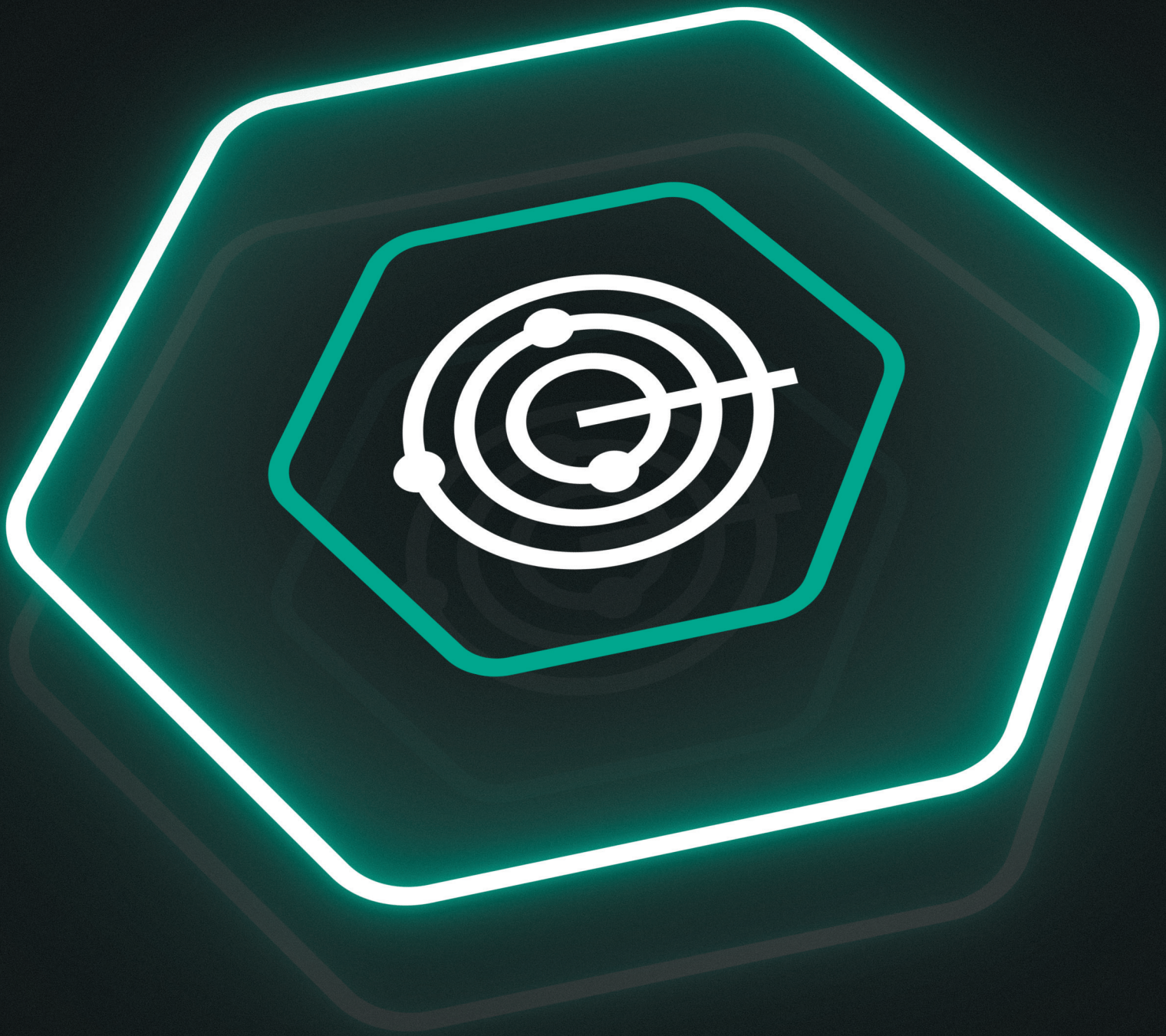


Kaspersky Anti Targeted Attack Platform

kaspersky GELECEĞİ YAKALAYIN

Günümüzde siber suçlular, sızma ve ele geçirme eylemleri için sürekli olarak yeni ve benzersiz yöntemler geliştirmektedir. Tehditler gelişip daha karmaşık ve yıkıcı bir hâle gelmeye devam ettikçe hızlı algılama ile en hızlı ve en uygun müdahale çok önemli bir role sahip olmuştur.

Artan siber tehdit oranlarının bir adım önünde kalabilmek ve yaşanan finansal kayıpları sınırlamak için

işletmelerin BT güvenlik savunmalarını yeniden düşünmeleri çok önemlidir.

Birleştirilmiş bir çözüm ile benzersiz siber güvenlik

Profesyonel siber suçlular, bu günlerde çok vektörlü bir yaklaşım tercih ediyor. Kaspersky Anti Targeted Attack Platform, ağ düzeyinde gelişmiş tehdit keşfi ve EDR özelliklerini birleştirirken BT güvenlik uzmanlarına üst düzey çok boyutlu tehdit algılamayı yönetmek, en son teknolojileri uygulamak, etkili araştırmalar yürütmek, proaktif olarak tehditleri saptamak ve hızlı, merkezi bir müdalahalede bulunmak için ihtiyaç duydukları tüm araçları sağlar ve bunların hepsini tek bir çözüm aracılığıyla gerçekleştirir.

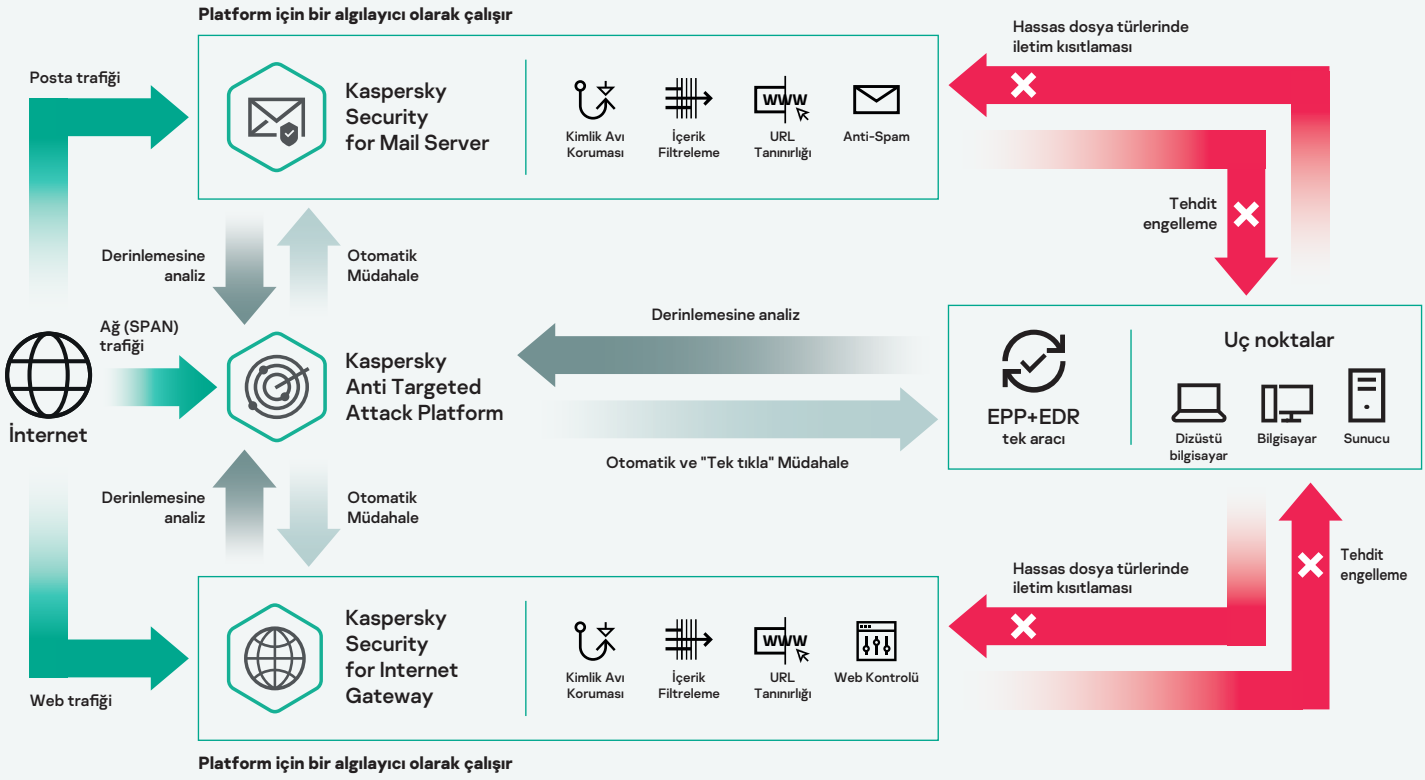
Kaspersky Anti Targeted Attack Platform:

- **TEHDITLERI** tespit etme ve müdahalede bulunma süresini azaltır
- **TEHDIT** analizini ve olay müdahalesini basitleştirir
- **GÜVENLIK** açıklarını ortadan kaldırmaya ve saldırının "bekleme süresini" azaltmaya yardımcı olur
- **TEHDIT** algılama ve müdahale sırasında manuel görevleri otomatik hâle getirir
- **DIĞER** önemli görevler için BT güvenlik personeline zaman kazandırır
- **YÖNETMELIKLERE** tam uyumluluğu destekler

Odağınız ve kontrolünüz altındaki en karmaşık saldırılar

Platform, Tehdit İstihbaratı'mız tarafından desteklenen ve MITRE ATT&CK çerçevesine eşleştirilen hepsi bir arada APT koruması sağlayan Kapsamlı Algılama ve Müdahale çözümü görevi görür. Tüm olası tehdit giriş noktaları (ağ, web, posta, bilgisayarlar, dizüstü bilgisayarlar, sunucular ve sanal makineler) sizin kontrolünüz altındadır.

Kaspersky Anti Targeted Attack Platform, **Kaspersky Endpoint Security for Business** ile tamamen entegre edilmiştir ve Kaspersky EDR ile tek bir aracı paylaşır. Platform ayrıca, kendisi için algılayıcı görevi gören ve daha karmaşık e-posta ve web tabanlı tehditlere otomatik müdahalede bulunabilen **Kaspersky Security for Mail Server** ve **Kaspersky Security for Internet Gateway** ile entegredir.



Tam gizlilik sağlayan güvenilir bir güvenlik çözümü

Tüm nesne analizi, giden veri akışı olmadan yerinde gerçekleştirilir ve Kaspersky Private Security Network, kurumsal verilerin tam izolasyonunu korurken gerçek zamanlı gelen itibar güncellemeleri sağlar.

Dijital dönüşümde yeniliği hızlandıracak birleşik bir platform bunu şu şekilde sağlar:

- **Bütünleyici iş devamlılığı.** En başından beri yeni süreçler için güvenlik ve uyumluluk oluşturuyoruz
- **Kurumsal BT altyapınız üzerinde** tam görünürlük
- **Görünürlük ve kontrolün gerekli olduğu yerlerde hem fiziksel hem de sanal ortamlarda dağıtım sağlayan** maksimum esneklik
- **Güvenlik, olaylara müdahale ve SOC ekiplerinizin maliyet verimliliğini ideal hâle getiren** tehdit algılama ve müdahale görevlerini otomatikleştirme
- **Genel güvenlik seviyelerini artırma ve eski güvenlik yatırımlarını koruyan**, mevcut güvenlik ürünleriyle sıkı ve basit entegrasyon

Ana özellikler:

Çok katmanlı sensör mimarisi – ağ, web ve e-posta sensörleri ve uç nokta aracılarının bir kombinasyonu sayesinde elde edilen çok yönlü görünürlük.

Kapsamlı tehdit algılama motorları – hızlı kararlar ve daha az yanlış pozitif veri için ağ sensörlerinden (ağ trafiği analizi) ve uç nokta aracılarından (EDR özellikleri) gelen verilerle çalışma.

Gelişmiş Korumalı Alan – Tehdit etkinliğinin derinlemesine analizi için güvenli bir ortam sağlayarak işletim sistemi bileşenlerinin rastgele seçilmesini, sanal makinelerde sürenin hızlandırılmasını, kaçınma önleyici teknikleri, kullanıcı etkinliği simülasyonunu ve MITRE ATT&CK bilgi bankasıyla eşleşen sonuçları destekler ve bunların hepsi son derece verimli davranış tabanlı algılamaya katkıda bulunur.

Geriye dönük analiz - güvenliği ihlal edilmiş uç noktaların erişilemediği veya verilerin şifrelendiği durumlarda bile, otomatik veri, nesne ve karar toplama ile merkezi depolama yoluyla.

İki Tehdit İstihbaratı etkileşimi modu - Kaspersky Security Network'ten küresel itibar verileriyle otomatik karşılaştırma ve Kaspersky Threat Intelligence Portal aracılığıyla manuel tehdit saptama ve araştırma sorguları.

Gerçek zamanlı otomatik tehdit saptama – Olaylar, Kaspersky tehdit saptama uzmanları tarafından oluşturulan benzersiz bir Saldırı Göstergesi (IoA) kümesiyle ilişkilendirilir ve MITRE ATT&CK matrisiyle eşlenir; bu da net olay açıklamaları, örnekler ve müdahale önerileri sağlar.

Güçlü esnek sorgu oluşturucumuzla proaktif tehdit saptama – Analiz uzmanları tipik olmayan davranışları, şüpheli etkinlikleri ve altyapınıza özgü tehditleri aramak için karmaşık sorgular oluşturabilir.

Özet

Güvenilir veri koruma, BT altyapısı güvenliği, işletme süreçlerini dengeli yürütme ve uyumluluk, günümüzde sürdürülebilir kurumsal gelişmenin ön koşulları olarak kabul edilir.

Kaspersky Anti Targeted Attack Platform, BT güvenliğini geliştirmiş bir kuruluş olarak kurumsal altyapınızı APT benzeri tehditler ve hedefli saldırılardan koruyan güvenilir savunmalar oluşturmanıza, ek BT güvenlik kaynağı kullanımına ihtiyaç duymadan düzenleme uyumluluğunu desteklemenize olanak sağlar. Otomasyon kullanımını artıran ve sonuç kalitesini iyileştiren birleştirilmiş çözüm sayesinde karmaşık olaylar hızlı şekilde belirlenir, soruşturulur ve yanıtlanır. Bu yaklaşım, BT güvenliği veya SOC ekibinizi manuel görevlerden kurtararak ekip verimliliğinin artmasına olanak sağlar.

Sektörün en etkili çözümü olduğu kanıtlanmıştır

SE Labs, Kaspersky Anti Targeted Attack Platform'u çeşitli bilgisayar korsanlığı saldırılarına karşı test etti **ve bize üç A puanlamasını verdi**.

Bağımsız "ICSA Labs: Gelişmiş Tehdit Savunması (2019, Üçüncü Çeyrek)" testinde Kaspersky Anti Targeted Attack Platform, **%100 tespit oranı ve sıfır yanlış pozitif değer sağladı**.

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

Radicati Group, Kaspersky'yi **Pazar Çeyreği 2020'de Gelişmiş Sürekli Tehdit (APT) Koruması'nda En İyi Şirket olarak tanımaktadır**.

Kaspersky, Gartner Peer Insights Customers' Choice for EDR Solutions 2020 etkinliğinde En İyi Tedarikçi seçildi

2020 yılında Gartner Peer Insights Customers' Choice for EDR Solutions için dünya çapındaki sadece 6 tedarikçiden biri olarak belirlenen şirketimizde bu başarı, Genişletilmiş EDR çözümümüz için müşterilerden gelen en iyi olumlu görüş olmuştur ve Kaspersky Anti Targeted Attack Platform'un merkezinde bulunan Kaspersky EDR ile bu başarı elde edilmiştir.

Gartner feragatnamesi

Gartner Peer Insights Customers' Choice, belgelendirilmiş bir metodolojiye uygulanan bireysel son kullanıcı yorumlarının öznel görüşlerini, değerlendirmeleri ve verileri kapsar; Gartner veya iştiraklerinin görüşlerini temsil etmez ya da onlar tarafından bir onay teşkil etmez.

MITRE | ATT&CK®

Algılama kalitesi MITRE ATT&CK Değerlendirmesi tarafından onaylandı

Kaspersky Anti Targeted Attack Platform'un temel unsuru olan Kaspersky EDR, MITRE 2. Değerlendirme Turu'na (APT29) katılarak günümüzdeki hedefli saldırıların önemli aşamalarında uygulanan temel ATT&CK Teknikleri'ni tespit etmede yüksek performans sergiledi.

Daha fazla bilgi almak için: kaspersky.com/MITRE

Kaspersky Anti Targeted Attack Platform hakkında daha fazla bilgi almak için:

kaspersky.com/enterprise-security/anti-targeted-attack-platform

Siber Tehdit Haberleri: www.securelist.com
BT Güvenliği Haberleri: business.kaspersky.com
KOBİ'ler için BT Güvenliği: kaspersky.com.tr/business
Kurumlar için BT Güvenliği: kaspersky.com.tr/enterprise

www.kaspersky.com

2020 AO Kaspersky Lab.
Kayıtlı ticari markalar ve hizmet markaları ilgili sahiplerine aittir.

Kanıtlanmış başarılara sahibiz. Bağımsızız. Şeffafız. Teknolojinin hayatlarımızı geliştirdiği, daha güvenli bir dünya oluşturmakta kararlıyız. Teknolojiyi, ortaya çıkardığı sonsuz sayıdaki fırsattan herkes yararlanabilsin diye daha güvenli hale getiriyoruz. Daha güvenli bir gelecek için siber güvenliğe önem verin.

Daha fazla bilgi için: kaspersky.com.tr/transparency

Proven. Transparent. Independent.