DeviceTrust Nedir?

Ürünlerimiz > Bilgi Güvenliği

DeviceTrust™

Device Trust, mobil ve web uygulamalarınızı cihaz seviyesinden API uç noktasına kadar koruyan bütünleşik bir güvenlik katmanıdır. Donanım tabanlı parmak iziyle SIM Swap saldırılarından sofistike bot faaliyetlerine, tersine mühendislik girişimlerinden malware kaynaklı kritik kayıplara kadar uzanan geniş bir tehdit yelpazesine karşı uçtan uca bir güvenlik kalkanı sağlar. Karmaşık siber saldırıları henüz kullanıcı cihazındayken durdurur; kurumsal itibarınızı ve kullanıcı güvenliğini en üst seviyede koruma altına alır.

Kimler için Uygun?

Device Trust, dijital varlıklarını korurken operasyonel maliyetlerini optimize etmek isteyen, **yüksek güvenlik standartlarını hedefleyen tüm profesyonel yapılar için tasarlanmıştır.**

- **Finansal Kurumlar ve Fintech'ler:** Mobil bankacılık ve ödeme sistemlerinde **SIM Swap**, hesap ele geçirme (ATO) ve malware saldırılarını kaynağında **durdurur.** Finansal dolandırıcılık risklerini minimize ederek kurum itibarını **korur.**
- **Mobil Uygulama ve Oyun Geliştiricileri:** Uygulamanın klonlanmasını, modifiye edilmesini veya hile (cheat) araçlarıyla manipüle edilmesini **önler.** Fikri mülkiyetinizi ve uygulama içi ekonominizi tersine mühendislik girişimlerine karşı **korur.**
- **Kripto Varlık ve Dijital Cüzdan Platformları:** Cüzdan oturumlarını fiziksel cihaza kriptografik olarak **mühürler.** Anahtar hırsızlığı ve yetkisiz erişim denemelerini donanım tabanlı parmak izi teknolojisiyle imkansız hale **getirir.**
- **E-Ticaret ve Pazaryerleri:** Botları, sahte kullanıcı kayıtlarını ve veri kazıma (scraping) girişimlerini **engeller.** Kullanıcı deneyimini bozmadan sadece gerçek müşterilerin sisteme erişmesini **garanti eder.**
- **Büyük Veri ve SaaS Sağlayıcıları:** Hassas verilerin (PII) sızdırılmasını ve API uç noktalarının suistimal edilmesini **engeller.** Modüler yapısı sayesinde, her ölçekteki işletme için ekonomik ve sürdürülebilir bir güvenlik altyapısı **inşa eder.**

CORE SDK

Device Trust - CORE Paketi, Mobil uygulamanızı tersine mühendislik girişimlerine ve ortam manipülasyonlarına karşı koruma altına alır. Root, Jailbreak, emülatör ve hooking gibi bilinen tüm riskleri gerçek zamanlı tespit ederek saldırı yüzeyini daraltır. Uygulamanın orijinalliğini ve bütünlüğünü doğrularken; cihaz eşleştirme ve ekran güvenliği özellikleriyle dolandırıcılığı önler, böylece uygulamanızın sadece güvenli ve yetkilendirilmiş cihazlarda çalışmasını garanti eder.

Root / Jailbreak Tespiti

Cihazın işletim sistemi üzerindeki en yüksek yetki seviyelerine erişilip erişilmediğini kontrol eder. Root veya jailbreak işlemleri, cihazın yerleşik güvenlik protokollerini devre dışı bıraktığı için, uygulamanızın güvenli olmayan ve savunmasız bir ortamda çalıştırıldığını tespit ederek olası veri sızıntılarını ve yetkisiz erişimleri raporlar.

Hata Ayıklayıcı Tespiti

Uygulamanın bir hata ayıklayıcı (debugger) aracıyla çalıştırılıp çalıştırılmadığını tespit eder. Saldırganlar genellikle uygulamanın çalışma zamanındaki davranışlarını izlemek, hassas verileri bellekte okumak veya kod akışını manipüle etmek için bu modu kullandığından, aktif hata ayıklama oturumlarını tespit ederek engeller.

Emülatör / Simülatör Tespiti

Uygulamanın gerçek bir fiziksel cihaz yerine, saldırıların daha kolay modellenebildiği sanal bir ortamda (emülatör veya simülatör) çalıştırıldığını belirler. Bot çiftlikleri ve otomatik saldırı araçları genellikle emülatörleri tercih ettiği için, bu özellik sahte cihaz trafiğini ayırt etmenize olanak tanır.

Kanca Tespiti

Frida veya Xposed gibi dinamik analiz çerçevelerinin (Hook Detection) varlığını tespit eder. Bu araçlar, uygulama çalışırken fonksiyonların arasına girerek iş mantığını değiştirebilir veya şifrelenmemiş verileri okuyabilir; bu özellik, çalışma zamanındaki bu tür yetkisiz müdahaleleri anında yakalar.

DeviceTrust

Ürünlerimiz > Bilgi Güvenliği

Manipülasyon Tespiti

Uygulama bütünlüğü, dijital imzasının, paket adının veya orijinal yüklendiği mağaza bilgisinin herhangi bir değişikliğe uğrayıp uğramadığını kontrol ederek sağlanır. Bu özellik, zararlı kod enjeksiyonu veya korsan sürüm oluşturma gibi uygulama manipülasyonlarını (tampering) tespit ederek, uygulamanın bütünlüğünün bozulmadığından emin olur.

Korsan Yazılım Tespiti

Uygulamanın yetkisiz kişilerce kopyalanıp kopyalanmadığını anlamak için BundleID ve TeamID doğrulaması yapar. Saldırganların uygulamanızı indirip, kodunu değiştirerek kendi hesaplarına yönlendirecek şekilde yeniden paketleyip dağıtmasını engeller; böylece finansal kayıpların ve marka itibarının zedelenmesinin önüne geçer.

Sistem VPN Tespiti

Cihazda trafiği yönlendiren aktif bir sistem VPN bağlantısı olup olmadığını belirler. Kötü niyetli VPN profilleri, uygulama trafiğini izleyebilir veya manipüle edebilir; bu özellik, ağ trafiğinin güvenilmeyen bir tünelden geçip geçmediğini tespit ederek ağ güvenliğini denetler.

Ekran Kaplama Tespiti

"Cloak & Dagger" saldırılarına karşı, uygulamanın üzerine çizilen şeffaf veya sahte ekran katmanlarını (overlay) tespit eder. Kullanıcının aslında görmediği bir butona tıklamasını sağlayan veya sahte bir giriş ekranıyla şifrelerini çalan bu saldırı türünü engelleyerek kullanıcı etkileşimini korur.

Cihaz Kilidi

Kullanıcının cihazında PIN, desen, parmak izi veya yüz tanıma gibi bir ekran kilidi güvenlik önleminin aktif olup olmadığını kontrol eder. Cihazın fiziksel güvenliğinin sağlanmadığı durumlarda uygulamanın hassas işlemler yapmasını kısıtlamak için kritik bir veri noktası sağlar.

Erişilebilirlik İzinleri İstismarı

Görme engelliler için tasarlanan erişilebilirlik servislerinin, kötü niyetli yazılımlar tarafından ekranı okumak, tuş vuruşlarını kaydetmek veya kullanıcı adına tıklama yapmak için kullanılmasını engeller. Bu izinlerin yetkisiz veya şüpheli kullanımını tespit ederek veri hırsızlığı ve dolandırıcılık riskini minimize eder.

Yükleme Kaynak Analizi

Uygulamanın Google Play veya App Store gibi güvenilir resmi mağazalar dışından yüklenip yüklenmediğini kontrol eder. Alternatif marketlerden veya doğrudan dosya paylaşımıyla yüklenen uygulamalar, güvenlik denetimlerinden geçmediği için yüksek risk taşır; bu özellik kaynağı belirsiz yüklemeleri tespit eder.

Cihaz Eşleştirme

Uygulama bulunduğu fiziksel cihaza kriptografik yöntemlerle eşler (Device Binding). Bu işlem, uygulamanın kopyalanıp başka bir cihaza taşınmasını veya klonlanmış bir sürümünün farklı bir ortamda çalıştırılmasını imkansız hale getirerek, uygulamanın sadece yetkilendirilen orjinal cihazda çalışmasını garanti eder.

Keystore / Keychain Bütünlüğü

Android Keystore veya iOS Keychain sisteminin bütünlüğünü ve erişilebilirliğini kontrol eder. Uygulamanın şifreleme anahtarlarını ve hassas verilerini sakladığı bu donanım destekli güvenli alanın tehlikeye girip girmediğini doğrulayarak, kritik verilerin güvenli bir ortamda saklandığından emin olur.

Geliştirici Modu Denetimi

Cihazın "Geliştirici Seçenekleri"nin açık olup olmadığını kontrol eder. Bu mod, normal kullanıcılar için genellikle gereksiz ve kapalıdır ancak saldırganlar tarafından USB hata ayıklama, sahte konum veya diğer ileri seviye manipülasyon ve saldırıları gerçekleştirmek için sıklıkla kullanıldığından önemli bir risk göstergesidir.

Kod Karıştırma Kontrolü

Uygulama kodunun güvenli bir şekilde karıştırılıp karıştırılmadığını (obfuscation) kontrol eder. Kodun okunabilirliğini azaltan bu önlemin eksik veya hatalı olması, saldırganların tersine mühendislik yapmasını kolaylaştırır; bu özellik obfuscation tekniklerinin düzgün uygulanıp uygulanmadığını çalışma zamanında denetler.

ZERO SDK

Device Trust - ZERO Paketi, Uygulamanın silinmesi veya güncellenmesi gibi durumlardan etkilenmeyen, donanım tabanlı bir parmak izi oluşturarak benzersiz bir cihaz kimliği sunar. Dinamik risk analiziyle mobil uygulamanızın tüm işlemlerini güvence altına alır. Oturumları fiziksel cihaza bağlayarak SIM Swap ve yetkisiz erişimleri kaynağında durduran bütünleşik bir güvenlik katmanı sağlar.

Mobil Parmak İzi ve Cihaz Kimliği

Cihazın üzerindeki işlemciler, sensörler ve işletim sistemi konfigürasyonları gibi karakteristik donanım özelliklerinden türetilen benzersiz bir parmak izidir. Bu yöntem, yazılımsal değişikliklerden etkilenmeyen kararlı bir yapı sunar; böylece uygulama silinip tekrar yüklense bile aynı cihaz tanınmaya devam eder.

Uygulama Doğrulama

Her API isteğine, SDK tarafından tek kullanımlık olarak üretilen ve taklit edilemez bir dijital imza (kriptogram) eklenir. Kriptogram, isteği yapanın bir bot veya taklit yazılım değil, doğrulanmış orijinal uygulamanız olduğunu garanti altına alarak API geçidinizi yetkisiz isteklere karşı korur.

DeviceTrust

API Koruması

Otomatik saldırı araçlarına (scriptler, botlar) karşı aktif bir filtreleme uygular. JSON enjeksiyonlarından hacimsel DDoS girişimlerine kadar geniş bir tehdit yelpazesini engeller. Sistem, API çağrısının taklit edilemez bir insan etkileşimi ve orjinal uygulama ortamından kaynaklandığını doğrulayarak operasyonel güvenliğinizi sağlar.

Dinamik Risk Skoru

Her API çağrısı için , mobil cihazın güvenlik durumunu ve aktif tehditleri (root, emülatör vb.) tespit ederek dinamik bir risk skoru üretir. Bu skor sayesinde şüpheli işlemleri tespit edebilir, riskli işlemleri reddedebilir veya ek doğrulama adımlarıyla güvenliği sıkılaştırarak dolandırıcılıkla gerçek zamanlı mücadele edebilirsiniz.

Cihaz Eşleştirme

Kullanıcı oturumlarını kullanılan fiziksel cihaza "mühürleyerek" hırsızlığa karşı korur. Token'lar çalınsa bile bu anahtarın farklı bir cihazdan geldiğini tespit eder ve erişimi reddeder. Saldırganların tokenları başka bir cihazda kullanmasını engelleyerek hem Session Hijacking gibi kimlik hırsızlığı senaryolarına karşı kesin bir çözüm sunar.

SIM Swap Koruması

Kullanıcı kimliğini fiziksel cihazla eşleştirerek, telefon numarasının çalınmasına veya kopyalanmasına dayalı saldırılara karşı tam direnç sağlar. Bu sayede, saldırganlar SIM kart kopyalama , SIM Swap veya SMS şifrelerini (OTP) ele geçirme saldırısı yapsalar dahi fiziksel cihaz eşleşmediği için erişim sağlayamazlar.Kullanıcının kimliğini fiziksel cihazıyla eşleştirerek, telefon numarasının çalınmasına veya kopyalanmasına dayalı saldırılara karşı tam koruma sağlanır. SIM kart kopyalama, SIM Swap veya SMS tek kullanımlık şifre (OTP) ele geçirme gibi saldırılar yapılsa bile, fiziksel cihaz eşleşmesi olmadığı için yetkisiz erişim anında engellenir.

CORE Paket Doğrulaması

ZERO, istemci tarafındaki koruma kalkanı olan CORE paketinin aktif ve işlevsel olduğunu her API çağrısında kriptografik olarak doğrular. Eğer saldırgan CORE modülünü susturmaya veya baypas etmeye çalışırsa, ZERO bunu bir anomali olarak tespit eder ve saldırı girişimini bloke eder.

Veri ve İşlem Bütünlüğü

Mobil uygulama ile API arasındaki iletişimi güvenceye alır. Uygulamadan gönderilen verilerin, sunucuya ulaşana kadar yolda değiştirilmediğini garanti eder. Saldırganların araya girerek parametre manipülasyonu yapmasını, yetkisiz veri enjekte etmesini veya işlem detaylarını değiştirmesini engelleyerek operasyonel güvenliği en üst düzeye çıkarır.

FORT SDK

Device Trust - FORT paketi, Mobil uygulamanız için tam kapsamlı veri güvenliği sağlar. Hassas verileri, şifreleme anahtarlarını ve sunucu trafiğini uçtan uca şifreleyerek; veri hırsızlığına ve araya girme (MiTM) saldırılarına karşı tam koruma sağlar. Dinamik SSL Pinning ile ağ trafiğinizi, Güvenli Kasa ile tüm hassas verileri hem cihazda hem de transfer sırasında uçtan uca şifreleyerek korur.

Dinamik Sertifika Sabitleme

(Dynamic TLS/SSL Pinning) Geleneksel SSL Pinning'in aksine, sertifika değişimlerinde uygulama güncellemesi gerektirmez. Sunucu kimliğini yalnızca güvenilir sertifikalarla doğrulayarak; sahte sertifika otoriteleri veya güvensiz kök sertifikalarla yapılan trafik çözme (decryption) girişimlerini engeller. Charles Proxy ve Burp Suite gibi izleme araçları, kötü niyetli Wi-Fi / Proxy sunucuları üzerinden gerçekleştirilen "Ortadaki Adam" (Man-in-the-Middle) ve SSL sökme (SSL Stripping) saldırılarını tespit eder. Ağ katmanındaki zafiyetleri kapatarak verinin sadece hedeflenen sunucuya ulaşmasını garanti altına alır.

Güvenli Kasa

Uygulama içerisindeki API anahtarlarını, sertifikaları ve diğer önemli bilgileri şifrelenmiş güvenli bir kasa (secure vault) içinde saklamanızı sağlar. Saldırganların statik analiz araçlarıyla uygulamanızı tarayıp bu kritik bilgilere erişmesini engeller. Uzaktan yönetim yeteneği ile, uygulama güncellemesi gerektirmeden, güvenli kasa içindeki verilerin uzaktan güncellenmesini, değiştirilmesini veya geçersiz kılınmasını mümkün kılar.

Durağan Veri Şifreleme

Cihaz üzerinde durağan halde (data-at-rest) bulunan tüm uygulama ve kullanıcı verilerini güçlü kriptografik yöntemlerle şifreler. Veritabanı dosyalarından ön belleklere, kullanıcı tercihlerinden konfigürasyon ayarlarına kadar her türlü yerel veriyi koruma altına alır. Dosya sistemine doğrudan erişim sağlansa bile verilerin güvenliğini garanti ederek, kötü amaçlı yazılımların veya fiziksel saldırganların dosyaları okumasını imkansız hale getirir.

Uçtan Uca Şifreleme

Kişisel verileri (PII) ve finansal bilgileri kaynağında, yani mobil cihazda şifreleyerek veri mahremiyetini en üst düzeye çıkarır. Veri yüklerini (payload) cihazdan çıkmadan önce şifreler ve arka uç sistemlerinde sadece yetkili servislerin okuyabileceği güvenli bir protokol kurar. SSL sonlandırma noktalarından sonra bile verinin şifreli kalmasını sağlayarak, kötü niyetli sistem yöneticilerinin veya bulut sağlayıcılarının hassas verileri görmesini engeller.

MALWARE SDK

Device Trust MALWARE Paketi, mobil uygulamanızı ve son kullanıcılarınızı hedef alan dış tehditlere karşı geliştirdiğimiz en üst düzey güvenlik katmanıdır. Bu paket, uygulamanın çalıştığı cihazı aktif olarak tarar; kötü amaçlı yazılımları (malware), kimlik avı girişimlerini (phishing) ve kullanıcıyı kandırmaya yönelik sosyal mühendislik saldırılarını engeller.

DeviceTrust

Ürünlerimiz > Bilgi Güvenliği

Zararlı Yazılım Tespiti

Cihazı sürekli izleyen ve potansiyel tehditleri belirleyen aktif bir antivirüs motoru gibi çalışır. Bilinen kötü amaçlı yazılımları , aktif saldırı kampanyalarını ve uygulamanızın sahte / korsan kopyalarını tespit eder. Cihazda yüklü olan uygulamaları tarar, kara listedeki zararlı yazılımları tespit eder.

Riskli İzin Tespiti

SMS okuma izni ile Tek Kullanımlık Şifreleri (OTP) çalmaya çalışan veya ekran kaydı (Screen Recording) yetkisiyle kullanıcı giriş bilgilerini izleyen uygulamaları tespit eder. Gereksiz yere yüksek yetki isteyen bu "casus" yazılımları belirleyerek Hesap Ele Geçirme (ATO) saldırılarını engeller. Rehbere erişme, konumu takip etme veya mikrofonu dinleme gibi kritik izinleri, meşru bir işlevi olmaksızın talep eden şüpheli uygulamaları tespit eder. Kurumunuzun güvenlik politikalarına uygun olarak hangi izinlerin "tehlikeli" kabul edileceğini tanımlamanıza olanak tanır.

Korsan Yazılım Tespiti

Cihazdaki uygulamaların yükleme kaynaklarını analiz ederek güvenilirliğini denetler. Google Play veya App Store gibi resmi kanalların güvenlik denetiminden geçmemiş, USB, Web veya alternatif marketler aracılığıyla yüklenen yazılımları tespit eder. Saldırganların güvenlik önlemlerini devre dışı bırakarak dağıttığı modifiye edilmiş veya zararlı kod enjekte edilmiş korsan uygulamaları tespit eder.

Sahte Uygulama Tespiti

Uygulamanızın güvenlik kontrolleri devre dışı bırakılmış olası sahte klonlarını, Bundle ID, imza sertifikası ve paket yapısını denetleyerek tespit eder. Bu sayede, saldırganların uygulamanızı kopyalayıp ödeme altyapısını kendi hesaplarına yönlendirdiği kötü niyetli senaryolar önlenir. Orijinal uygulamanızın işlevlerini taklit eden ancak gelirlerinizi çalan bu sahte versiyonlar erkenden belirlenerek finansal kayıplar engellenir.

DeviceTrust

WEB

Device Trust - WEB, web uygulamalarınızı ve web API'lerinizi korumak için tasarlanmış, tarayıcı tabanlı gelişmiş bir güvenlik çözümüdür. Tarayıcı içindeki WebAssembly gücünden yararlanarak, botları, veri kazıyıcıları (scrapers) ve otomatik saldırıları, kullanıcı deneyimini bozan CAPTCHA'lara ihtiyaç duymadan engeller.

Tarayıcı Parmak İzi ve Cihaz Kimliği

Tarayıcı ve işletim sistemi özelliklerini analiz ederek manipülasyona dirençli bir cihaz kimliği oluşturur. Sahte hesap açılışlarını, hesap ele geçirme (ATO) girişimlerini ve diğer suistimallerini tespit eder. Saldırgan IP, Konum, Kullanıcı veya çerez değiştirse bile cihazı tanır.

Bot Engelleme

E-ticaret ve biletleme platformlarında sunulan ürün veya biletleri milisaniyeler içinde tüketen "Scalping" botlarını engeller. Yüksek hızlı bot aktivitelerini işaretleyerek, gerçek müşterilerinizin stoklara erişmesini sağlar ve otomatik alım scriptlerinin haksız kazanç elde etmesinin önüne geçer.

Otomasyon Engelleme

Selenium veya Puppeteer gibi otomasyon altyapılarını, script tabanlı botları ve başsız (headless) tarayıcıları anında tespit eder. API uç noktalarınızı hedef alan bu otomatik trafiği filtreleyerek; kimlik bilgisi doldurma (credential stuffing) saldırılarını, DDoS benzeri hacimsel kötüye kullanımları ve sahte kullanıcı kayıtlarını altyapınızdan uzak tutar.

Gizli Mod Tespiti

Web sitenize Gizli Mod" (Incognito) açılan anonim oturumları tespit ederek bu kullanıcılara kısıtlama getirme veya ek doğrulama isteme gibi özel kurallar ve akışlar uygulamanıza olanak tanır. Kimliğini gizlemeye çalışan kişilerin yüksek riskli işlemlerde bulunmasını engeller ve dolandırıcılık riskini minimize eder.

Tersine Mühendislik Tespiti

Yetkisiz Kod inceleme ve dinamik analiz girişimlerini kaynağında durdur. Geliştirici araçlarının (DevTools) açılmasını veya aktif hata ayıklama (debugging) oturumlarını anında tespit eder. Bu özellik, saldırganların uygulamanızın kaynak kodunu izlemesini, değişkenleri okumasını ve güvenlik mantığını analiz etmesini imkansız hale getirir. Kötü niyetli kişilerin veya rakiplerin algoritmalarınızı kopyalamasını engeller.

İşlem Bütünlüğü Denetimi

Her API çağrısı, tarayıcı parmak izi ve tehdit verilerini taşıyan imzalı bir kriptogram ile mühürlenir. Bu yapı, oturumları kaynak tarayıcıya kriptografik olarak bağlayarak çalınmasını ve saldırganların araya girmesini önler. Veri paketlerinin yolda değiştirilip değiştirilmediğini denetleyerek enjeksiyon ve tampering saldırılarını engeller, bu sayede finansal işlemlerinizin ve veri akışınızın manipüle edilmeden sunucuya ulaşmasını garanti eder.

Anti-Scraping

Verilerinizin, Büyük Dil Modellerini (LLM) eğitmek veya izinsiz veri toplamak amacıyla kullanılmasını engelleyerek fikri mülkiyetinizi korur. API'lerinizi hedef alan yapay zeka tabanlı kazıyıcıları (scrapers) ve tarayıcıları (crawlers) durdurur. Platformunuzdaki fiyatların, içeriklerin ve kullanıcı verilerinin otomatik araçlarla kopyalanmasını önlerken ; video içeriklerinizin yetkisiz indirilmesine veya başka sitelere gömülmesine (embedding) karşı aktif koruma sağlar.

WebAssembly Tabanlı Koruma

Tarayıcı tarafındaki güvenlik ajanımız, manipülasyona açık standart JavaScript yerine, kurcalamaya karşı dirençli WebAssembly (Wasm) modülleri üzerinde çalışır. Bu mimari, güvenlik kodunun saldırganlar tarafından analiz edilmesini ve tersine mühendislik yöntemleriyle çözülmesini son derece zorlaştırır. Sistem, entegre "Kendi Kendine Bütünlük Kontrolü" sayesinde ajanın kodunun değiştirilmediğini veya bypass edilmediğini sürekli olarak denetler. Her API çağrısında oluşturulan imzalı ve doğrulanabilir kriptogram (kriptografik kanıt) , tarayıcının manipüle edilmemiş, güvenli bir uç nokta olduğunu matematiksel olarak kanıtlar.

Karşılaştırma Tablosu

Özellik Grubu	Güvenlik Özelliği	CORE	ZERO	FORT	MALWARE	WEB
Çalışma Zamanı	Root / Jailbreak & Emülatör Tespiti	●				
	Hook (Frida/Xposed) & Debugger Tespiti	●				
	Uygulama Bütünlüğü (Anti-Tampering)	●				
Cihaz & Oturum	Donanım Tabanlı Cihaz Parmak İzi		●			●
	SIM Swap & Session Hijacking Koruması		●			
	Dinamik Risk Skoru		●			
Veri & Network	Dinamik Risk Skoru			●		
	Dinamik Risk Skoru			●		
	Dinamik Risk Skoru			●		
Dış Tehditler	Aktif Malware & Antivirüs Motoru				●	
	Riskli İzin (SMS/Screen Record) Analizi				●	
	Sahte/Korsan Uygulama Tespiti				●	
Web Güvenliği	WebAssembly (Wasm) Tabanlı Ajan					●
	Bot & Scraper Engelleme (Anti-Bot)					●
	DevTools & Gizli Mod Tespiti					●