

# Apifort

Bağlantıları Koruyun, Geleceği Güvence Altına Alın  
APIFORT: API Güvenlik Çözümünüz

**Gartner**

**Peer Insights™**



Gartner Peer Insights üzerinde

4.3 / 5 değerlendirme puanı

(ilk müşteri geri bildirimlerine dayalı)

# API ve API Güvenliđi

API'ler (Uygulama Programlama Arayüzleri), farklı yazılım uygulamaları arasında iletişim kurmayı ve etkileşimde bulunmayı sağlayan köprülerdir.

API güvenliđi, API'leri yetkisiz erişimden, veri sızıntılarından ve diđer güvenlik tehditlerinden korumayı hedefleyen uygulamaları, önlemleri ve teknolojileri ifade eder.



# 2025'te 5 Büyük API Vakası



1. **DeepSeek**: Yanlış yapılandırılmış bir backend API, 1 milyondan fazla sohbet kaydı ve API anahtarının açığa çıkmasına yol açtı.



2. **Volkswagen Connected Services**: BOLA zafiyeti nedeniyle kullanıcılar, kendilerine ait olmayan araçların verilerine erişebildi.



3. **Salesloft – Drift**: Çalınan OAuth kimlikleri, Salesloft API'leri üzerinden kullanılarak Salesforce müşteri verilerinin ele geçirilmesine yol açtı.

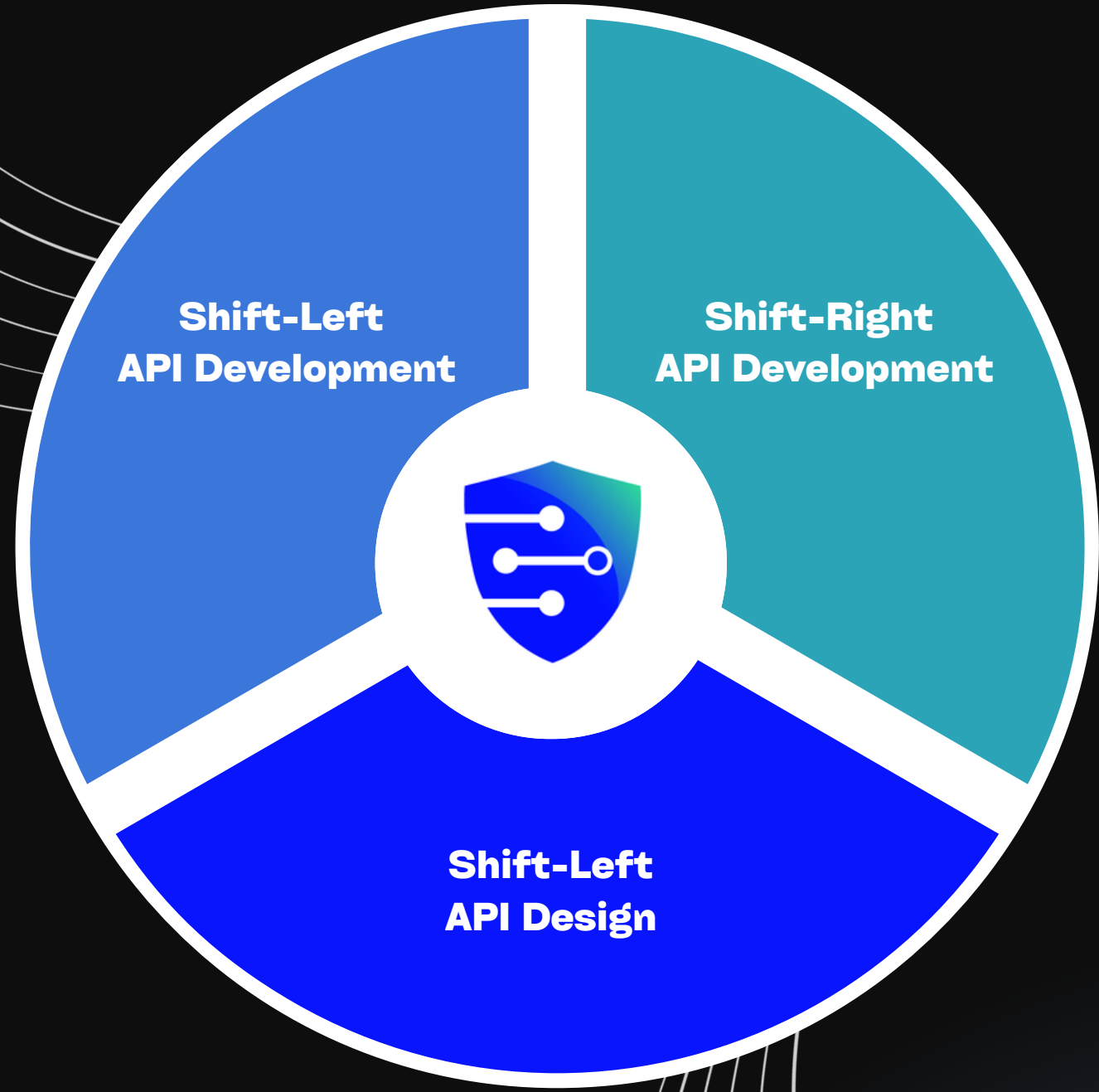


4. **McHire (McDonald's)**: Zayıf yönetici erişimleri ve IDOR açıkları, iş başvurusu yapan adayların verilerinin sızmasına neden oldu.



5. **HPE OneView**: Kimlik doğrulama gerektirmeyen bir REST API açığı, uzaktan kod çalıştırmaya (RCE) imkân tanıdı ve CISA'nın aktif tehdit listesine girdi.



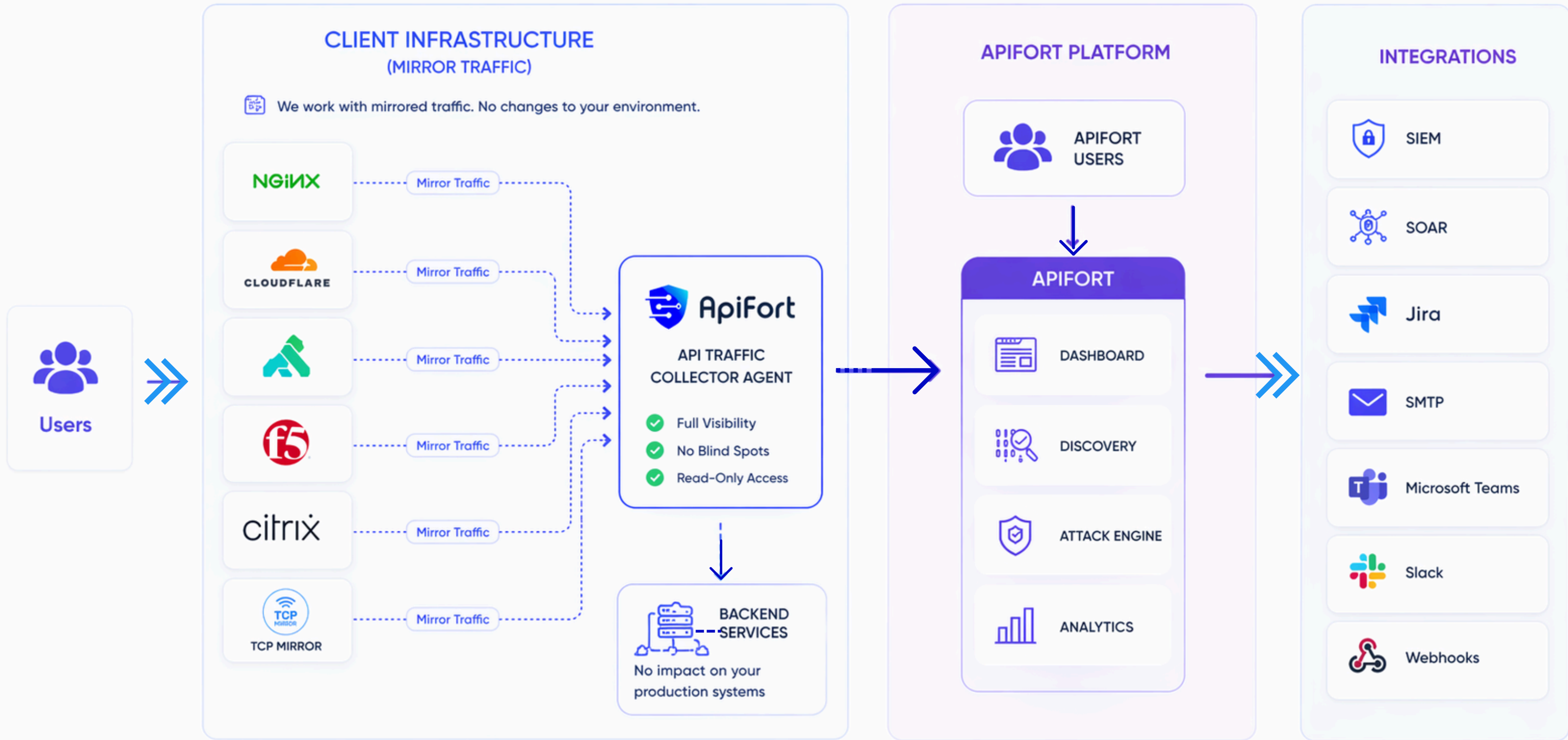


# ApiFort Nedir?

APIFORT, geniş bir güvenlik tehditleri ve zayıflıklar yelpazesine karşı API'leri korumak amacıyla tasarlanmış gelişmiş bir siber güvenlik çözümüdür.

APIFORT, modern web uygulamalarını, mikro servisleri ve bulut, yerinde (on-prem) ve hibrit ortamlardaki API'leri korur.





**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**

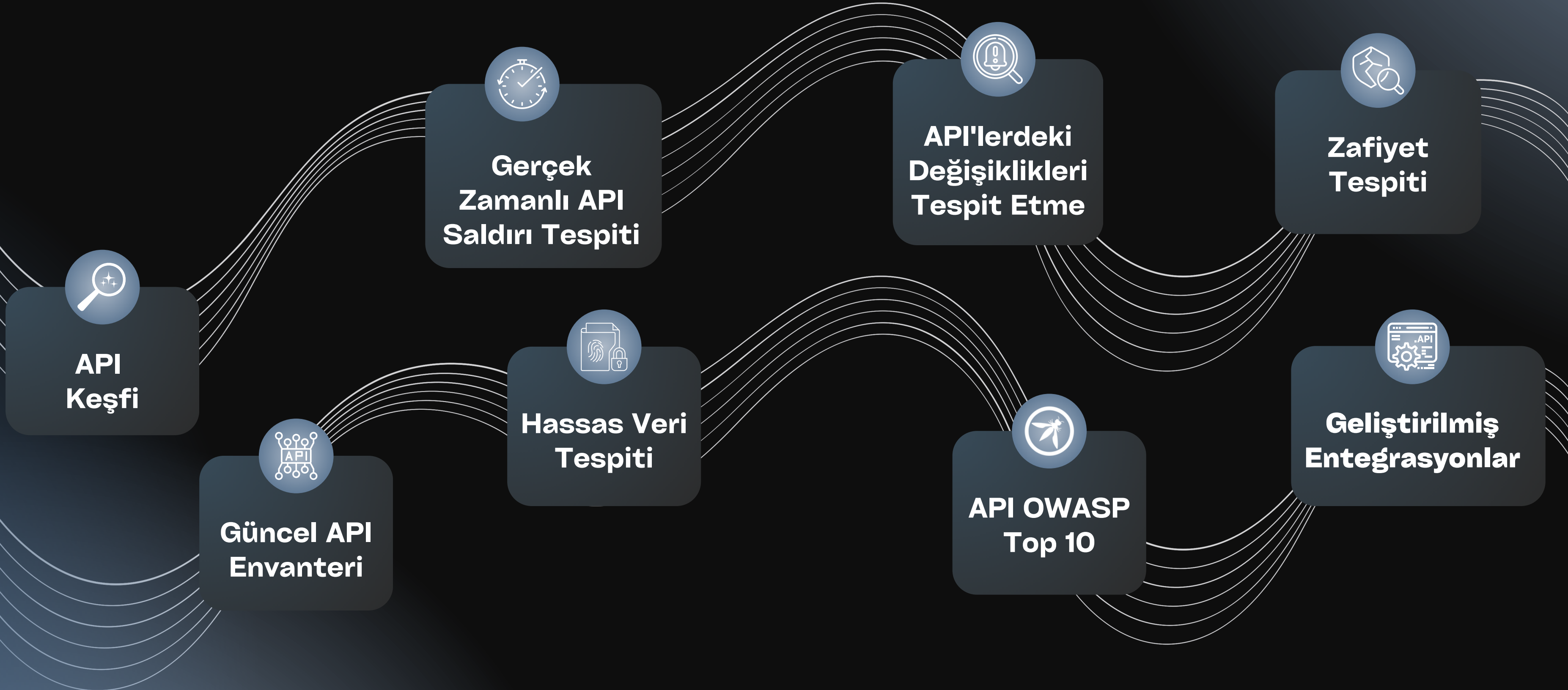
Detect and respond instantly.



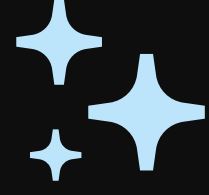
**Secure & Reliable**

Built for scale. Enterprise ready.

# ApiFort'un Temel Özellikleri



# Keşif



Tüm Detaylarıyla API'leri ve Endpointleri Keşfet

## Geliştirilmiş API Envanteri

Gerçek zamanlı uygulama trafik verilerini baz alarak API özelliklerini yeniden oluşturma

## Gerçek Zamanlı API Trafiği

F5, NGINX, GoReplay, Kong gibi birden fazla entegrasyon ile API trafiği izleme



## Kapsamlı API Risk Puanı ile Güvenlik Stratejisini Güçlendirin

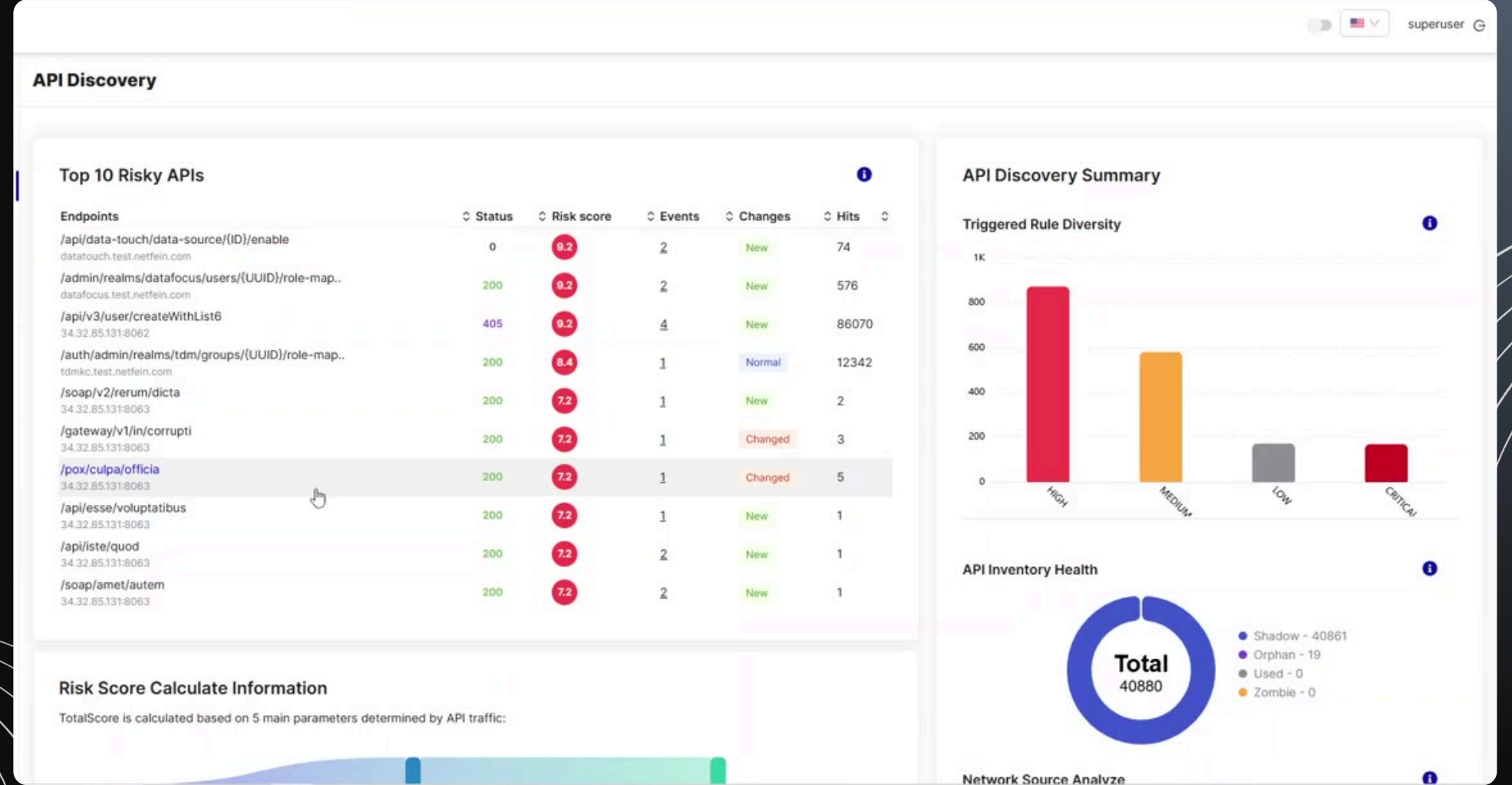
Kullanımı, veri türlerini ve iç/dış erişimi değerlendirme

## API Veri Sınıflandırması

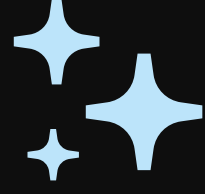
- Hassas verileri kişisel, finansal ve kimlik bilgileri olarak tanımlama
- İç/dış sınıflandırması

## API Drift İzleme ve Bilgilenme

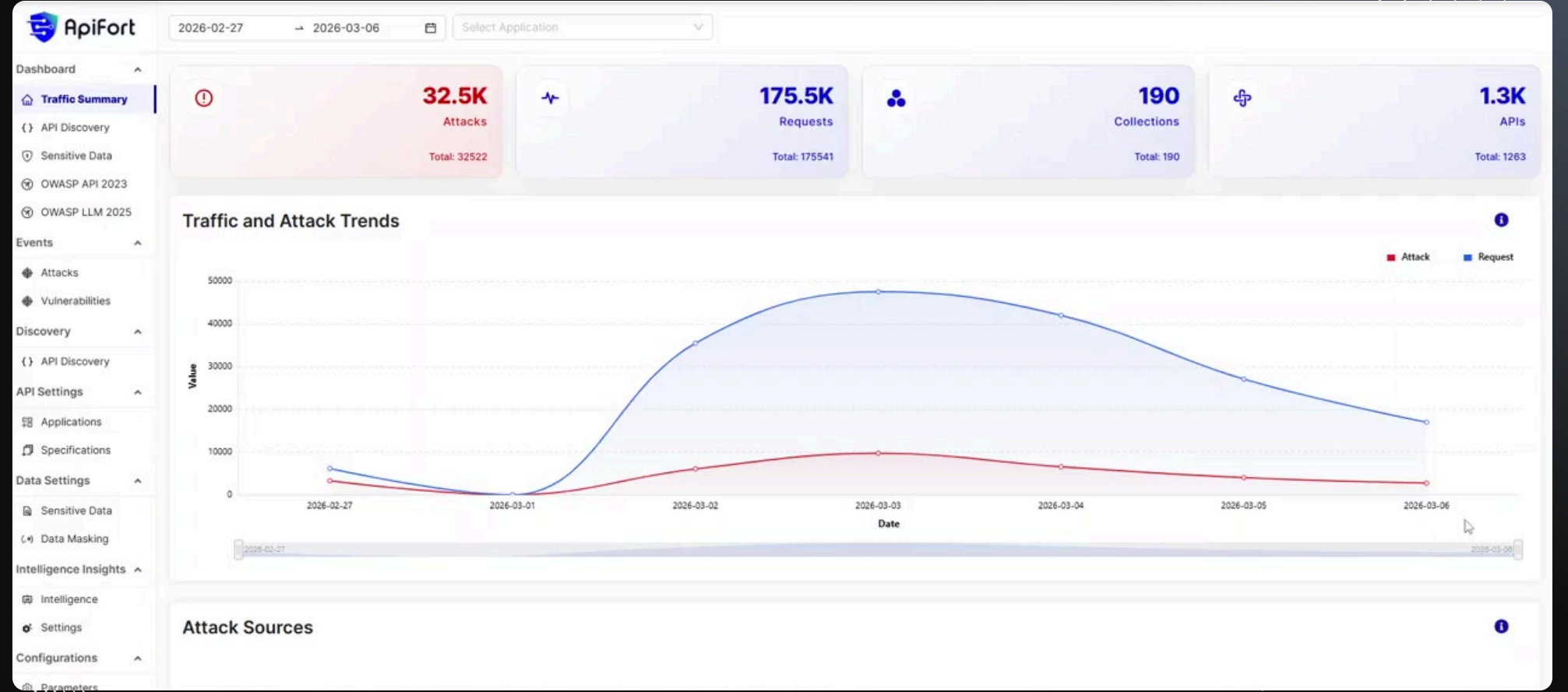
Yeni API'ler veya uygulamalar için uyarılar verme ve değişiklikleri görüntüleme



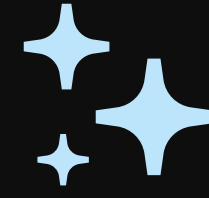
# Tespit



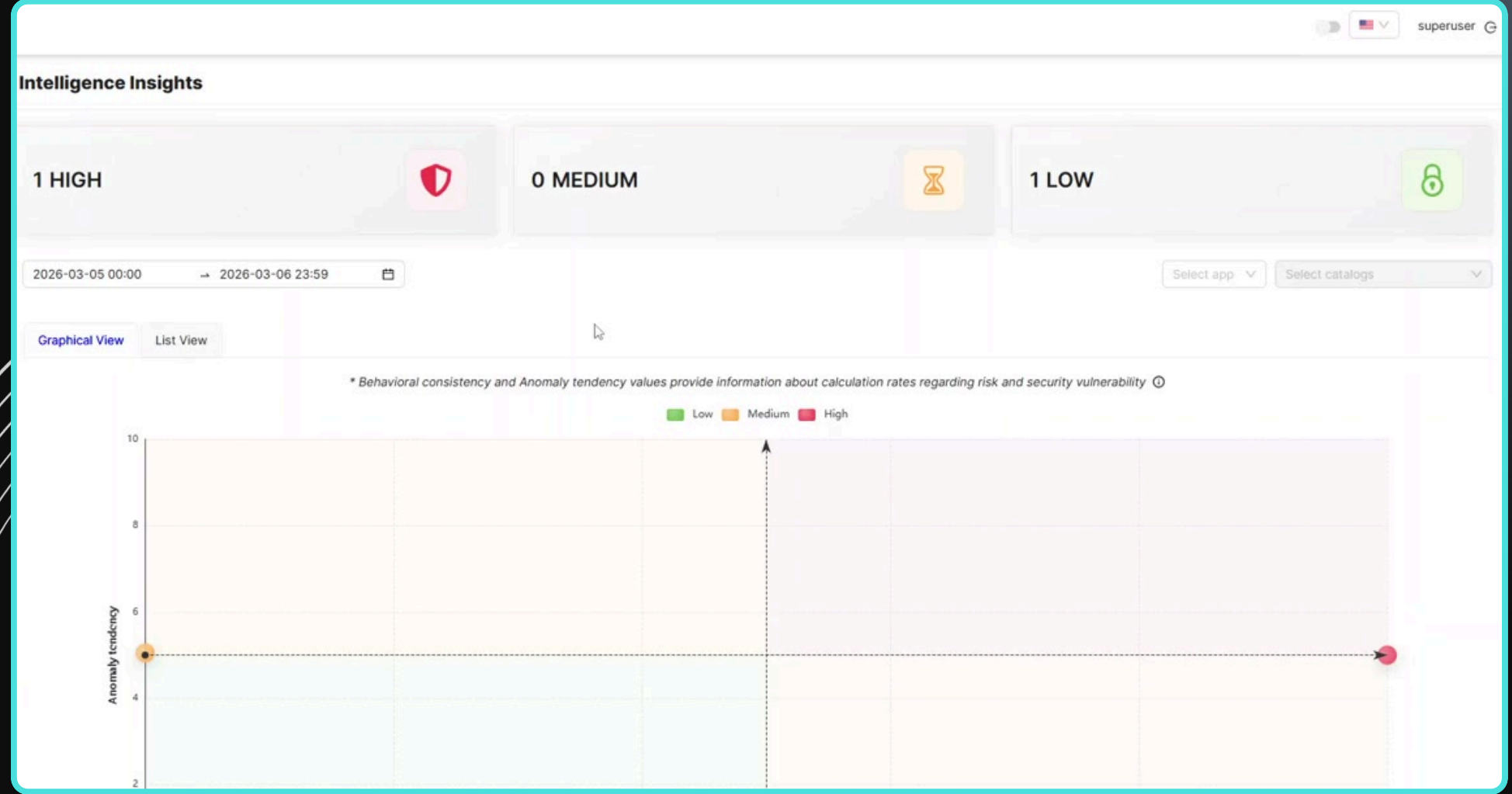
- ✦ Tüm Olayları Listeleme ve Detaylarını Filtreleme: Yöntem, Tıklanma Sayısı, Risk Puanı vb.
- ✦ API Trafik, Saldırı Türleri ve Zafiyetleri Görüntüleme
- ✦ Uygulamaları ve Koleksiyonları Yönetme
  - ✦ Hassas Veri Tanımlarını Yönetme
- ✦ Parametreleri ve Kuralları Yönetme
  - ✦ Swagger URL veya Koleksiyon Dosyası Ekleme



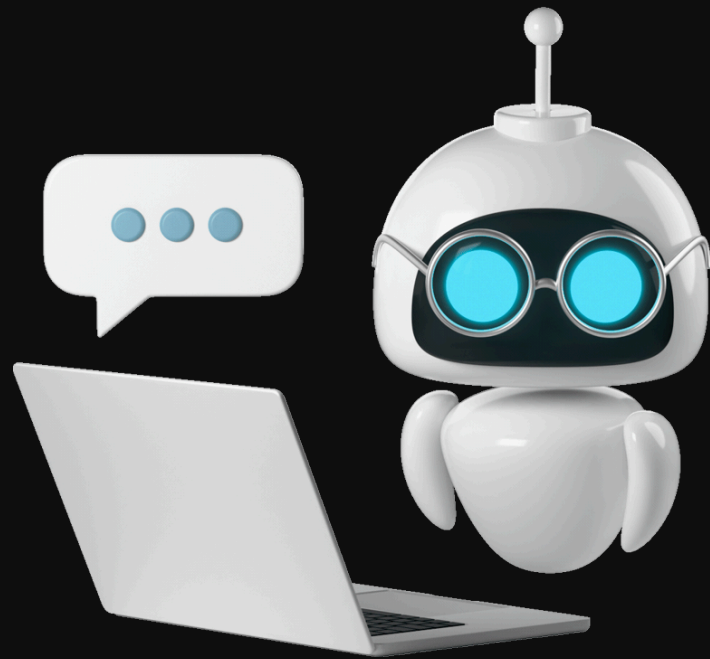
# Intelligence Insights



- ✦ yapay zeka kullanarak API'leri güvence altına alır
- ✦ geleneksel kurallar eklemek yerine, API'lerin kullanım davranışlarını öğrenerek güvenliğini sağlamayı hedefler
- ✦ genel kullanım kalıplarının dışında kalan ve kötü niyetli olabilecek davranışları tespit eder



API



# APIFORT'ta Yenilikler:

## Yapay Zeka Destekli Güvenlik Otomasyonu

### Yapay Zeka Destekli Hassas Veri Tespiti

Doğal dil istemleriyle hassas veri tespiti için regex desenleri oluşturun. Üretilen ifadeleri anında test edin ve en uygun deseni tek tıklamayla uygulayın.

### Yapay Zeka Destekli Veri Maskeleye Yapılandırması

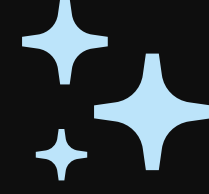
Yapay zeka tarafından oluşturulan regex önerileriyle maskeleye politikalarını daha hızlı oluşturun. Sonuçları gerçek zamanlı olarak doğrulayın ve maskeleye desenlerini doğrudan arayüz üzerinden kullanıma alın.

### Yapay Zeka Destekli Özel Kural Oluşturma

Koruma gereksinimlerinizi doğal dilde tanımlayarak özel güvenlik kuralları oluşturun. Yapay zeka, APIFORT'un kural yapısına uygun kuralları otomatik olarak oluşturarak manuel işlemleri ve yapılandırma karmaşıklığını azaltır.

The screenshot displays the 'AI Regex Assistant' interface. The main window is titled 'AI Regex Assistant' and has a subtitle 'Create regex with artificial intelligence'. Below the title, there is a question: 'What kind of regex do you need?'. Three buttons are visible: 'Write a regex that captures email addresses', 'Write a regex that validates IPv4 addresses', and 'Write a regex that captures HTTP and HTTPS URLs'. A fourth button, 'Write a regex that captures HTTP and HTTPS URLs', is also visible below the main window. A 'Get Suggestions' button is located at the bottom right of the main window. Below the main window, a smaller dialog box is open, titled 'What kind of rule do you need?'. It contains three buttons: 'Generate a rule for detects exposed OpenAPI specification files that reveal internal API structure.', 'Generate a rule for detects SQL injection attempts via query string or URL parameters.', and 'Generate a rule for detects NoSQL injection'. A text input field contains the text 'Generate a rule for detects NoSQL injection'. A 'Get Suggestions' button is at the bottom right of this dialog. Below the dialog, a message states 'AI can make mistakes. Review the generated YAML before using it.' Below this, it says '1 suggestions found'. A single suggestion is shown with the following details: 'id: WEBHOOK\_TRIGGER\_DETECT', 'info:', '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'. At the bottom of the suggestion, there are 'Cancel' and 'Use This Rule' buttons.

# Entegrasyon Yetenekleri





Takımlar Arası İşbirliğini Kolaylaştırın: Mevcut DevOps ve Güvenlik Araçlarınızla API Güvenliğini Kolayca Entegre Edin!




## Evrensel Entegrasyon

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


## SOAR

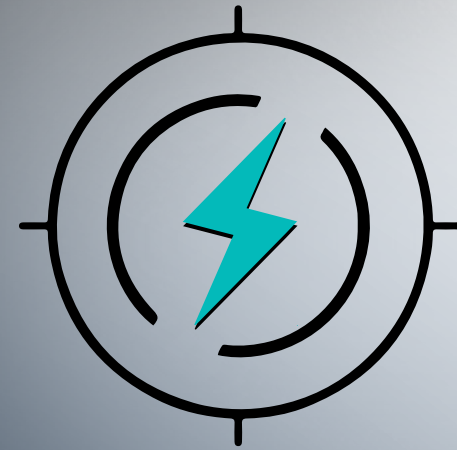
-  Splunk Phantom
-  Cortex XSOAR

## SIEM

-  Splunk SIEM
-  Sumo Logic SIEM
-  IBM QRadar SIEM

## Mesajlaşma Uygulamaları

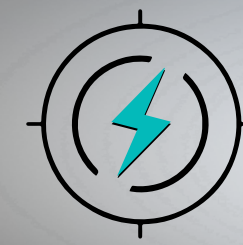
-  Slack
-  MS Teams



# ApiStrike

## ApiStrike ile Tanışın!

ApiStrike, kuruluşların API'lerindeki olası güvenlik açıklarını erken tespit edip gidermelerine yardımcı olmak için tasarlanmış güçlü bir API tarama modülüdür.



# 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

# Yerli Güç, Küresel Vizyon

Apifort, %100 yerli teknolojiyle geliştirilmiş bir API güvenliği platformudur.



## Mevzuat ve KVKK ile Tam Uyum

Yerli altyapı, regülasyonlara uyumu kolaylaştırır.

## Yerel Destek ve Servis

Hızlı müdahale, dil engeli olmadan etkili iletişim ve sürdürülebilir hizmet kalitesi.

## Esnek Geliştirme ve Kuruma Özel Uyum

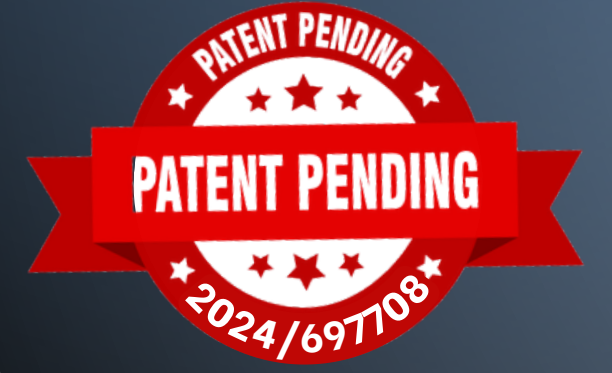
Değişen ihtiyaçlara hızlı yanıt, özelleştirilebilir mimari.

## Veri Güvenliği

Tüm veriler yurtiçinde barındırılır; dışa bağımlılık ve veri sızıntısı riski minimize edilir.

## Hızlı Tedarik ve Proje Süreçleri

Gecikmesiz kurulum, entegrasyon ve destek imkanı.



Zamanınız ve ilginiz için

**Teşekkürler!**