



Kaspersky Endpoint Detection and Response

Siber suçlular gün geçtikçe daha tecrübeli hâle geliyorlar ve mevcut korumadan başarılı bir şekilde kurtulabiliyorlar. İşinizin her alanı risklere açık olabilir; bu, iş açısından çok önemli işlemleri aksatabilir, üretkenliğe zarar verebilir ve işletme maliyetlerini artırabilir.

Kaspersky EDR ile kuruluşunuz şunları yapabilir:

- Tehditleri kötü amaçlı yazılımların ötesinde etkili bir şekilde **İZLEME**
- Gelişmiş teknolojileri kullanarak tehditleri etkili bir şekilde **TESPİT ETME**
- Ham verileri ve kararları merkezi olarak **TOPLAMA**
- Saldırlara hızlı bir şekilde **MÜDAHALE ETME**
- Tespit edilen tehditlerle kötü amaçlı eylemleri **ÖNLEME**

Tüm bunları, araştırma ve müdahale etmeyi kolaylaştıran kullanımı kolay bir web arayüzü aracılığıyla yapabilirsiniz.

Kaspersky EDR ve IDC Endpoint Security 2020 raporundan alınan önemli noktalar*

● Zayıf bir EPP çözümü, bir EDR aracının değerini yok eder

Kaspersky, tek bir aracı yoluyla güçlü ve eksiksiz uç nokta savunmaları (EPP+EDR) sunar

● Böylece, insanlar ve zaman, EDR araçları için yeni yatırım getirisi metriği hâline gelir

Kaspersky, karmaşık sorunlara yüksek düzeyde otomasyon uygulayarak güvenlik uzmanlarınızın değerli zamanlarını geri kazandırır

● EDR, uç noktaların dışındaki verilerden faydalanmalıdır

Kaspersky, tek bir araçla gelişmiş posta ve web tabanlı tehdit algılama ve görünürlük sağlayarak EDR etkinliğini artırır

İlk olarak uç nokta savunmanızı güçlendirin

Verilerin, kullanıcıların ve kurumsal sistemlerin iş süreçlerini oluşturmak ve uygulamak için bir araya geldiği kurumsal uç noktalar, siber suçlular için birincil hedef olmaya devam etmektedir. Kurumsal uç noktalarınızı korumak ve bu uç noktalarının altyapınıza giriş noktaları olarak kullanılmasını önlemek için BT güvenliği ekibiniz, mevcut savunmalarınızı güçlendirmenin yollarını aramalıdır. Yaygın tehditlerin otomatik olarak engellenmesinden karmaşık olaylara hızlı ve uygun şekilde müdahale etmeye kadar eksiksiz uç nokta koruma döngüsünü uygulamak, önleyici teknolojilerin gelişmiş savunma özellikleriyle desteklenmesini gerektirir.

Kaspersky Endpoint Detection and Response (EDR), kurumsal ağdaki tüm uç noktalarda kapsamlı görünürlük ve üstün savunmalarla birlikte güçlü güvenlik sağlayarak karmaşık tehditleri ve APT benzeri saldırıları tespit etmek, önceliklendirmek, araştırmak ve etkisiz hâle getirmek için rutin görevleri otomatik hâle getirir.

Öne Çıkan Noktalar

- Kaspersky EDR, en çok test edilen ve en çok ödül alan Endpoint Protection Platform (EPP) ürünümüz olan **Kaspersky Endpoint Security for Business**'i güçlü EDR özellikleriyle geliştirerek genel güvenlik seviyenizi güçlendirir. Yaygın tehditlere karşı otomatik koruma ve karmaşık saldırılara karşı gelişmiş savunma için tek aracı, olay yönetimini kolaylaştırır ve bakım maliyetlerini en aza indirir. Uç noktalar üzerinde ek yük oluşmaz ve ek maliyetler çıkmaz. Yalnızca iş istasyonlarınızın ve sunucularınızın en gelişmiş tehditler ve hedefli saldırılara karşı tamamen korunduğunu bilirsiniz.
- Kaspersky EDR; ilk kanıt toplama için gereken süreyi azaltır, tam telemetri analizi sağlar ve EDR işlemlerinin otomasyonunu en üst düzeye çıkarır; böylece ek BT güvenlik kaynaklarına gerek kalmadan genel olaya müdahale sürelerini azaltır.
- Kaspersky EDR, **Kaspersky Anti Targeted Attack Platform**'a eklenerek EDR özelliklerini ve ağ düzeyinde gelişmiş tehdit tespitini birleştirir. BT güvenliği uzmanları hem uç nokta hem de ağ düzeylerindeki üstün, çok boyutlu tehdit saptamayı ele almak için ihtiyaç duydukları tüm araçlara sahip olur, en gelişmiş teknolojileri uygular, etkili soruşturmalar gerçekleştirir ve hızlı, merkezi müdahalede bulunurlar. Tüm bunlar tek bir çözüm aracılığıyla gerçekleştirilir.

* IDC PERSPECTIVE, Endpoint Security 2020: The Resurgence of EPP and the Manifest Destiny of EDR

Kaspersky EDR, kuruluşunuzun şunları istemesi durumunda idealdir:

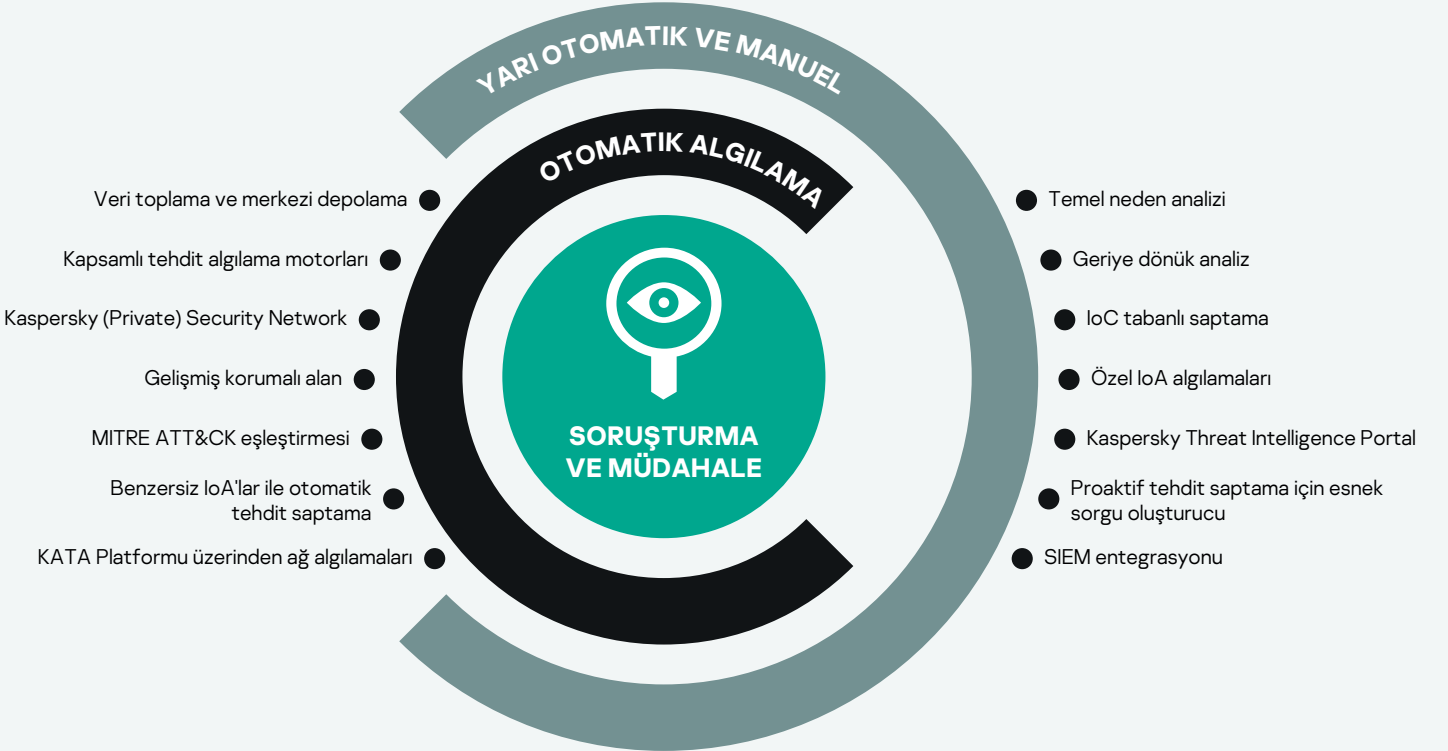
- Olaylara müdahale için kullanımı kolay ve kurumsal bir çözüm ile güvenliğinizi yükseltme
- Tehdit tanımlamasını ve müdahaleleri, soruşturmalar sırasında iş kesintisi olmadan otomatik hâle getirme
- Gelişmiş teknolojiler sayesinde uç nokta görünürlüğünüzü ve tehdit algılamanızı geliştirme
- Tehdit unsurlarının hedeflerine ulaşmak için kullandıkları belirli Taktikler, Teknikler ve Prosedürleri (TTP'ler) anlayarak daha etkili savunma ve güvenlik kaynağı ataması sağlama
- Birleşik ve etkili tehdit saptama, olay yönetimi ve müdahale süreçleri oluşturma
- Şirket içi SOC'nizin verimliliğini artırma (ilgili olmayan uç nokta kayıtlarını analiz ederek ekibinizin zamanını boşa harcamayın)
- Uç nokta kayıtlarını, uyarı incelemelerini ve soruşturma sonuçlarının belgelerini zorla elde ederek uyumluluğa katkı sağlama

En karmaşık tehditleri hızlı bir şekilde tespit edip gerekli müdahaleyi yapma

Kaspersky EDR, üst düzey uç nokta koruması sağlar ve SOC verimliliğini artırır; bu sayede gelişmiş tehdit algılaması sunar ve güvenliği ihlal edilmiş uç noktaların erişilemez olduğu veya verilerin bir saldırı sırasında şifrelendiği durumlarda bile geçmişe dönük veri erişimine olanak tanır. Benzersiz Saldırı Göstergeleri (IoA'lar), MITRE ATT&CK zenginleştirme ve esnek sorgu oluşturucu aracılığıyla güçlendirilmiş araştırma yetenekleri ve Threat Intelligence Portal bilgi tabanımıza erişim - Tüm bunlar, etkili tehdit saptama ve olaylara hızlı müdahaleyi kolaylaştırarak hasarın sınırlandırılmasını ve önlenmesini sağlar.

Kullanım senaryoları:

- Tüm ağınızda zorla girmelere karşı proaktif kanıt araması
- Saldırgan büyük hasarlara ve kesintiye neden olmadan bir saldırıyı hızlı algılama ve düzeltme
- Kesintisiz bir iş akışı ile binlerce uç noktada olayların hızlı bir şekilde araştırılması ve merkezi olarak yönetimi
- Diğer güvenlik çözümleri tarafından tespit edilen uyarıların ve olası olayların doğrulanması
- Manuel görevleri en aza indirmeye, kaynaklarınızı boşa çıkarmaya ve "uyarı aşırı yüklenmesi" olasılığını azaltmaya yardımcı olmak için rutin işlemlerin otomatik hâle getirilmesi





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

2020 yılında Gartner Peer Insights Customers' Choice for Endpoint Detection and Response Solutions için dünya çapındaki sadece 6 tedarikçiden biri olan Kaspersky, hizmetimiz ve desteğimiz sayesinde bu tedarikçiler arasında en yüksek puanı almıştır ve bu da Kaspersky EDR için müşterilerden gelen en iyi olumlu görüş olmuştur.

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

Taktikler, Teknikler ve Prosedürler (TTP'ler) analizinin karmaşık olay soruşturmasındaki önemini ve MITRE ATT&CK'nın şu anki güvenlik pazarındaki rolünü bilme:

- Kaspersky EDR, MITRE 2. Değerlendirme Turu'na (APT29) katılarak 2. Tur kapsamında günümüzdeki hedefli saldırıların önemli aşamalarında uygulanan temel ATT&CK Teknikleri'ni tespit etmede yüksek performans sergiledi.
- Kaspersky EDR tarafından yapılan tespitler, rakibinizin TTP'lerinin derinlemesine analizi için MITER ATT&CK bilgi tabanından alınan verilerle zenginleştirilmiştir.

Daha fazla bilgi için: kaspersky.com/MITRE

Kurum genelinde Kaspersky EDR'nin iş açısından faydaları:

- 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 ve BT güvenlik personeline zaman kazandırır
- Tehdit analizini ve olay müdahalesini basitleştirir
- Tehditleri tespit etme ve müdahalede bulunma süresini azaltır
- Tam uyumluluk sağlamaya yardımcı olur

Ve daha fazlasını istiyorsanız... Kaspersky Managed Detection and Response

Kaspersky EDR'ye tam olarak yönetilen ve bireysel olarak uyarlanmış devamlı savunmanın eklenmesi, olaylarla ilgili işleme görevlerini Kaspersky'ye vererek veya şirketteki ekibinizde belirli senaryolarda aksiyon alacak, güvenlik açısından yeterli yetkilere sahip uzmanlar olmadığında uzman kararlar ve benzersiz tehdit saplama için bize danışarak BT güvenliği kaynaklarınızın korunabileceği anlamına gelir.

Kaspersky EDR hakkında daha fazla bilgi almak için:

[kaspersky.com.tr/
enterprise-security/
endpoint-detection-
response-edr](https://kaspersky.com.tr/enterprise-security/endpoint-detection-response-edr)

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 başarılarla sahibiz. Bağımsız. 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.**