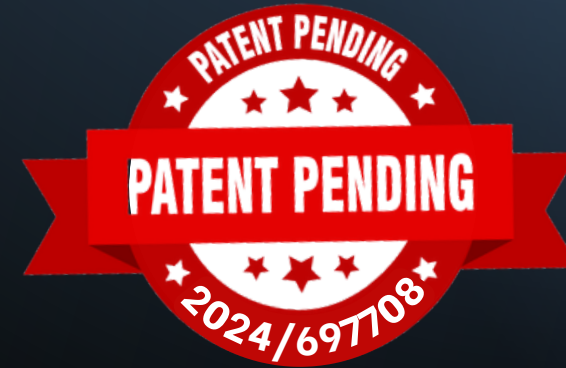




Apifort

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.

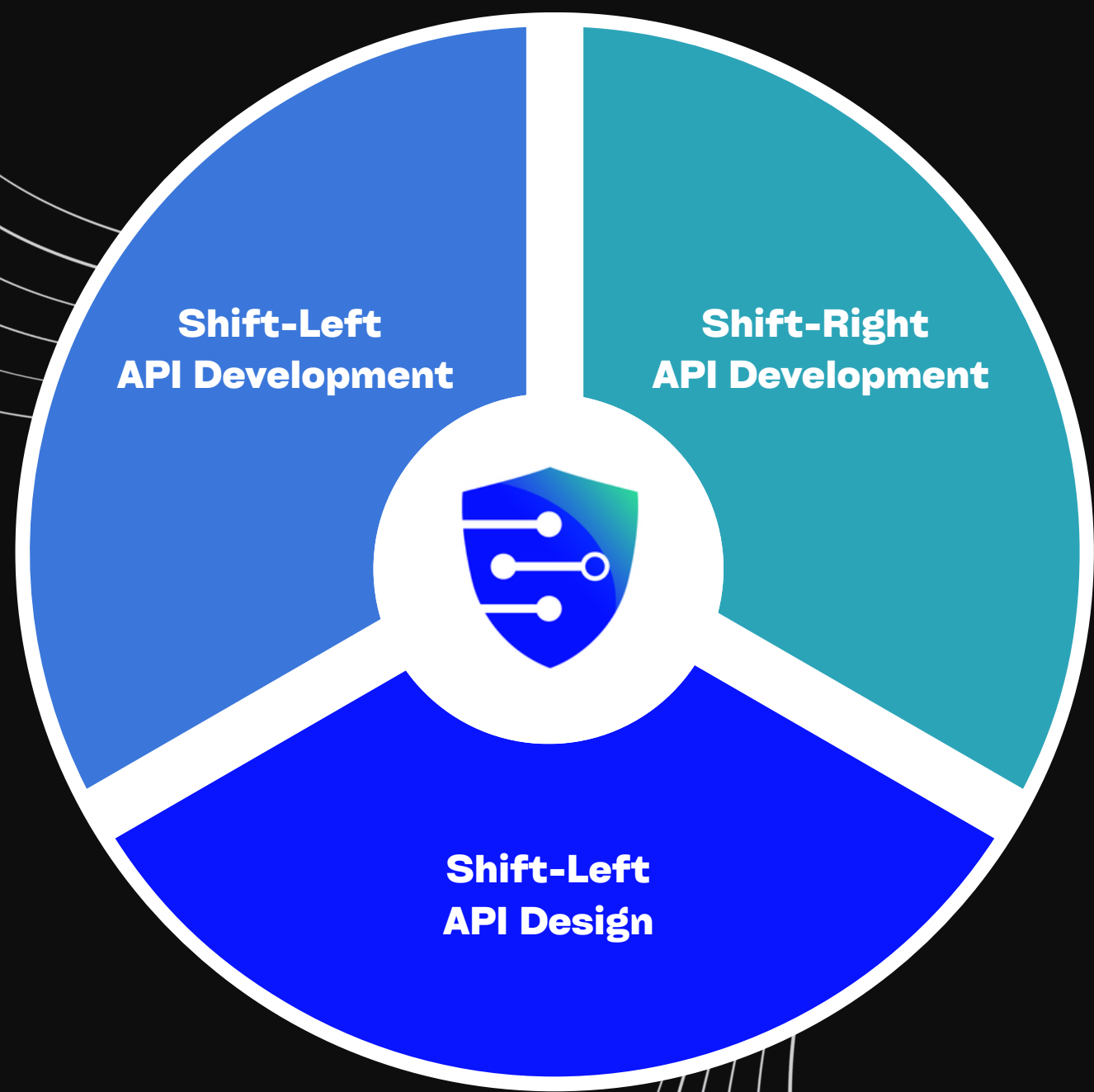


- **McHire (McDonald's):** Weak administrative access controls and IDOR vulnerabilities led to the exposure of job applicant data.



- **HPE OneView:** An unauthenticated REST API vulnerability enabled remote code execution (RCE) and was added to CISA's list of actively exploited vulnerabilities.



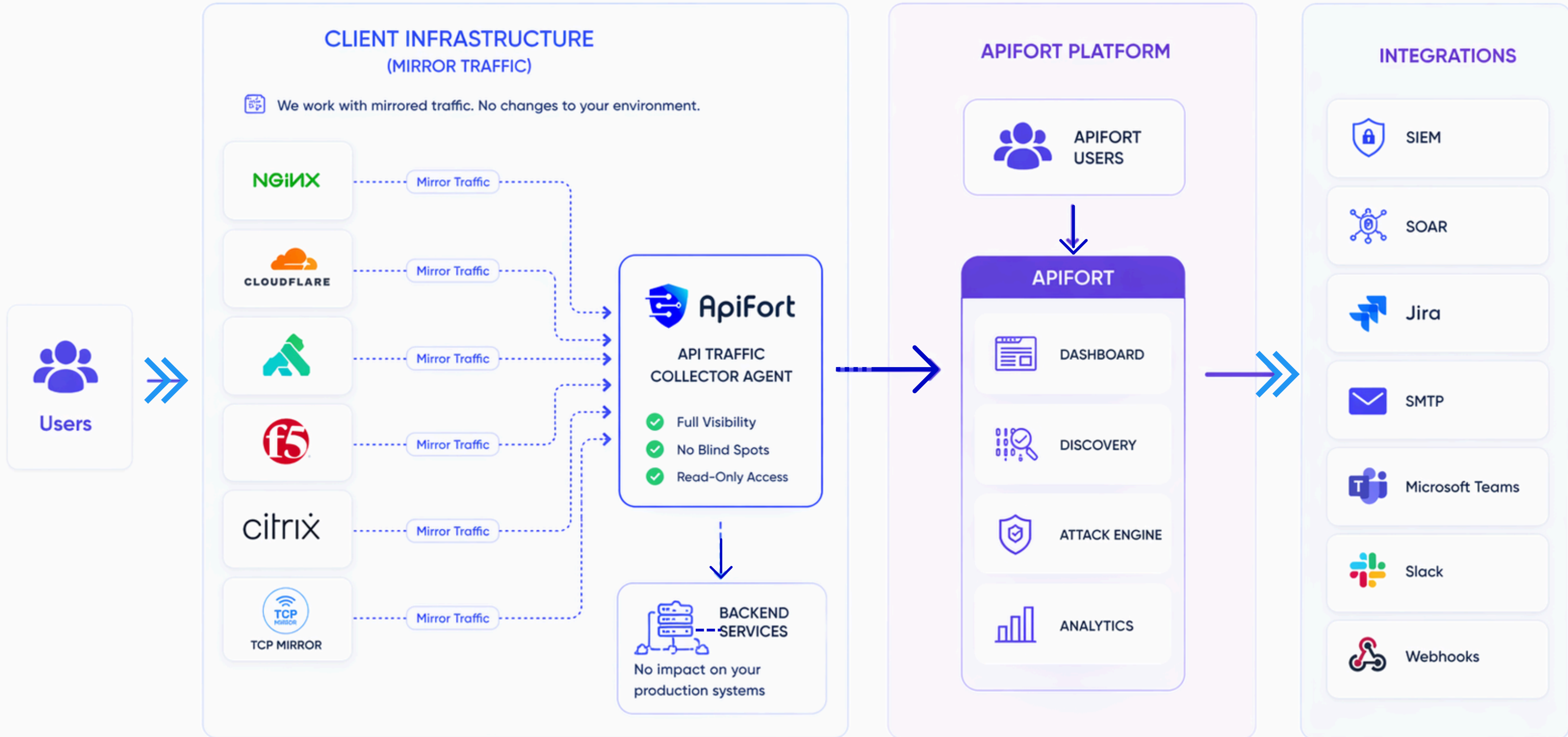


What is ApiFort? ✨

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.





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

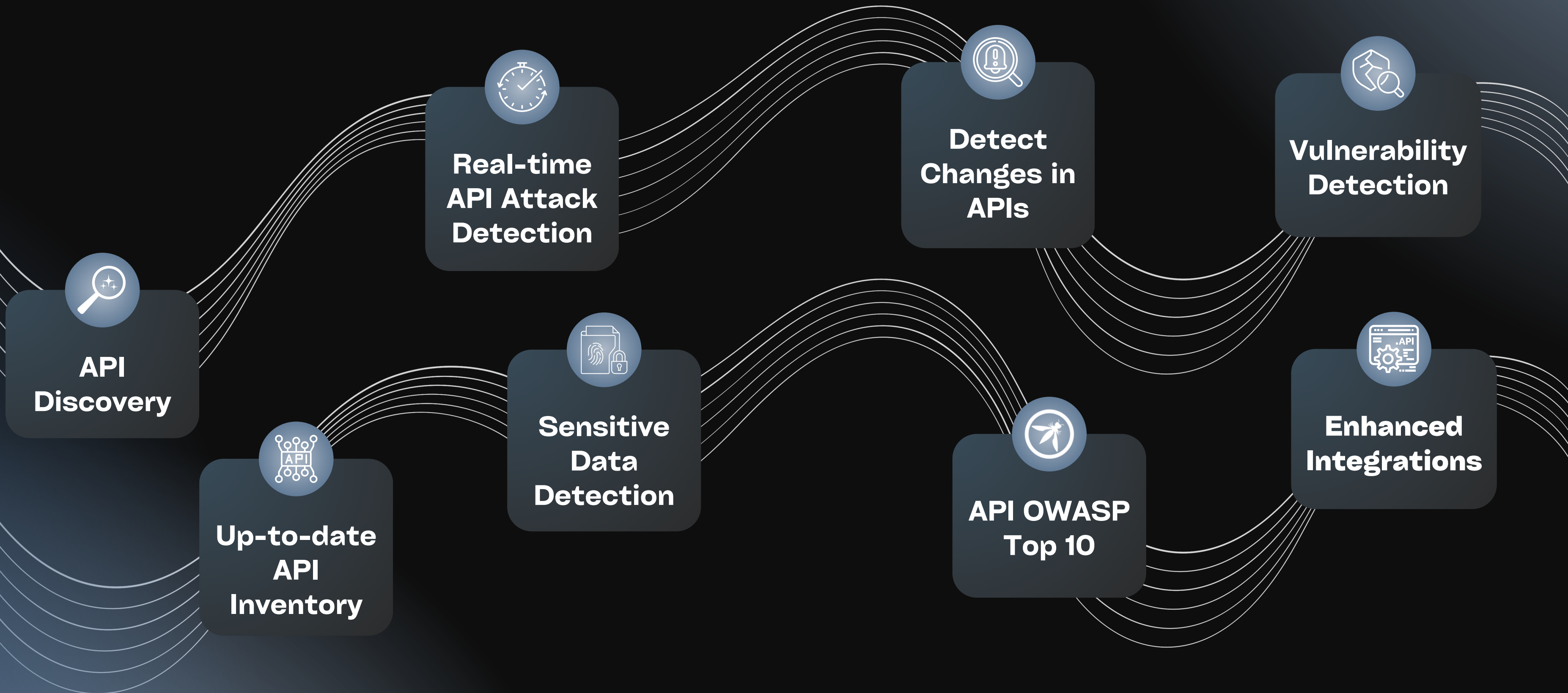
Detect and respond instantly.



Secure & Reliable

Built for scale. Enterprise ready.

Key Features of Apifort



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

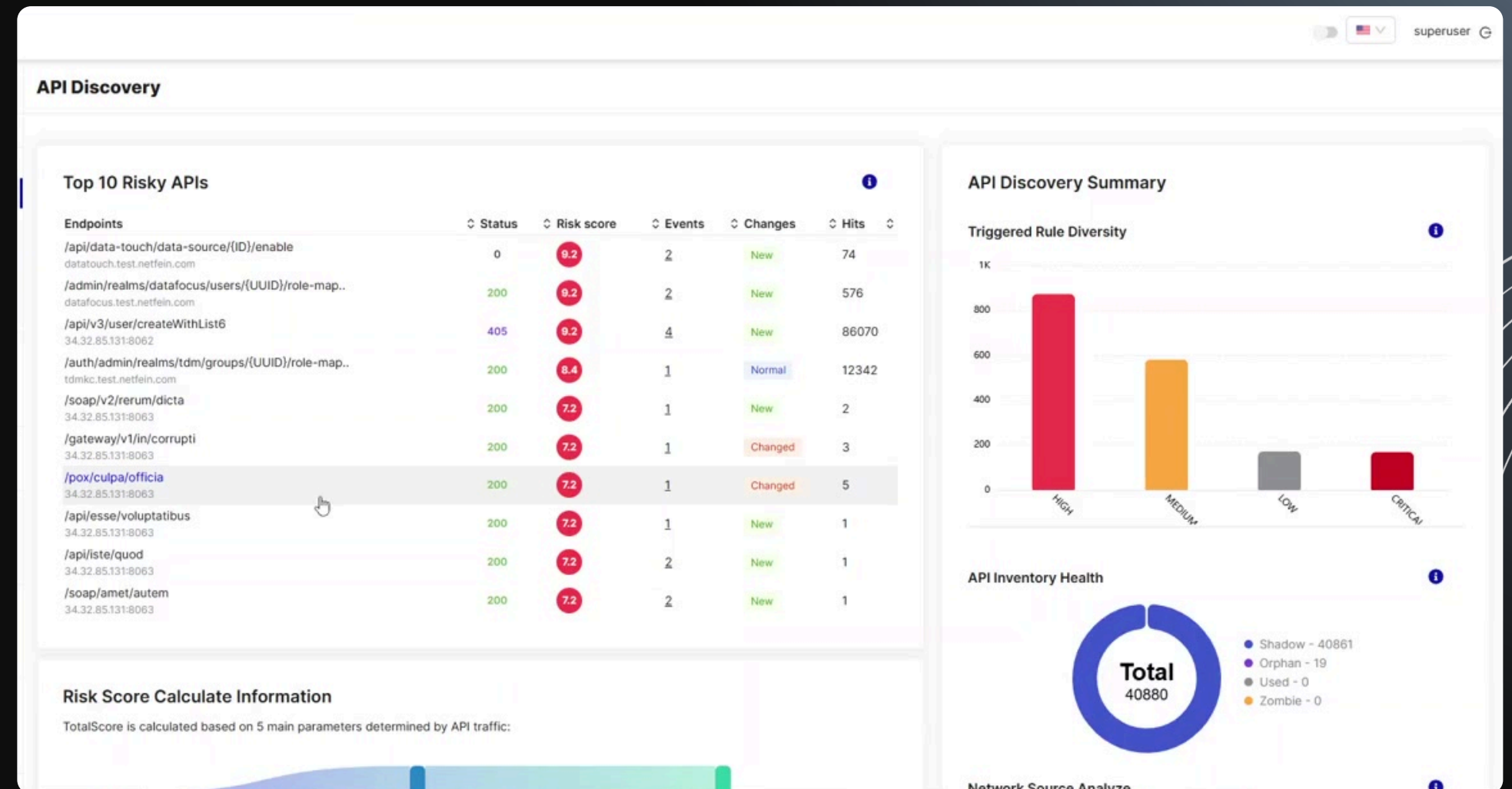
Evaluate Usage, Data Types, and Internal/External Access

API Data Classification

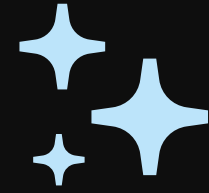
- Detect and Identify Sensitive Data as Personal, Financial, and Credentials
- Internal/External Classification

Informed with API Drift Tracking

Receive Alerts for New APIs or applications, and view changes

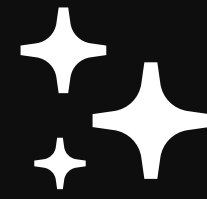


Detection



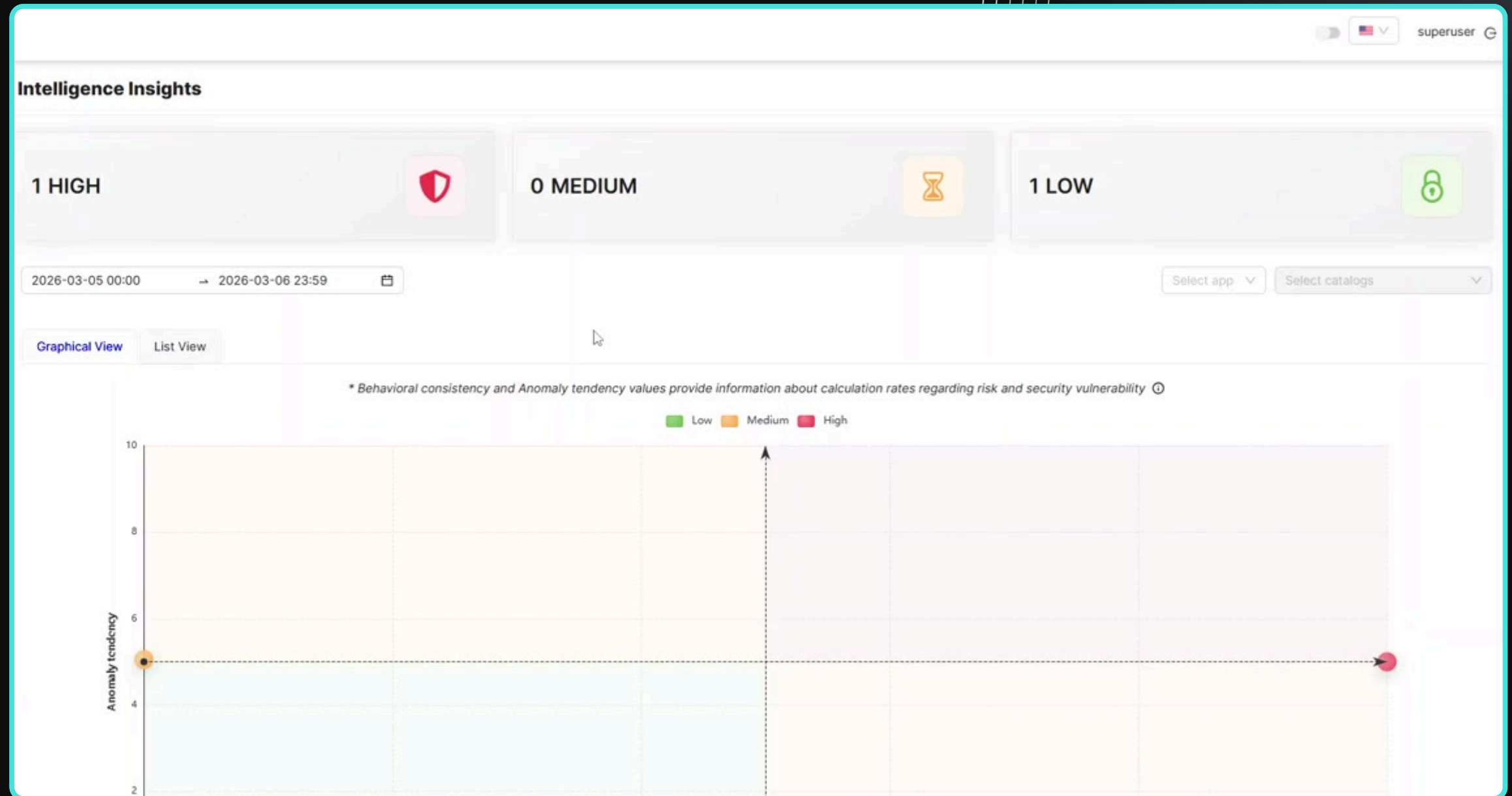
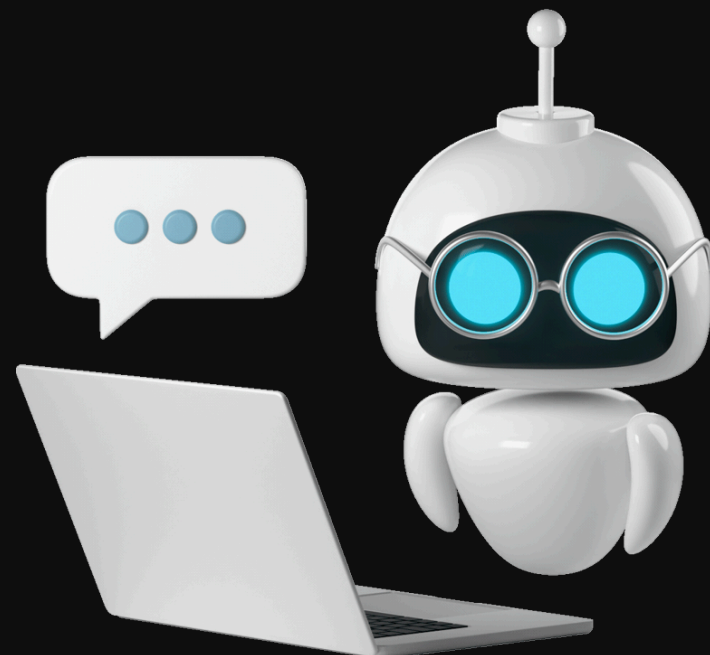
- ✦ list and filter all the Events with their details as Method, Hits, Risk score, Severity etc.
- ✦ view API Traffic, Attack Types and Vulnerabilities
- ✦ manage Applications & Collections
 - ✦ manage Sensitive Data Definitions
- ✦ manage Parameters & Rules
 - ✦ add Swagger URL or Collection File





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

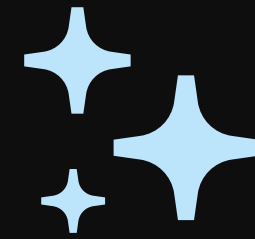
Accelerate masking policy creation with AI-generated regex recommendations. Validate results in real time and deploy masking patterns directly from the interface.

✦ 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.





The image displays two screenshots of the APIFORT interface. The top screenshot shows the 'AI Regex Assistant' window, which prompts the user to 'Create regex with artificial intelligence'. It offers several suggestions for regex patterns, such as 'Write a regex that captures email addresses' and 'Write a regex that validates IPv4 addresses'. A 'Get Suggestions' button is visible at the bottom right. The bottom screenshot shows the 'AI-Driven Custom Rule Generation' window, which prompts the user to 'What kind of rule do you need?'. It offers suggestions like 'Generate a rule for detects exposed OpenAPI specification files that reveal internal API structure.' and 'Generate a rule for detects NoSQL injection'. A 'Get Suggestions' button is visible at the bottom right. Below the suggestions, a single rule is displayed with details: 'id: WEBHOOK_TRIGGER_DETECT', 'name: Webhook Trigger Detection', 'description: Detects when a webhook endpoint is invoked.', 'details: > Webhooks are HTTP callbacks that allow external services to notify an application of events. An unauthorized or unexpected webhook invocation can indicate malicious activity or misconfiguration.', 'impact: > - Unauthorized data exfiltration - Potential remote code execution if the webhook payload is processed insecurely - Service disruption if the webhook endpoint is abused', and 'solutions: >'. A 'Cancel' button and a 'Use This Rule' button are visible at the bottom right.

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

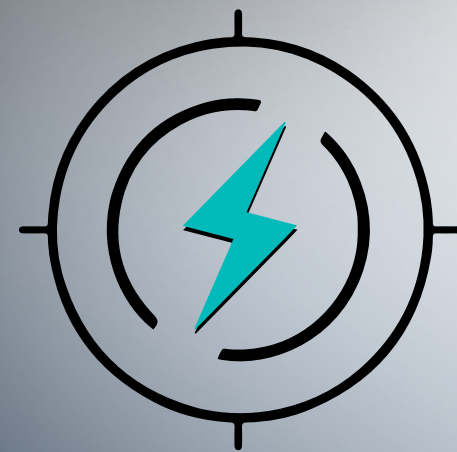
-  Splunk Phantom
-  Cortex XSOAR

SIEM

-  Splunk SIEM
-  Sumo Logic SIEM
-  IBM QRadar SIEM

Messengers

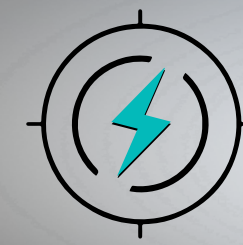
-  Slack
-  MS Teams



ApiStrike

Meet ApiStrike

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



ApiStrike



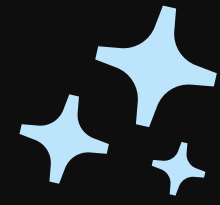
Run an API Security Scan and Review Test Results with ApiStrike

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

[Get Started](#)

The screenshot shows the 'Tests' page in the ApiStrike interface. The page title is 'Tests v.1.5.1'. On the left is a sidebar with navigation options: Dashboard, Vulnerabilities, Projects, Tests (selected), and Rules. The main content area has a 'Filters' button and a 'Clear Filters' button. Below these are date range filters: '2025-11-25 00:00' to '2025-12-25 23:59', and dropdown menus for 'Status' and 'Project Name'. The main table lists test results with columns: Project Name, Status, Duration, Vuln Count, AI Recommendation, Attack URL, and Version. The table contains 8 rows of data.

Project Name	Status	Duration	Vuln Count	AI Recommendation	Attack URL	Version
Project Scan	🟡	0ms	0	✖	https://petstore.swagger.io/v2	2025.12
PaymentChannel External API Documentation	🟢	401.64s	0	✖	https://prepentegrasyon.tosia.com	2025.12
PaymentChannel External API Documentation	🟢	109.51s	0	✖	https://prepentegrasyon.tosia.com	2025.12
PaymentChannel External API Documentation	🟢	225.09s	0	✖	https://prepentegrasyon.tosia.com	2025.12
PaymentChannel External API Documentation	🟡	0ms	0	✖	https://prepentegrasyon.tosia.com	2025.12
PaymentChannel External API Documentation	🟢	172.87s	0	✖	https://prepentegrasyon.tosia.com	2025.12
PaymentChannel External API Documentation	🟡	0ms	0	✖	https://prepentegrasyon.tosia.com	2025.12
PaymentChannel External API Documentation	🔴	0ms	0	✖	https://prepentegrasyon.tosia.com	2025.12



Thank You

For your time and attention.

