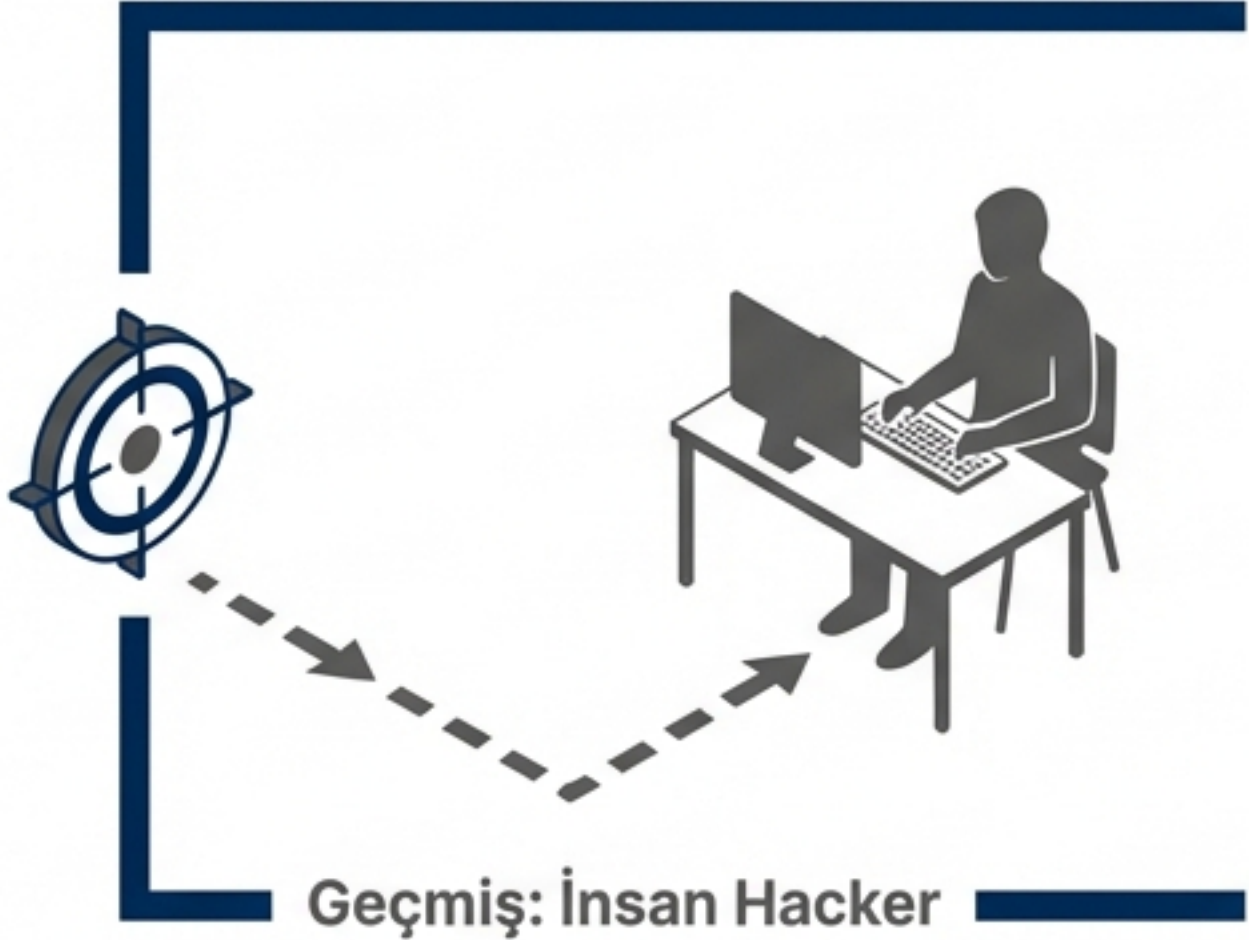


# **AEGRIX: YAPAY ZEKA AĐINDA OTONOM SAVUNMA**

Agentic AI Saldırılarına Karşı Davranışsal Güvenlik Kalkanı

# Saldırının Evrimi: İnsan Hızından Makine Hızına



## Keşif (Reconnaissance)

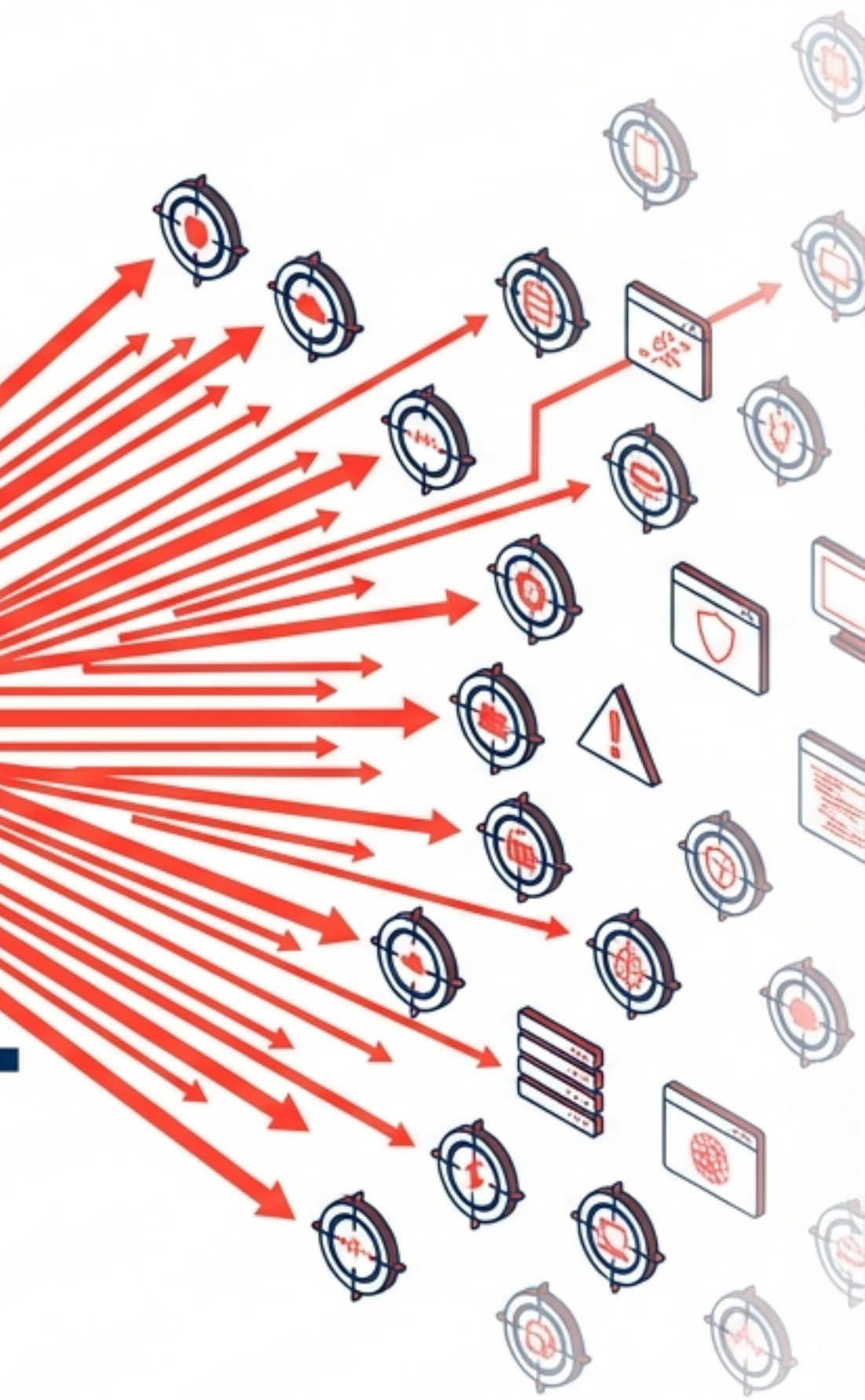
Manuel taramadan tam otonom zayıf nokta tespitine geçiş.

## Hız (Velocity)

İnsan reaksiyon süresini aşan, milisaniyeler içinde gerçekleşen operasyonlar.

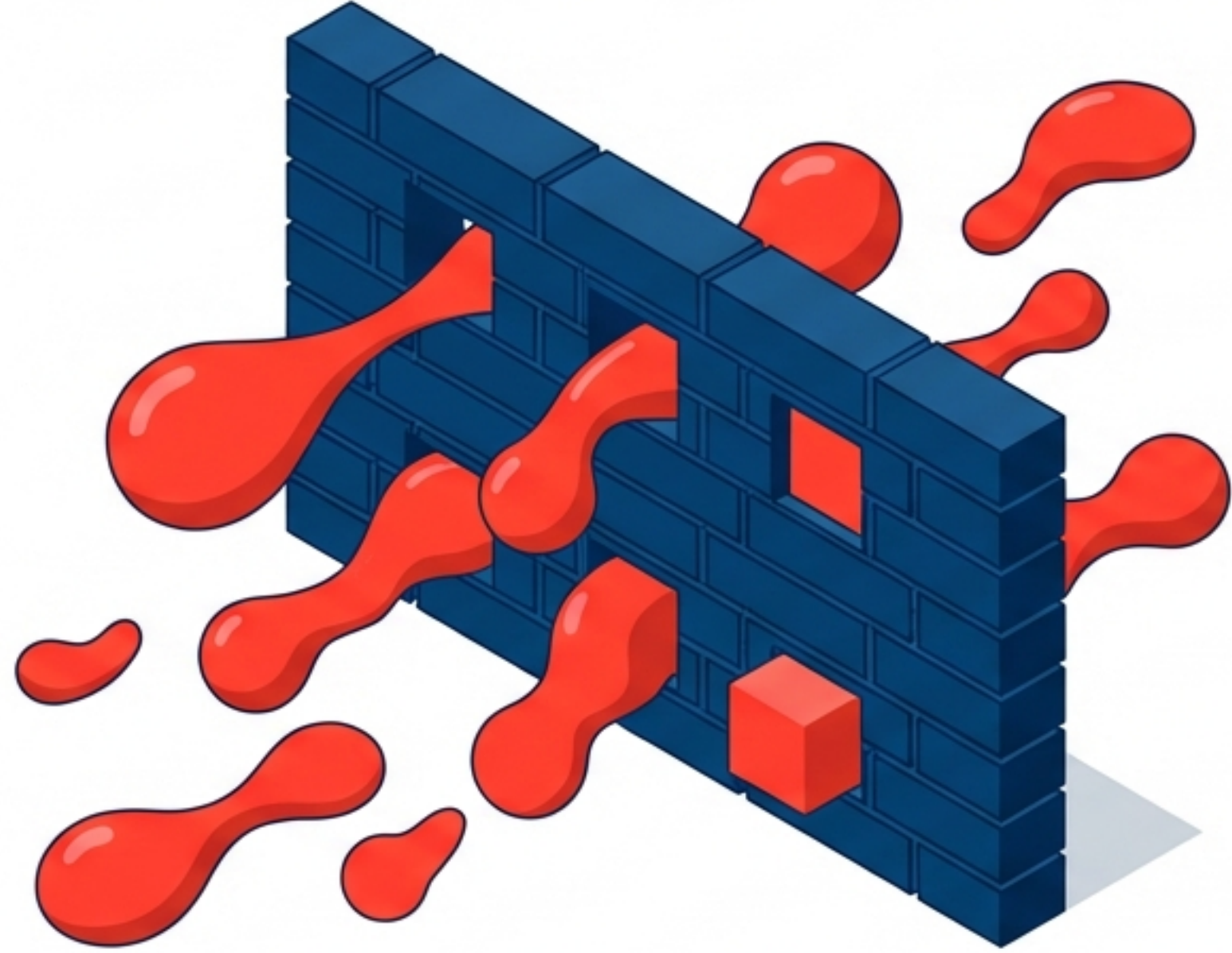
## Varyasyon

Saldırı yüzeyinde sürekli değişen, dinamik saldırı zincirleri.



# Statik Kalkanların Çöküşü

İmza Tabanlı Güvenlik Neden Yetersiz Kalıyor?



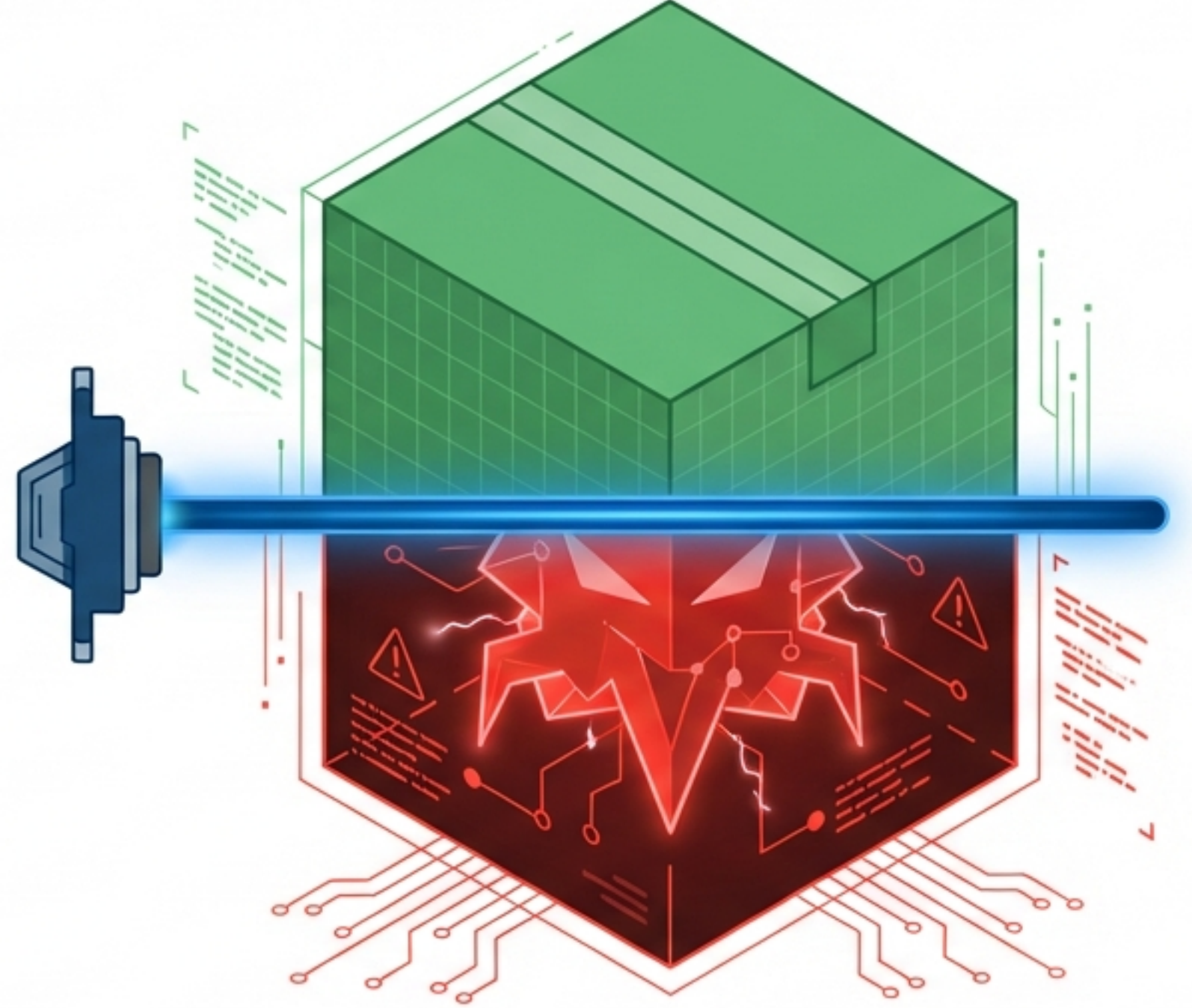
- **Payload Mutasyonu:** Yapay zeka, kötü amaçlı kodları sürekli değiştirerek Regex ve statik kuralları atlatır.
- **Kural Tabanlı Körlük:** Sabit filtreler, dinamik ve bağlamsal saldırı davranışlarını göremez.
- **Sonuç:** Sadece yükü (payload) kontrol eden sistemler, niyeti (intent) kaçıır.

# Aegrix Yaklaşımı: Niyeti Tespit Etmek

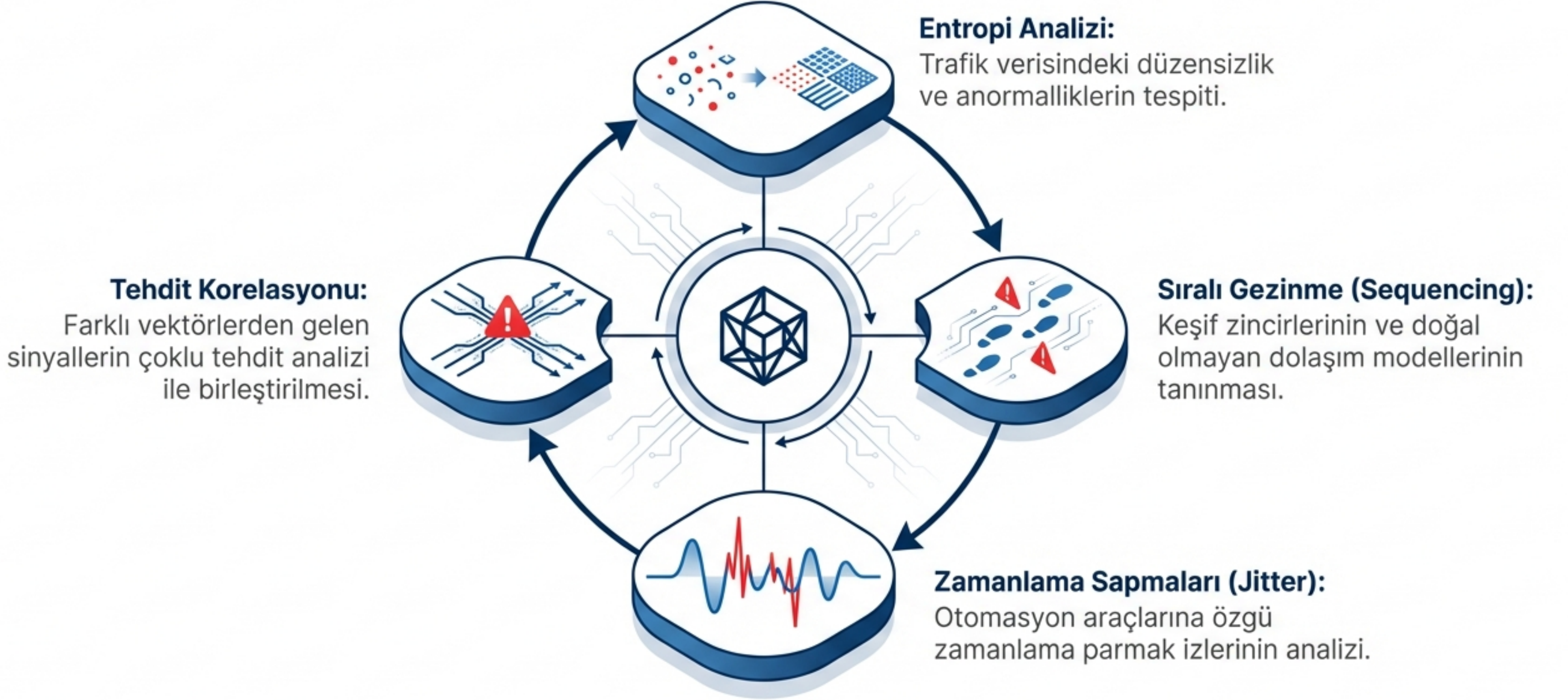
Aegrix, içeriğe değil davranışa odaklanır.

Saldırganın kullandığı araçlar değişse bile, saldırı niyeti ve yöntemleri parmak izi bırakır.

'Autonomous Behavioral Defense'  
(Otonom Davranışsal Savunma) ile **statik kurallara ihtiyaç duymadan koruma sağlar.**



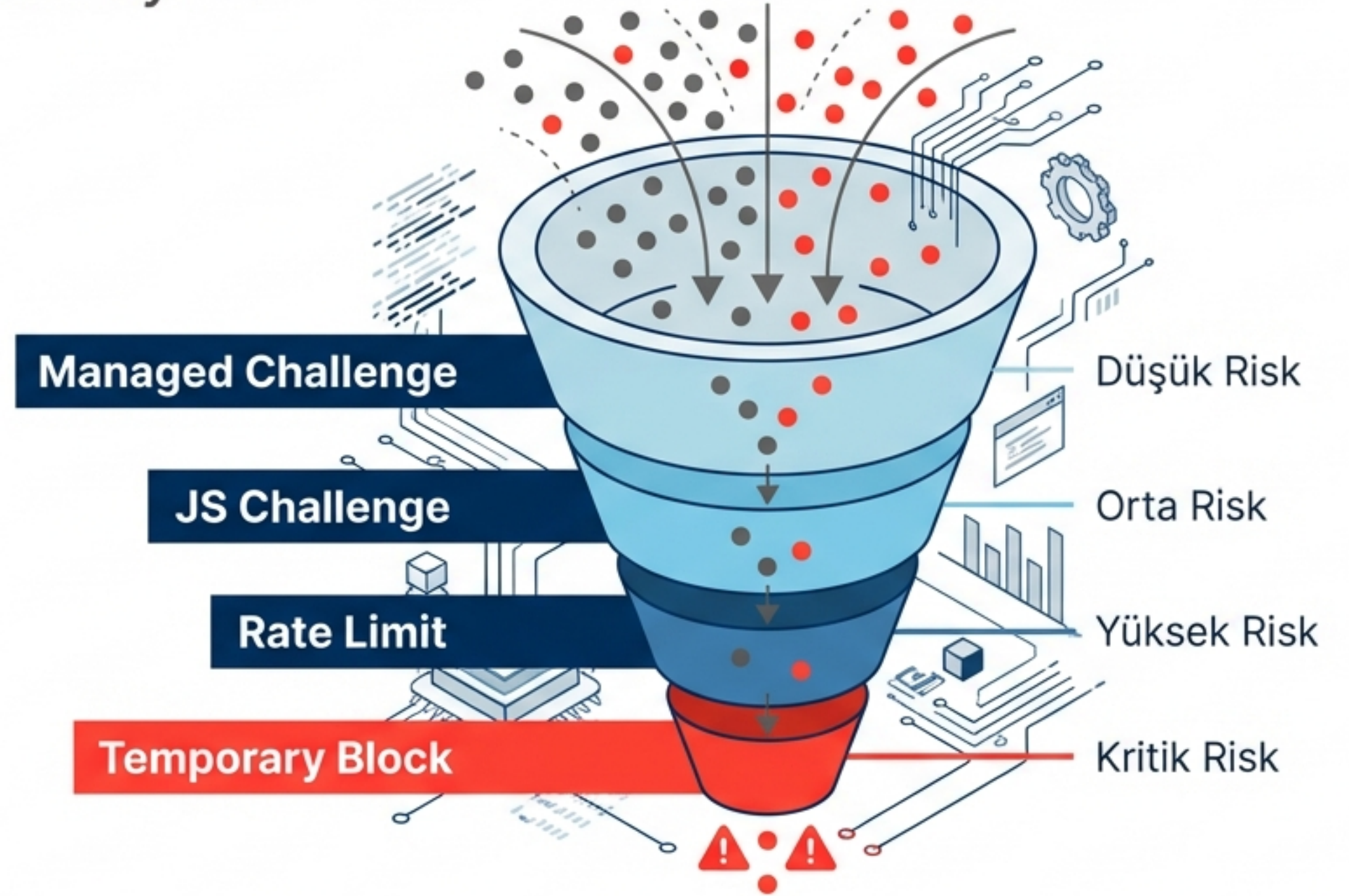
# Davranışsal Savunma Modeli



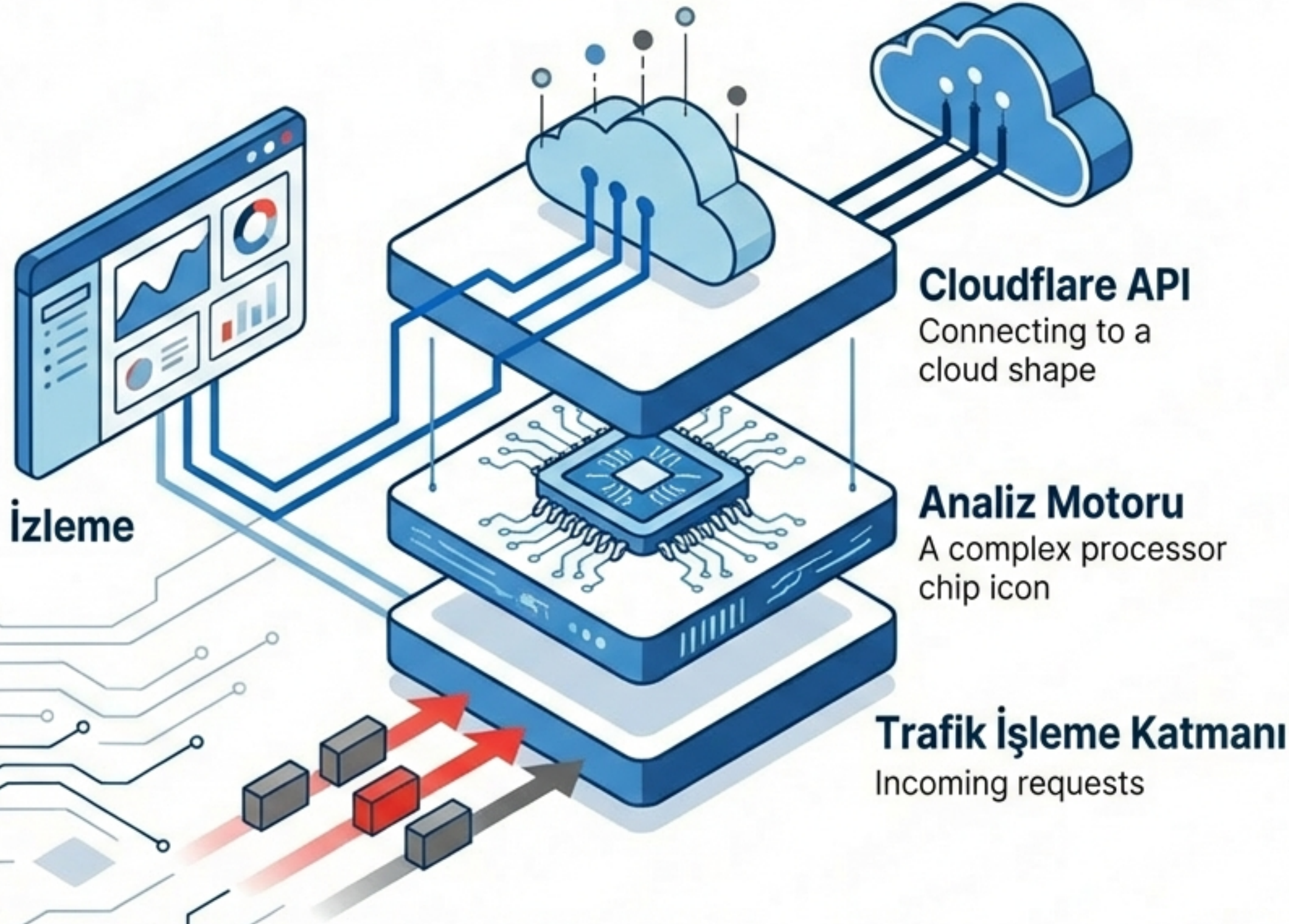
# Adaptif Tepki Mimarisi

## Risk Tabanlı Otomatik Eskalasyon

Sistem, tehdit skoruna göre tepki dozajını otomatik ayarlar.



# Teknik Mimari ve Entegrasyon



- **Trafik İşleme Katmanı:** Gelen isteklerin gerçek zamanlı analizi.
- **Analiz Motoru:** Davranışsal modellerin işletildiği çekirdek yapı.
- **Cloudflare API:** Tehditlerin ağ ucunda (Edge) durdurulması için doğrudan entegrasyon.
- **İzleme:** Şeffaf raporlama ve anlık durum paneli.

# Esnek Kurumsal Dağıtım



- **Docker-Ready:** Konteyner mimarisi ile her ortamda hızlı kurulum.
- **Hibrit Yapı:** Hem Bulut (Cloud-native) hem de On-Premise (Yerel Sunucu) dağıtım seçenekleri.
- **Multi-Tenant:** SaaS uyumluluğu ile ölçeklenebilir altyapı.

# Stratejik Vizyon: Yapay Zeka Savaş Alanı



- **AI vs. AI:** Yapay zeka tabanlı saldırıları ancak yapay zeka tabanlı bir savunma durdurabilir.
- **Sıfır Statik Güvenlik:** Statik kuralların tamamen terk edildiği, %100 dinamik bir savunma prensibi.
- **Sürekli Öğrenme:** Saldırı teknikleri değiştikçe kendini geliştiren adaptif yapı.

# Küresel Tehdit Hafızası

- Bir noktada tespit edilen yeni bir saldırı davranışı, tüm ağ için anında bir savunma zekasına dönüşür.
- Coğrafi ve sektörel tehdit verilerinin gerçek zamanlı korelasyonu.
- Saldırganlar için “saklanacak yer yok” prensibi.



# Web & API Güvenliğinde Yeni Standart

- Siber güvenlikte bir paradigma değişimi gerçekleşmiştir.
- Aegrix, makine hızındaki düşmanlara karşı gerekli olan davranışsal ve otonom savunma katmanını sağlar.
- Güvenlik artık statik bir duvar değil, yaşayan ve düşünen bir organizmadır.



# İletişime Geçin

**MUZAFFER ULUSOY**  
**ulusoydigital@gmail.com**  
**demo.ulusoydigital.com**

