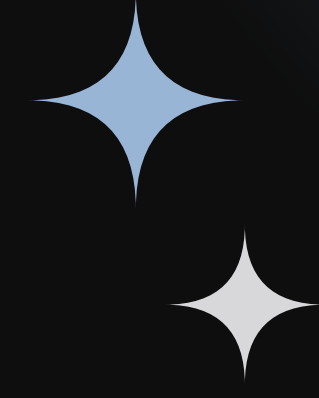




ApiFort

Bağlantıları Koruyun, Geleceği Güvence Altına Alın

APIFORT: API Güvenlik Çözümünüz





Genel Bakış

1

API ve API Güvenliği

2

Pazar Araştırması

3

APIFORT Nedir?

4

APIFORT'un Yetenekleri

5

APIFORT'ta Neler Var?

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 diğer 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.



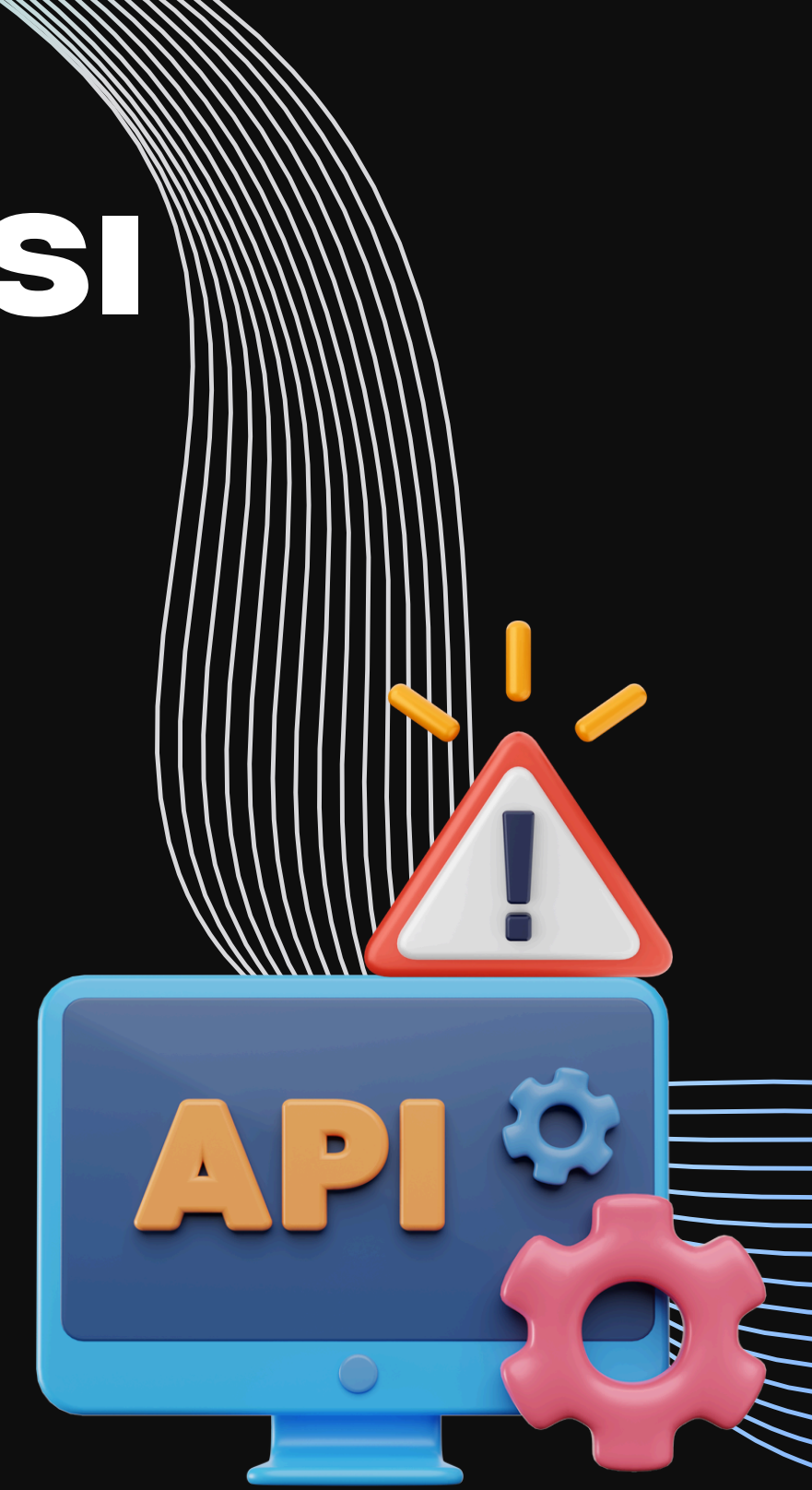
3. **Salesloft – Drift**: Çalınan OAuth kimlikleri, Salesloft API'leri üzerinden kullanılarak Salesforce müşteri verilerinin ele geçirilmesine yol açtı.



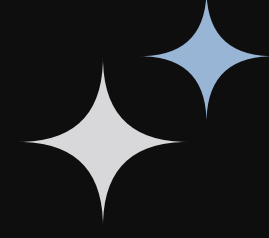
4. **McHire (McDonald's)**: Zayıf yönetici erişimleri ve IDOR açıkları, iş başvurusu yapan adayların verilerinin sızmasına neden oldu.



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

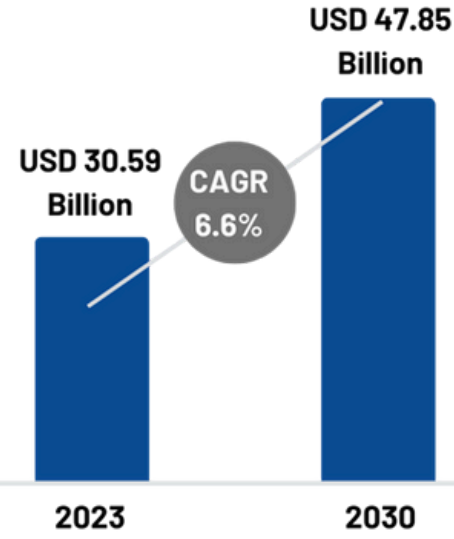


Pazar Arařtırması



GLOBAL API SECURITY MARKET

2024-2030



Virtue Market Research'e g re, K resel API G venlięi Piyasası 30.59 milyar ABD Doları deęerinde.

2030'un sonuna kadar 47.85 milyar ABD Doları piyasa b y kl ę ne ulařması bekleniyor.

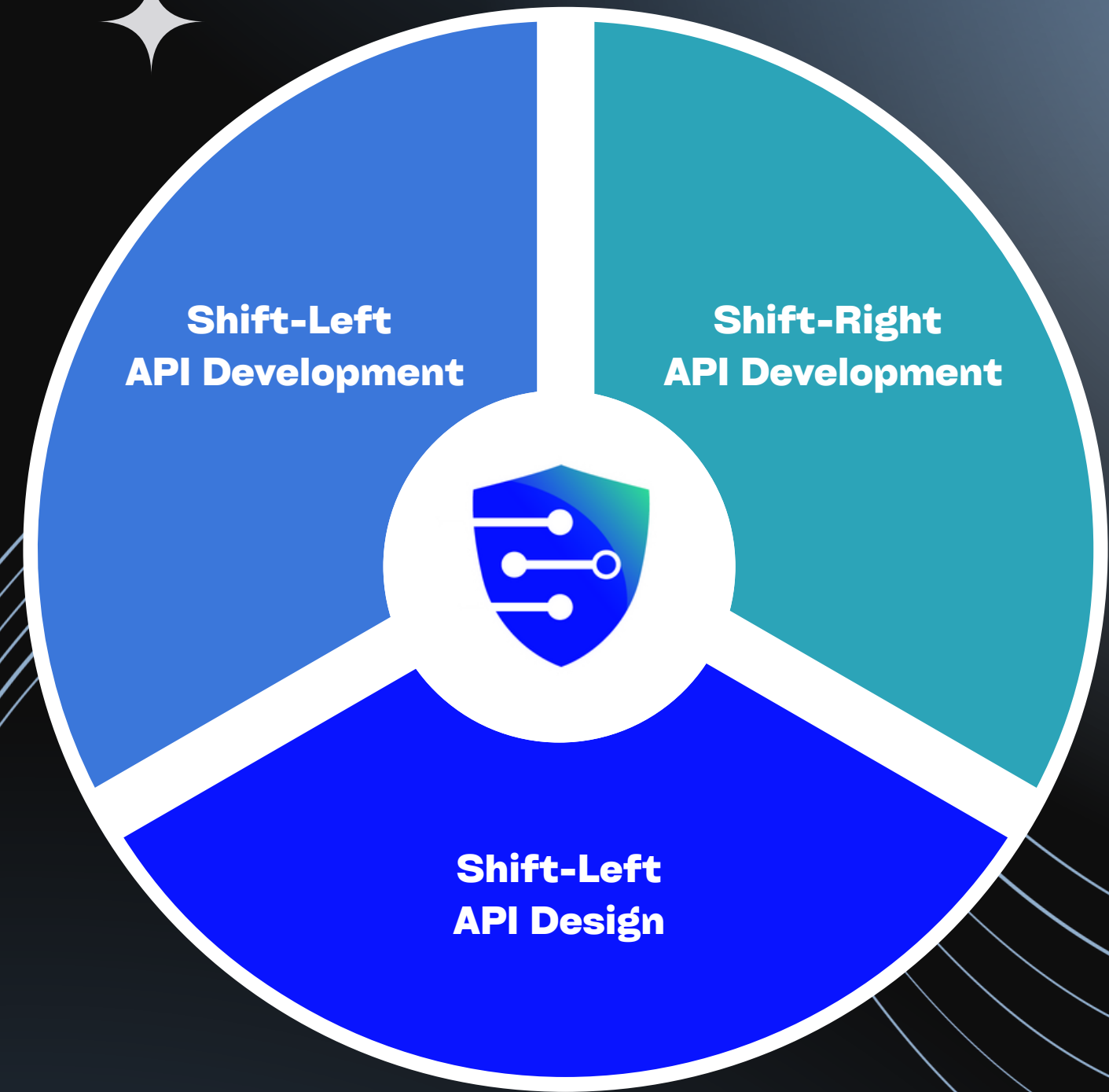
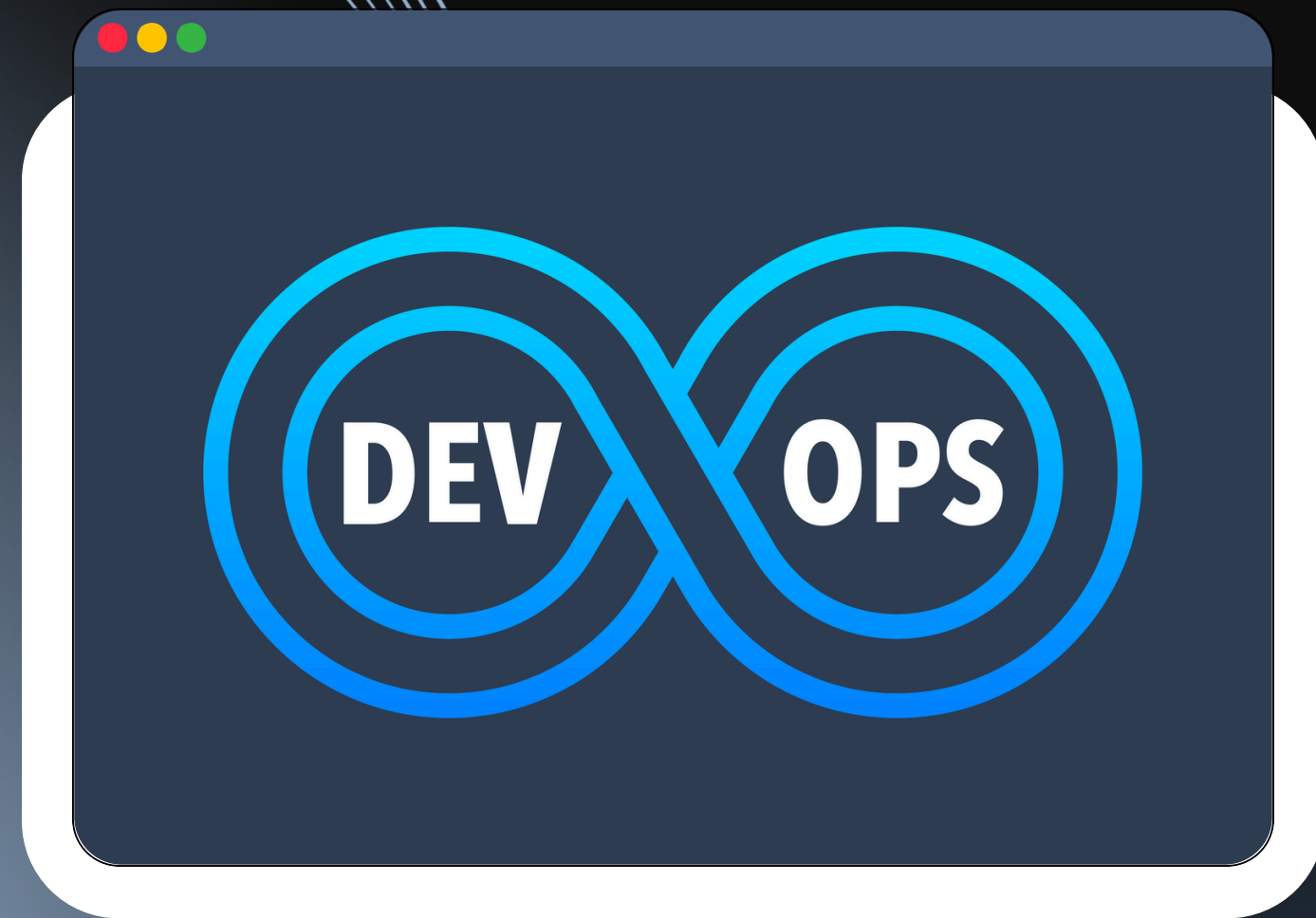
Piyasanın 2024-2030 tahmin d neminde yıllık bileřik b y me oranı (CAGR) %6.6 olarak  ng r l yor.



Pazar Payı



Pazar Ekosistemi



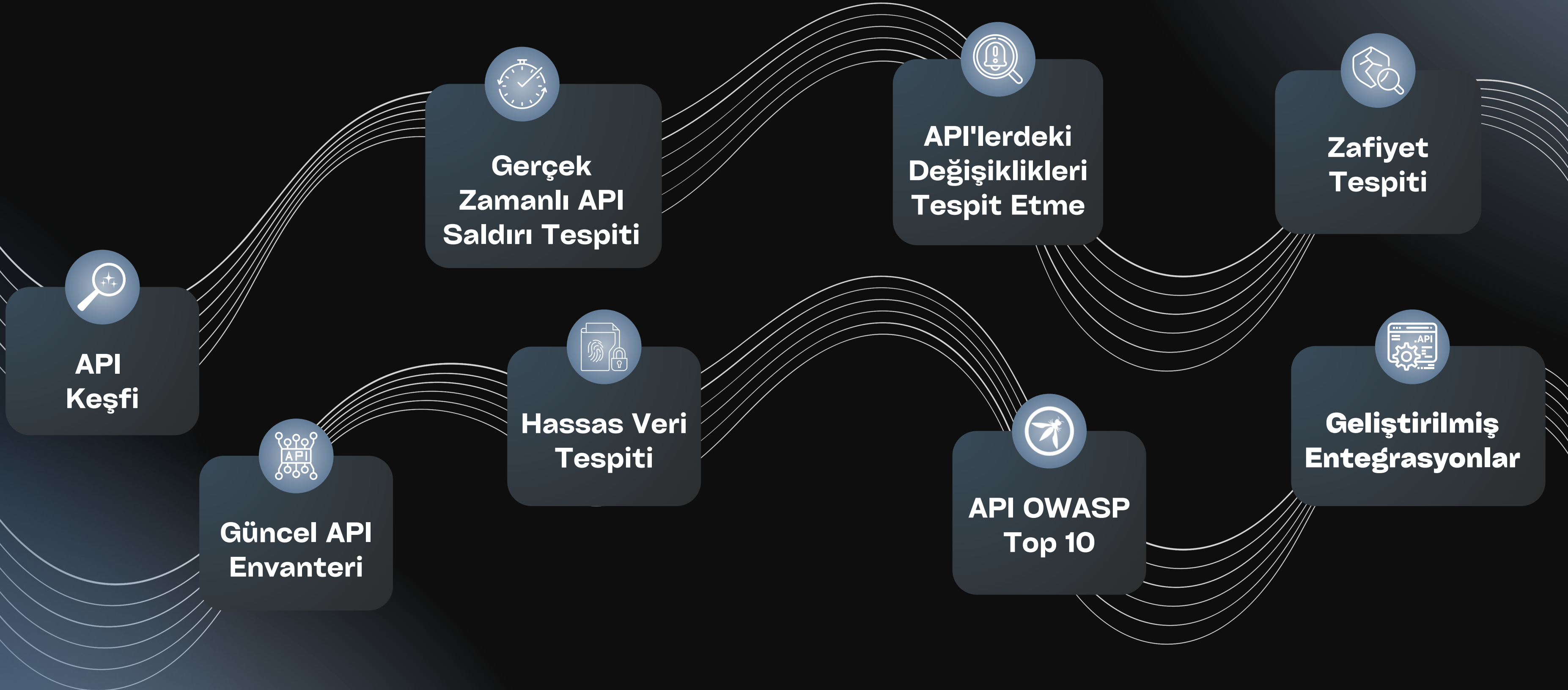


ApiFort Nedir?

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.

ApiFort'un Temel Özellikleri





ApiFort'ta

Neler Var ?



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

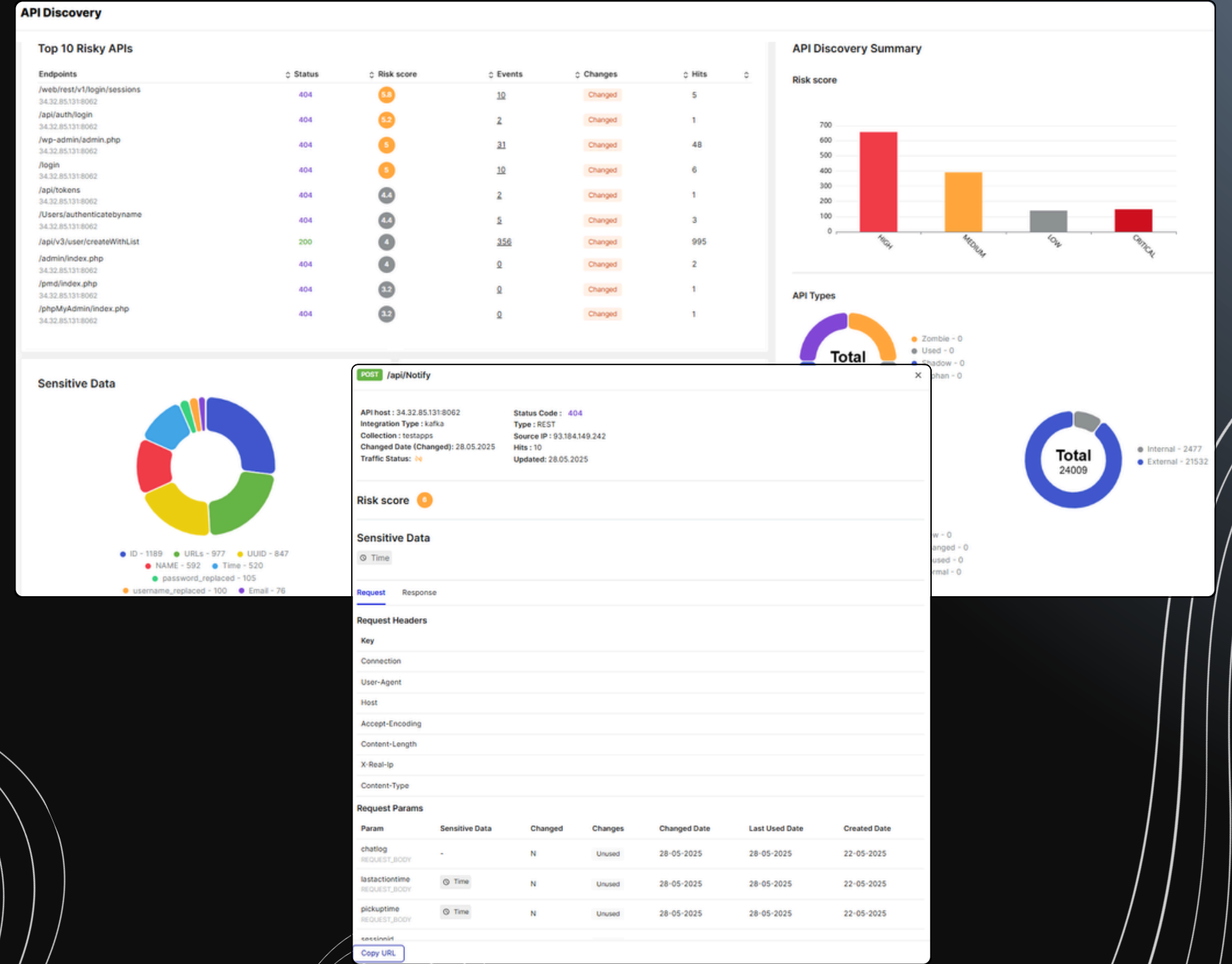
Kullanımı, veri türlerini ve iç/dış erişimi değerlendirme

API Veri Sınıflandırması

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

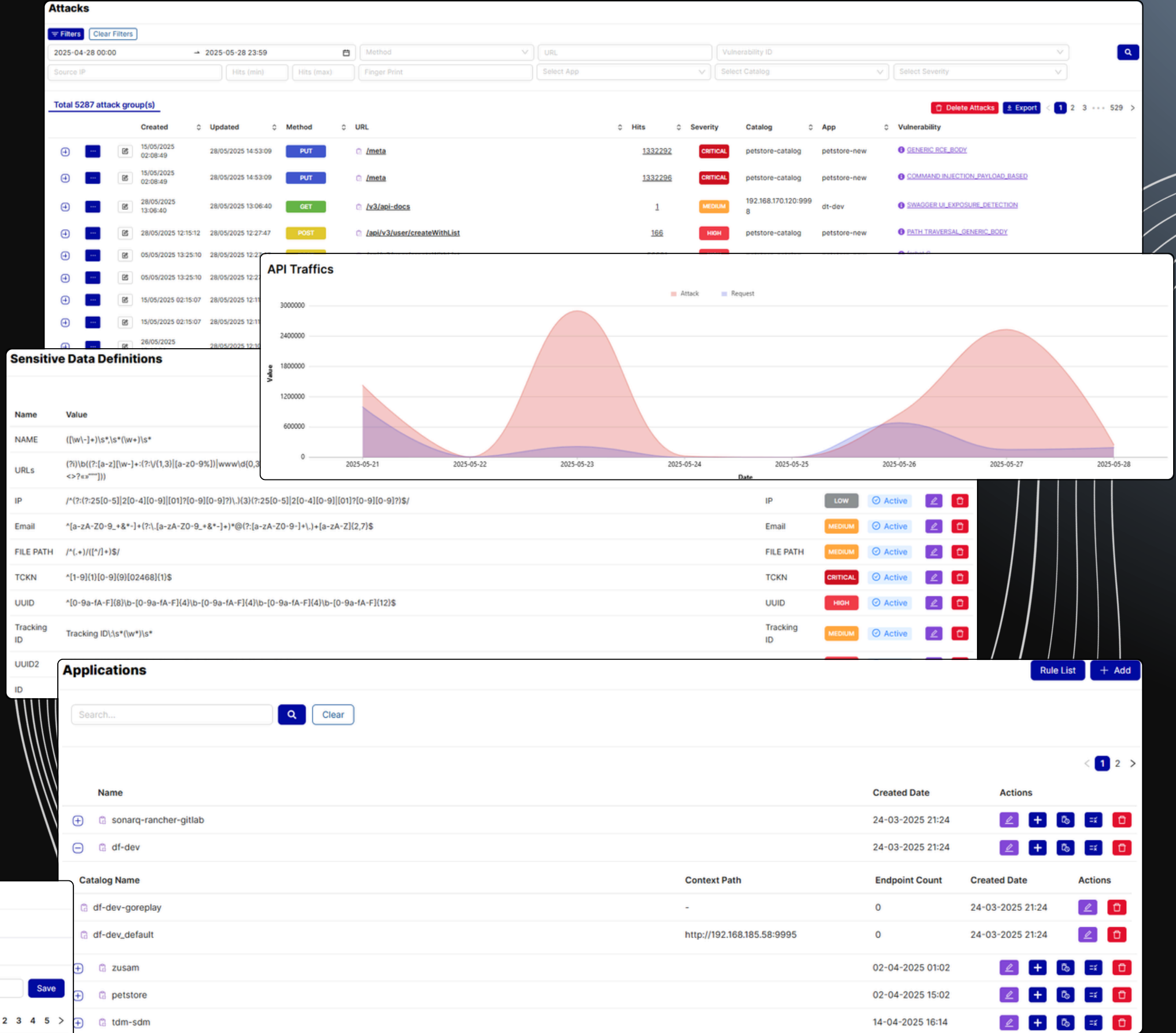
API Drift İzleme ve Bilgilenme

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

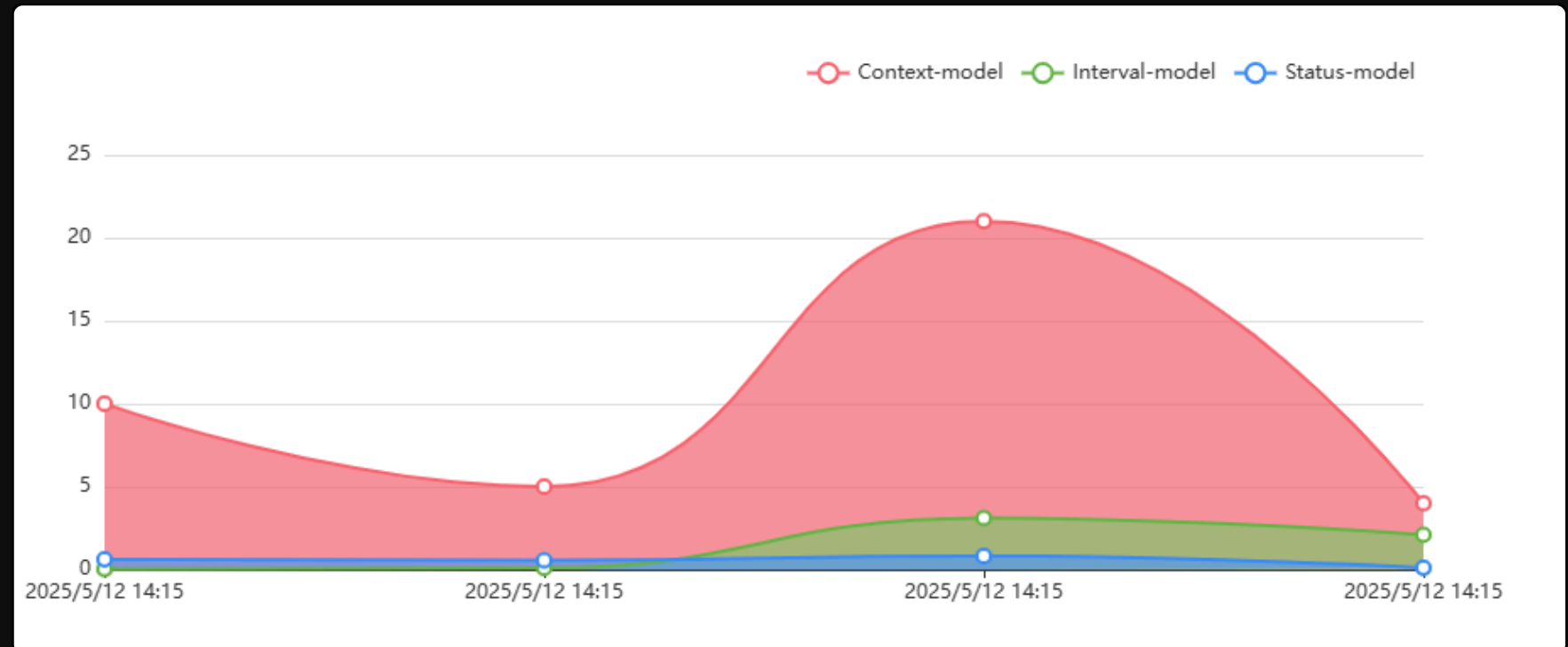
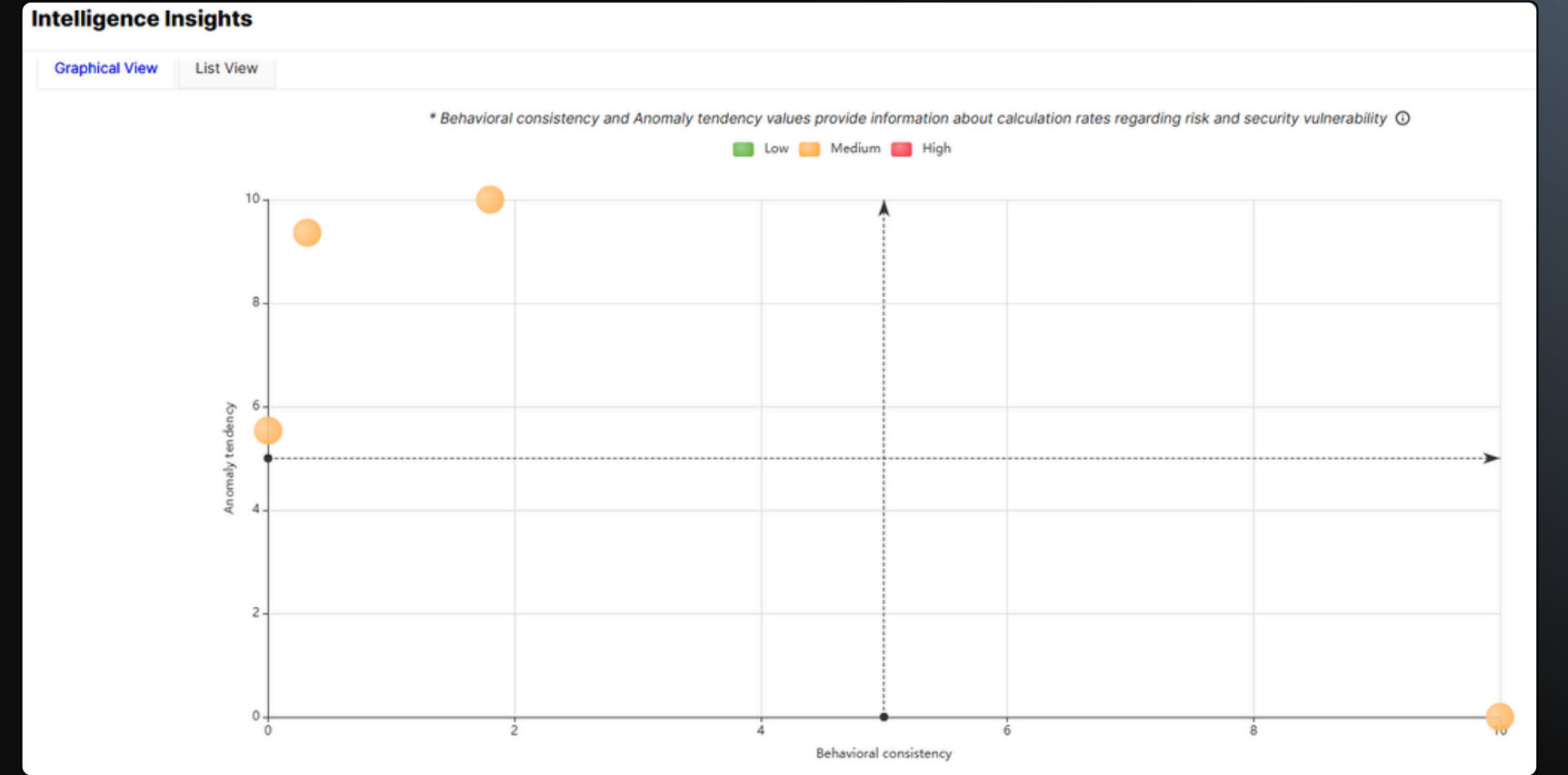
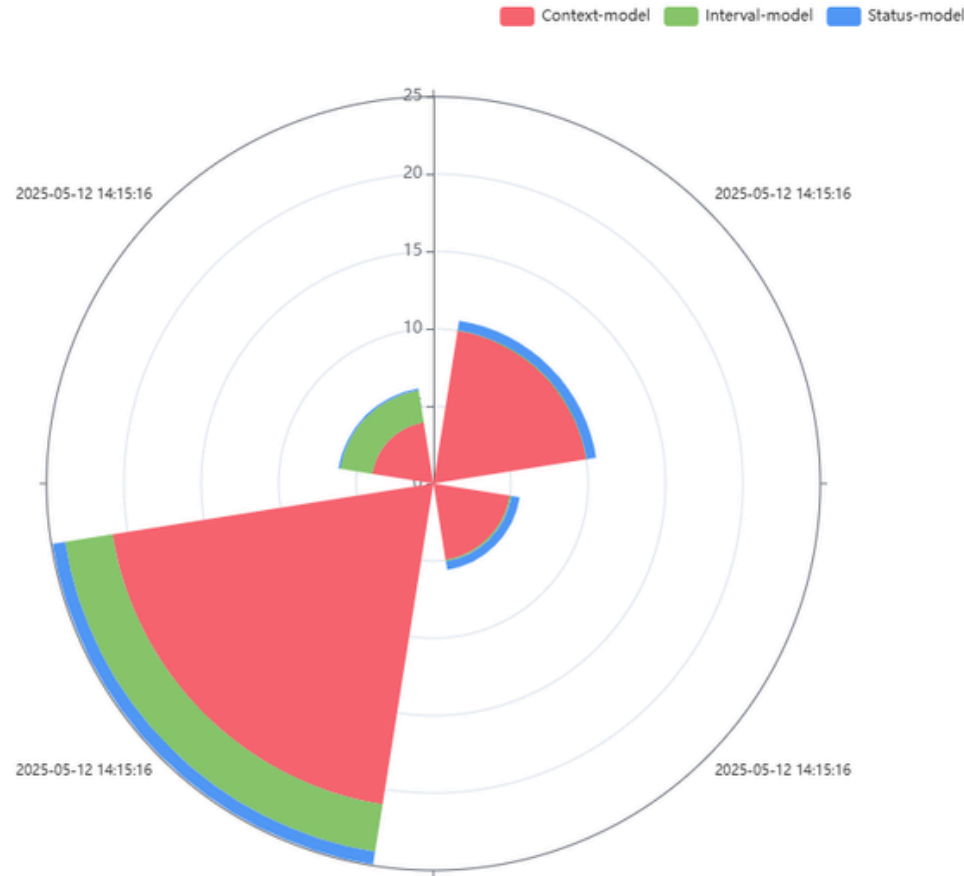


Specifications								
Select Catalog sonarq-rancher-gitlab df-dev zusam petstore tdm-sdm Cloudflare yt-test dt-dev petstore-new jenkins petstore-f5 soap								
Selected Collection: petstore API Specification URL API Specification File URL Prefix (/api/v3) Version (1, 1.1 ...) Description Save								
24 Record History < 1 2 3 4 5 >								
Version	Created Date	Endpoint	Deprecated	Orphan	Shadow	Zombie	Description	
75	24-04-2025 18:24	0	0	19	0	0	75.deneme	
109	29-04-2025 14:29	0	0	19	0	0	109.deneme	
104	29-04-2025 09:29	0	0	19	0	0	104.deneme	

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

Context Anomaly-Checks whether the types and numbers of parameters in the sent request and received response align with the expected usage of the endpoint.
Interval Anomaly-Analyzes the traffic on the endpoint to detect whether the number of requests within a given time frame has reached abnormal levels.
Status Anomaly-Examines the distribution of status codes in the responses returned by the endpoint to identify any irregularities.



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

DevOps Araçları

Yakında CLI desteğiyle birlikte sunulacak

- Atlassian OpsGenie
- Jenkins
- Azure DevOps

SOAR

- Splunk Phantom **Test**
- Cortex XSOAR **Geliştirme**

SIEM

- Splunk SIEM **Test**
- Sumo Logic SIEM
- IBM QRadar SIEM

Mesajlaşma Uygulamaları

- Slack
- MS Teams

Karşılaştırma Matrisi

	on-premise	on-premise	cloud
Özellikler	 ApiFort	 wallarm	 wallarm
OWASP API Top 10 tabanlı saldırı kategorilendirmesi	✓	✓	✓
Müşteri tanımlı imzalar	✓	✓	✓
Mikro brute force tespiti	✓	✓	✓
BOLA (Yetkisiz Nesneye Erişim) koruması	✓	✓	✗
Kimlik bilgisi doldurma (Credential Stuffing) tespiti	✓	✓	✓
Zafiyet analizi	✓	✗	✓
API spesifikasyonu karşılaştırması ve zombie/shadow API tespiti	✓	✓	✓
Özelleştirilebilir hassas veri tespiti	✓	✓	✓
Özelleştirilebilir hassas veri maskeleyme	✓	✓	✓

Karşılaştırma Matrisi

	on-premise	on-premise	cloud
Özellikler	 ApiFort	 wallarm	 wallarm
API risk skrolama	✓	✗	✗
API keşfi	✓	✗	✓
API imza değişikliği tespiti	✓	✓	✓
SIEM/SOAR entegrasyonları	✓	✓	✓
SSO (Tekli Oturum Açma) desteği	✓	✗	✗
Rol tabanlı erişim kontrolü (RBAC)	✓	✗	✗
Multi-tenant	✓	✓	✓
Yanlış pozitif işaretleme	✓	✓	✓
Çoklu odaklı gösterge panelleri	✓	✓	✓
Yapay zeka tabanlı Anomali Tespiti	✓	✗	✗

Karşılaştırma Matrisi

	on-premise	on-premise	cloud
Özellikler	 ApiFort	 wallarm	 wallarm
Bulut sağlayıcı trafik desteği (AWS, Azure, GCP)	✗	✗	✓
Çeşitli API trafik alma yöntemleri (F5, Nginx, Mirror, Doğrudan vb.)	✓	✓	✓
REST, SOAP, GraphQL API işleme	✓	✓	✓
API zafiyet tarayıcısı	✓	✗	✓
Trafik içi (in-line) destek	✗	✓	✓
WAF özellikleri	✗	✗	✓
API kötüye kullanımının önlenmesi	✗	✗	✓
Trafik içi (in-line) virtual patching	✗	✗	✓
IP beyaz listeye alma, kara listeye alma ve gri listeye alma	✗	✗	✓
API oturum yönetimi	✓	✗	✓



ApiFort

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 API'lerinizi Nasıl Korur?



API'leri tespit eder

Farklı ortamlar arasında Swagger URL/dosya seçeneklerini kullanarak API'leri tespit eder.

01



Özelleştirilebilir güvenlik taramaları yapar

Önceden tanımlı kuralları uygular. Kullanıcıların mevcut kuralları değiştirmesine veya yeni kurallar eklemesine olanak tanır.

02



Zafiyetleri açığa çıkarır

Endpoint'lerdeki kritik zafiyetleri gösterir.

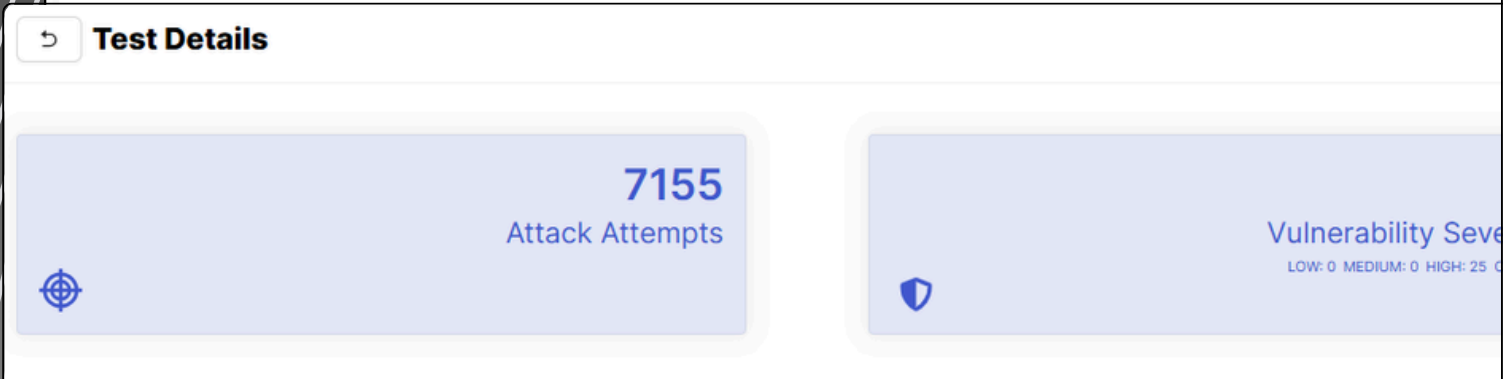
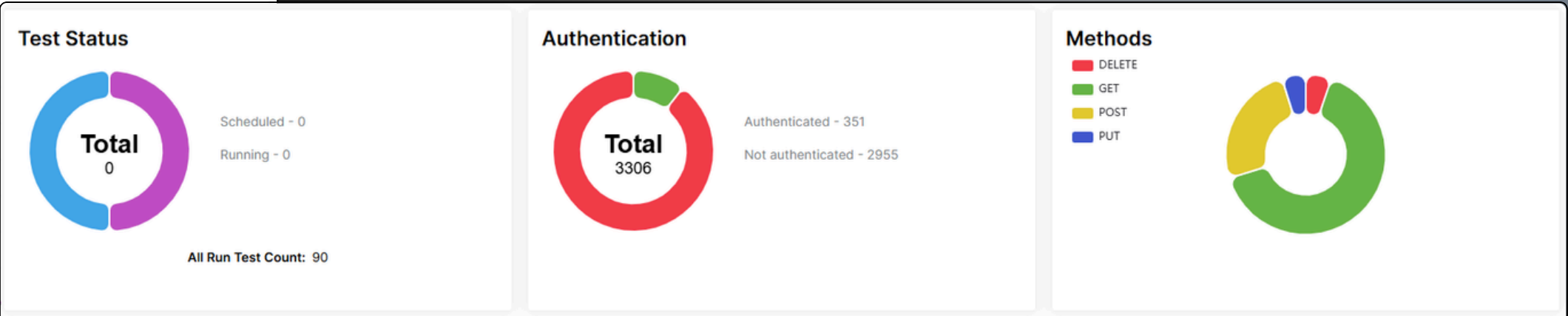
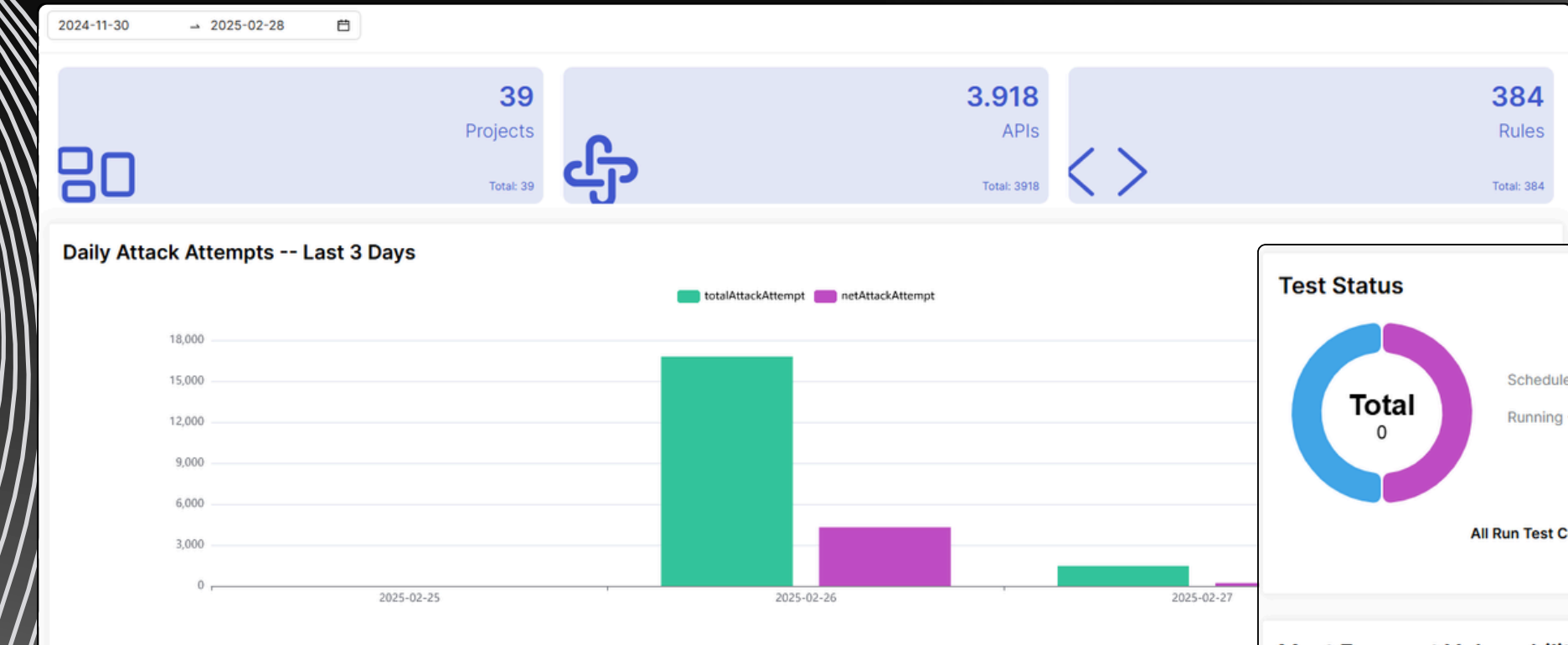
03



Güvenliği erken aşamada güçlendirir

API yaşam döngüsünü daha güvenli hale getirmek için, erken aşamada düzeltme yapılmasına olanak tanır.

04



Most Frequent Vulnerabilities

Vulnerability Type
CORS MISCONFIGURATION INVALID ORIGIN
HSTS SECURITY DETECTION
IDOR ATTACK URL BASED
IDOR ATTACK PAYLOAD BASED
DESCRIPTIVE ERROR MESSAGE INVALID PAYLOAD
PII SENSITIVE DATA LEAK

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

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

	Count
PUT - http://34.32.50.251:9090/api/pet	604
	494
	179
	109
	11
	10

Vulnerabilities Attack Attempts Endpoints

Method URL Vulnerability 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	

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

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!