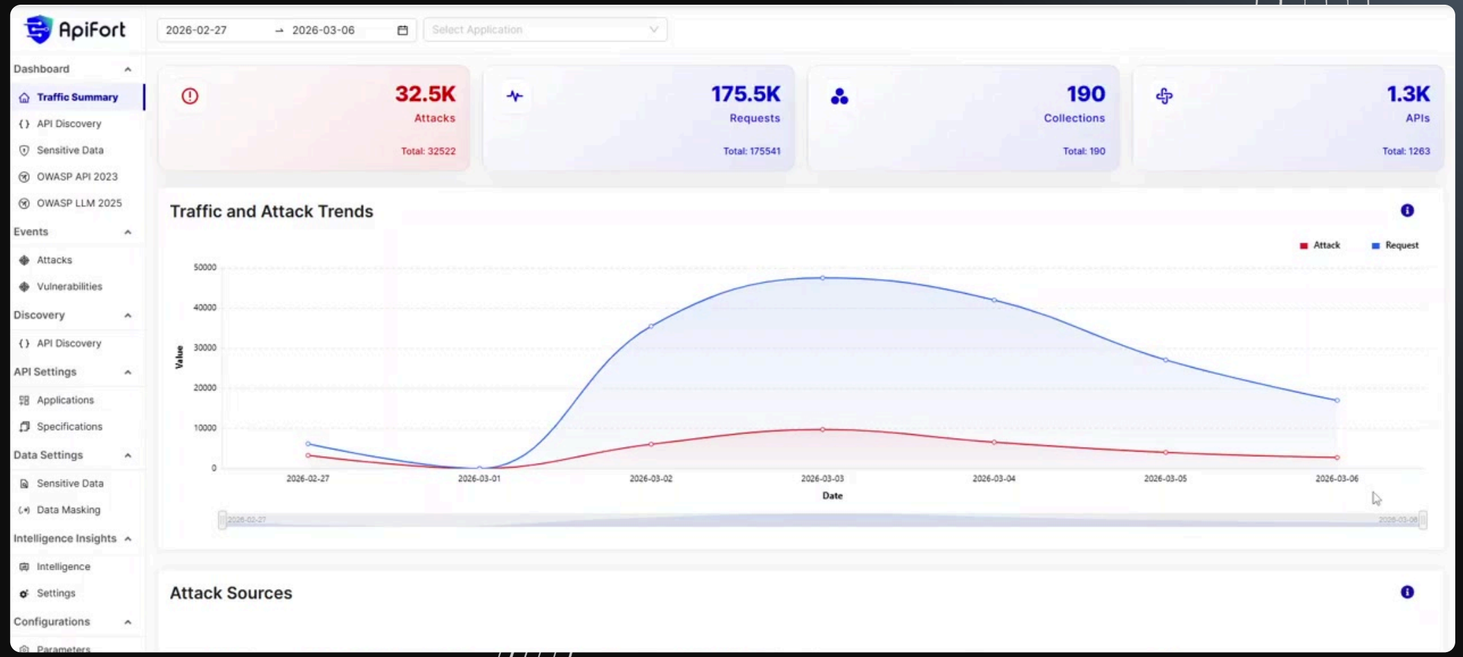
- Detect and Identify Sensitive Data as Personal, Financial, and Credentials
- Internal/External Classification

Informed with API Drift Tracking

Receive Alerts for New APIs or applications, and view changes

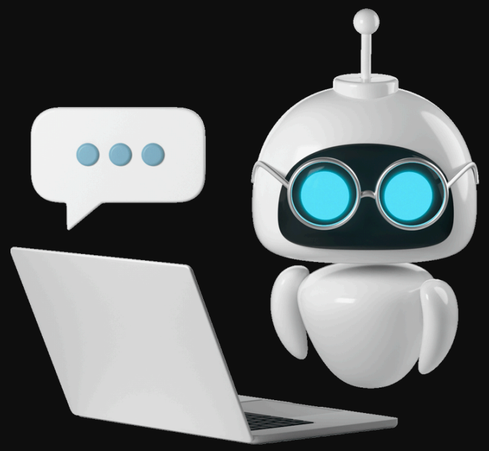
Detection

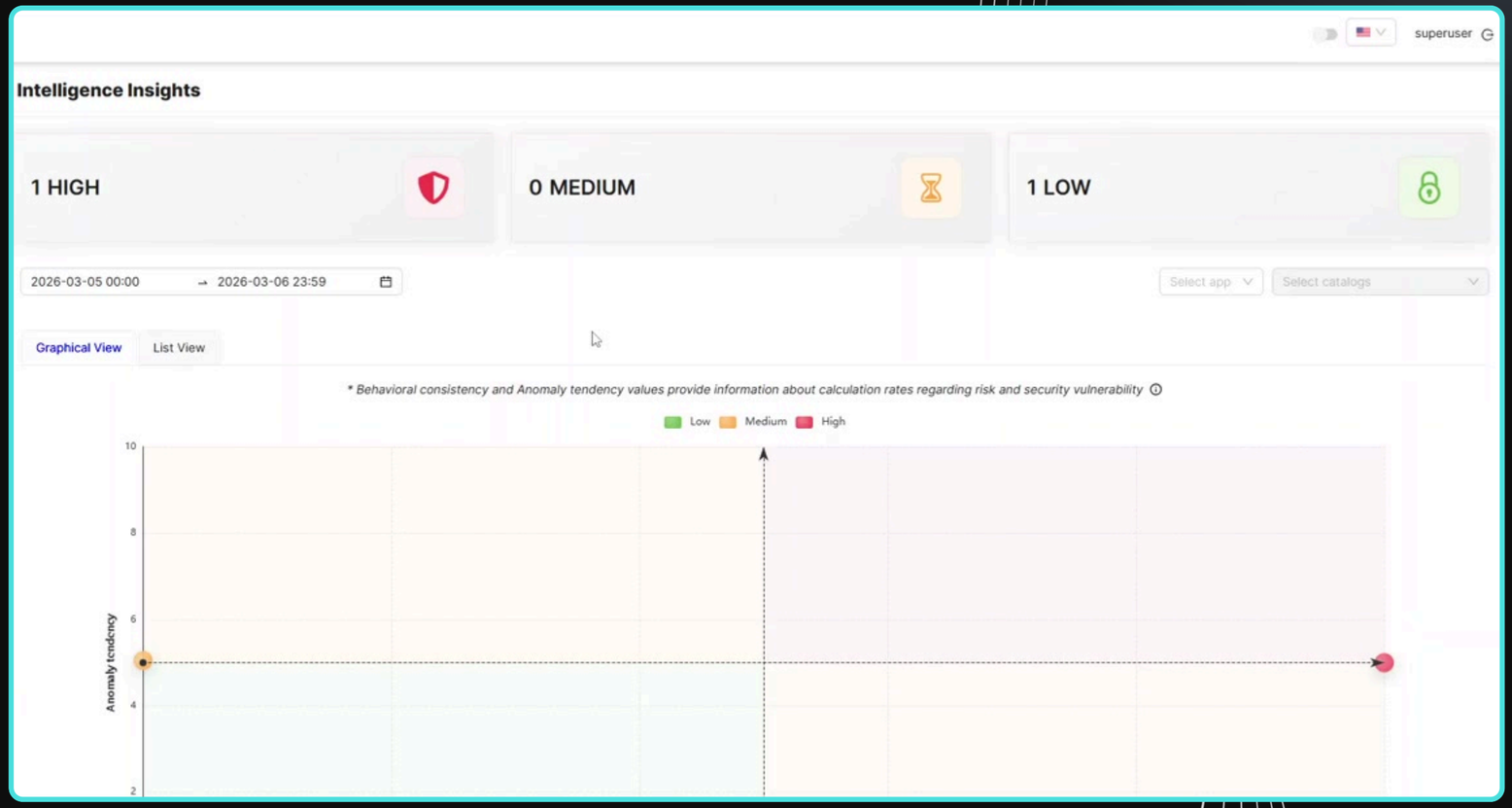
- list and filter all the Events with their details as Method, Hits, Risk score, Severity etc.
- view API Traffic, Attack Types and Vulnerabilities
- manage Applications & Collections
- manage Sensitive Data Definitions
- manage Parameters & Rules
- add Swagger URL or Collection File



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.





New in APIFORT:

AI-Powered Security Automation

AI-Assisted Sensitive Data Discovery

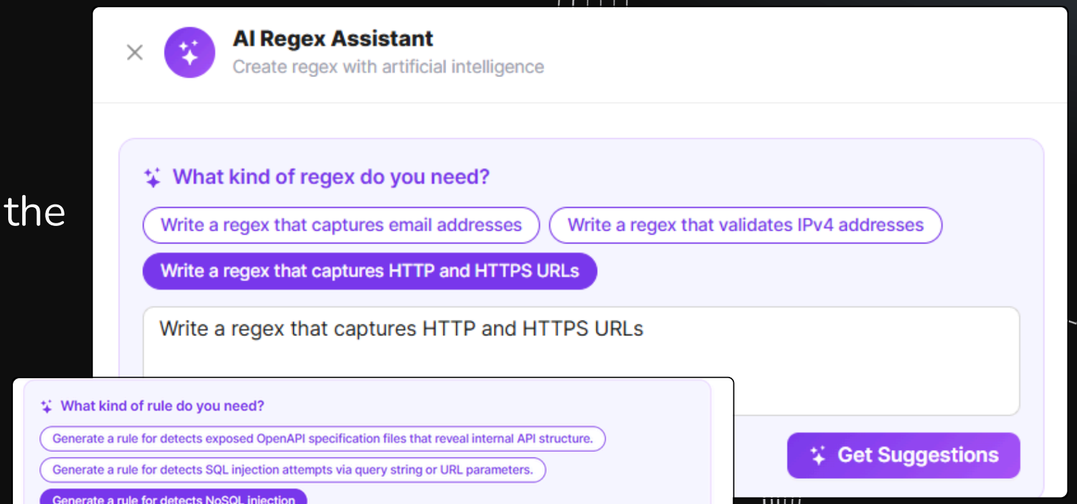
Generate regex patterns for sensitive data detection using natural language prompts. Test generated expressions instantly and apply the most suitable pattern with a single click.

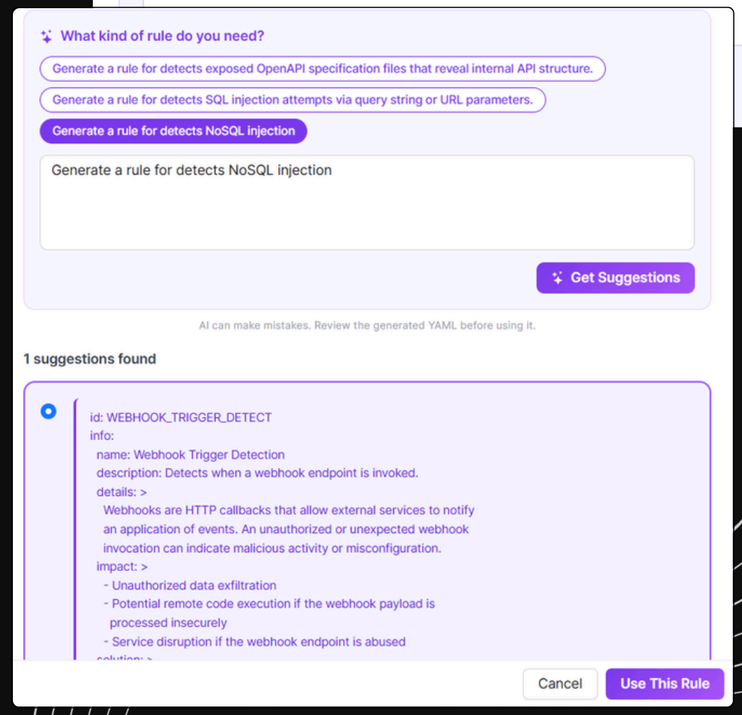
AI-Assisted Data Masking Configuration

Accelerate masking policy creation with AI-generated regex recommendations. Validate results in real time and deploy masking patterns directly from the interface.

AI-Driven Custom Rule Generation

Create custom security rules by describing protection requirements in natural language. AI automatically generates rules aligned with APIFORT's rule framework, reducing manual effort and configuration complexity.





Integration Capabilities

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

Universal Integration

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

SOAR

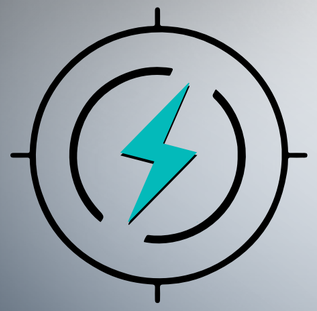
- Splunk Phantom
- Cortex XSOAR

SIEM

- Splunk SIEM
- Sumo Logic SIEM
- IBM QRadar SIEM

Messengers

- Slack
- MS Teams



ApiStrike

Meet ApiStrike

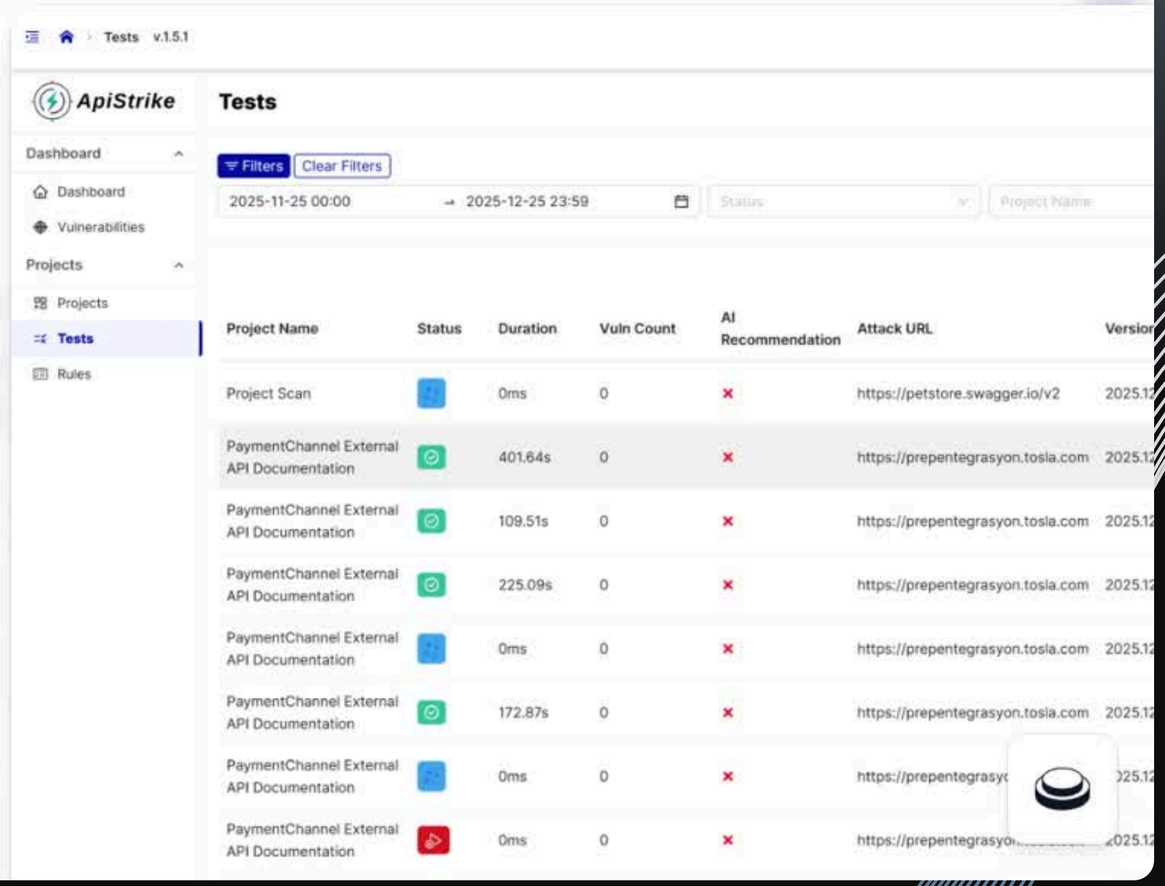
ApiStrike is a powerful API scan module designed to help organizations proactively identify and address potential vulnerabilities in their APIs.

ApiStrike

Run an API Security Scan and Review Test Results with ApiStrike

Discover how to add a project, configure API documentation, run a security scan, and interpret test findings.

Get Started



Thank You

For your time and attention.