kaspersky GELECEĞİ YAKALAYIN

# Müşteriler için optimum güvenlik rehberi

EDR sınıfı korumaya yapılan akıllı yatırım ve işletmenizin buna ihtiyaç duymasının nedenleri

# Yönetici özeti

Yıllardır, KOBİ'ler ve orta ölçekli kuruluşlar, işletmelerini çok çeşitli emtia tehditlerine karşı savunma konusunda uç nokta koruma platformlarına (EPP) güvenebildiler. Ancak siber suçluların, EPP'yi aşabilen yeni, bilinmeyen ve elden kaçabilen tehditlere gitgide daha fazla yönelmesiyle birlikte, bu savunmaların artık bu tür tehditlere karşı koruma sağlayabilen uç nokta tespit ve yanıt (EDR) ve/veya yönetilen tespit ve yanıt (MDR) çözümleriyle güncellenmeleri gerekiyor.

Bu müşteri rehberi, işletmeniz için optimum EDR sınıfı güvenliği sadece sekiz basit adımda nasıl belirleyebileceğinizi açıklıyor. Bu adımlara uç nokta savunmalarınızda bulunan herhangi bir kritik boşluğu tespit edebilmeniz için mevcut uç nokta korumanızı değerlendirerek başlayacaksınız. Aynı zamanda ulaşmak istediğiniz nokta hakkında açık olmanız ve kullanım senaryolarınızı göz önünde bulundurarak ihtiyaçlarınıza en çok uyan korumayı tanımlamanız gerekecek. Bunlarla birlikte, hem EDR'yi hem de MDR'yi dikkatle incelemeniz, bu çözümleri daha geniş güvenlik ortamınız dahilinde ele almanız ve potansiyel sağlayıcılardan istediğiniz önemli becerileri listelemeniz gerekecek.

Bu rehberi okuduğunuzda; savunmalarınızı neden ve nasıl güncellemeniz gerektiğini, mevcut çözümlerin avantajlarını ve sadece işletmenizin ihtiyaçlarına değil, aynı zamanda BT ekibinizin güvenlik becerilerine ilişkin uzmanlığına da uyum sağlayacak optimum seviyedeki bir güvenlik çözümünü nasıl oluşturabileceğinizi net bir şekilde anlayacaksınız.

## Savunmalarınızı neden ve hemen güncellemeniz gerekiyor?

Uç nokta tespit ve yanıt (EDR) gibi gelişmiş siber güvenlik çözümleri pazardaki en popüler konu başlıklarından bir tanesi; üstelik geçerli bir nedenle. Özellikle de işletmeniz, küçük ve orta ölçekli bir işletmeyse (KOBİ) veya orta ölçekli bir kuruluşsa.

Peki neden özellikle bu segmentlerdeki işletmeler? Siber güvenlik dünyasındaki değişiklikler, günümüz saldırganlarının her ölçekten kuruluşa, her faaliyet alanına ve her hazırlık seviyesine odaklandığı anlamına geliyor. Daha spesifik olmak gerekirse, üst segmentteki KOBİ'ler ve orta ölçekli kuruluşlar,

eskiden sadece çok daha büyük ölçekli işletmeleri hedef alan daha gelişmiş elden kaçabilen tehditlerin saldırısı altında.

Buna yanıt olarak, BT güvenlik ekipleri mevcut uç nokta koruma platformlarını (EPP) EDR ve/veya yönetilen tespit ve yanıt (MDR) çözümleriyle tamamlıyor ve bu sayede; güvenlik olaylarını tespit edip araştırabiliyor, tehdidi uç noktada kontrol edebiliyor ve iyileştirme için otomatik bir yanıt ve/veya rehberlik alabiliyor.

Ancak maalesef ki bu çözümleri benimsemek bazen çözüm sağladığı kadar problem de yaratabiliyor; şüpheli görünmelerine ve araştırılmaları gerekmesine rağmen, nihayetinde zararsız oldukları ortaya çıkan devasa hacimlerdeki tehditlere karşı güvenlik ekiplerini uyarabiliyorlar. Bu da, kurum içi güvenlik uzmanlığı sınırlı olan veya bu tür uyarılar ile ilgilenecek yeterli zamanı olmayan BT ekipleri için sorun yaratabiliyor.

**Yanlış pozitif sonuçları kovalamak ve bunaltıcı sayıda uyarı almak yerine işletmenizin siber güvenliğine odaklanın ve önemli kaynakları optimize edin**

Bu nedenle ideal olan çözüm; uç nokta korumasını EDR iş yükünü önemli ölçüde hafifleten EDR sınıfı bir güvenlik ile destekleyen çözümdür. Ne kadar çok tehdit önlenirse, güvenlik ekiplerinin araştırması gereken daha az şey olur. Bu da BT güvenlik ekiplerinin, yanlış pozitif sonuçlar ve bunaltıcı sayıdaki uyarıyla uğraşmak yerine önemli kaynaklarını optimize edebilecekleri ve siber güvenlik işine odaklanabilecekleri anlamına gelir.

O halde tehdit ortamındaki hangi değişiklikler daha gelişmiş koruma ihtiyacını ortaya çıkarıyor? Farklı işletme türleri için nasıl değişiklik gösteriyor? Peki, bu tür tehditleri; (nitelikli siber güvenlik çalışanı konusunda küresel olarak yaşanan eksiklik göz önünde bulundurulduğunda belki de en önemlisi olarak), işletmenize, BT ekibinizin büyüklüğü ile güvenlik becerilerine ve potansiyel olarak maruz kaldığınız siber saldırı türlerine karşı en uyumlu olan çözümle nasıl etkili bir şekilde ele alabilirsiniz?

## Bu müşteri rehberi, ana hatlarıyla aşağıdaki konulardan bahsederek size yardımcı olacak:

- Mevcut uç nokta güvenliği neden yeni tehdit ortamında koruma sağlamaz?
- Gelişen güvenlik gereksinimlerinizi nasıl değerlendirebilirsiniz?
- Hem gittikçe daha fazla maruz kaldığınız tehditler hem de BT ekibinizin güvenlik becerileri bakımından ihtiyaçlarınıza en çok uyum sağlayan korumayı nasıl belirleyebilirsiniz?
- Sınırlı zamana, personele ve/veya kurum içi güvenlik uzmanlığına sahipseniz ne yapmalısınız?
- Güncel çözümler daha geniş güvenlik ortamlarına nasıl uyum sağlar?

# Mevcut uç nokta güvenliği neden yeni tehdit ortamında koruma sağlamıyor?

Konu uç nokta güvenliğinizi iyileştirmeye geldiğinde, bunun sadece işletmenize iyi bir şekilde uyduğunu düşündüğünüz bir EDR çözümünü belirleme ve uygulama meselesi olduğunu düşünebilirsiniz. Ancak bir binanın temeli kontrol edilmeden ilave kat çıkılması nasıl tavsiye edilmezse, aynı şekilde sizin de yapmanız gereken ilk şey mevcut EPP'nizi değerlendirmektir.

Örneğin, IDC[1] şunları tavsiye ediyor:

- IDC, EDR hakkındaki hususları tartışmadan önce, ilk olarak mevcut EPP çözümünüzü ele almanızı öneriyor. EPP'ye ilişkin beklenti, uç noktaları bağımsız bir çözüm olarak koruması olmalıdır.
- Bütün uç nokta çözümünün sonuçlarını bozacağı için standartların altında veya yetersiz olan EPP'leri kullanmayı kabul etmeyin. Bir şirket yetersiz bir EPP'yi EDR (ve çok fazla güvenlik analisti zamanı) ile telafi etmemelidir.

**Bütün uç nokta çözümünün[1] sonuçlarını bozacağı için standartların altında veya yetersiz olan EPP'leri kullanmayı kabul etmeyin.**
**Bir şirket yetersiz bir EPP'yi EDR (ve çok fazla güvenlik analistinin zamanı) ile telafi etmemelidir.**

EPP; tüm işletmelere çok çeşitli emtia tehditlerine karşı koruma sağlama ve BT güvenliği konusundaki iş yükünü en aza indirme konularında hayati bir öneme sahiptir. Ancak konu elden kaçabilen tehditlere geldiğinde daha ötesini düşünmeniz gerekir.

Yeni tehdit ortamının neden olduğu riskleri azaltmaya, mevcut uç nokta korumanızın etkinliğini değerlendirerek ve savunmalarınızda bulunan potansiyel boşlukları belirleyerek başlamalısınız.

## Neden düşündüğünüz kadar güvende olmayabilirsiniz?

Siz işletmenizin iyi bir şekilde korunduğunu düşünürken, sadece 2019 yılının ilk yarısında bile dört milyardan fazla kullanıcının verisini riske atan **4.000**'e yakın veri ihlalinin[2] gerçekleştiği tahmin ediliyor.

Bu korkutucu sayı, yıllık olarak gerçekleştirdiğimiz Küresel Kurumsal BT Güvenlik Riskleri Araştırmamızın sonuçlarını özetleyen 2019 yılı BT Güvenlik Ekonomisi adlı Kaspersky raporunun girişinde alıntılanmıştır. 23 ülkeden neredeyse 5.000 KOBİ ve kuruluş ile yapılan görüşmeleri içeren anket bazı endişe verici istatistikleri ortaya koydu. Örneğin:

**%55**

İşletmelerin %55'i, işlerinde karşılaştıkları tehditlere karşı yeterli bilgi sahibi olmadıklarını hisseden %38'lik orana rağmen, ağlarının hacklenmediğinden 'tamamen emin'.

**%12**

Kuruluşların %12'si, onlar için en maliyetli güvenlik olayı olmasına rağmen, kötü amaçlı yazılımların bulaşmasından endişe duyuyor.

**%51**

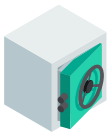
Kuruluşların %51'i ve KOBİ'lerin %47'si, genel veya hedefli güvenlik saldırıları arasındaki farkı ayırt etmenin giderek daha da zorlaştığını kabul ediyor.

**%66**

Kuruluş ve KOBİ'lerin %66'sı, özellikle siber güvenlik alanında küresel ölçekte yaşanan sorunlara rağmen 2020 yılında uzman BT çalışanlarına ilişkin yatırımlarını arttırmayı hedefliyorlardı.

1 IDC Doc # US45794219 - Uç Nokta Güvenliği 2020: EPP'nin Yeniden Ortaya Çıkışı ve EDR'nin Gidişatı - Ocak 2020
2 https://pages.riskbasedsecurity.com/2019-midyear-data-breach-quickview-report

Bu istatistiklerin ortaya koyduğu şey; işletmelerin siber tehdit dünyası hakkındaki algıları, potansiyel olarak en yüksek risklere (finansal riskler dahil) hangi tür saldırıların neden olduğu ve bu işletmelerin hazırlık seviyeleri ile kendilerini koruma becerileri arasında tehlikeli şekilde bir kopukluk olması.



2019 yılında yarattığı **2.73 milyon dolar** tutarındaki maliyet ile şirkete ait cihazlara kötü amaçlı yazılım bulaşması, kurumsal işletmeler için gerçekte en büyük finansal etkiye sahip veri ihlali biçimidir. Bu duruma rağmen, işletmelerin sadece %12'si kötü amaçlı yazılım bulaşmasını tehdit olarak görmektedir.

KOBİ'ler de kendileri için çok büyük maliyetler doğuran saldırıları göz ardı etmektedir. Küçük işletmeler için en maliyetli veri ihlali türleri üçüncü parti tarafından barındırılan BT altyapısını etkileyen durumlardır ve bu olayların maliyetleri **162 bin dolara** kadar çıkabilir. Buna rağmen KOBİ'ler bu durumu önem sıralamasında 5. sıraya koyar ve tüm dikkatlerini fiziksel bir cihazın kaybı veya hedefli bir saldırı nedeniyle veri kaybı gibi veri koruma konularına yönlendirirler.

Kurumsal işletmelerin ve KOBİ'lerin genel ve hedefli güvenlik saldırıları arasındaki farkı ayırt etmeyi çok daha zor bulmaları, deneyimledikleri olaylardaki potansiyel zararı tespit etmelerini veya değerlendirmelerini zorlaştırıyor. Bu durum, KOBİ ve kurumsal işletmelerin hem orta hem de gelişmiş kötü yazılım tehditlerine karşı giderek hassas davranmalarının muhtemel sebebi olabilir.

Rapor şu ifadeyle sona eriyor: "Artan siber saldırılarının bir adım önünde olmak ve meydana gelen finansal kayıpları azaltmak için işletmelerin BT güvenlik süreçlerine yapılan yatırımlarına devam etmeleri hayati önem taşımaktadır". Ancak bunu başarmalarının tek yolu, gittikçe daha fazla maruz kaldıkları gerçek tehditleri etkili bir şekilde ele almaları; yani, elden kaçabilen tehditlere karşı koruma sağlamada ihtiyaç duyulan EDR sınıfı güvenliğe yatırım yapmalarıdır.

# 1. Adım: Mevcut uç nokta korumanızı değerlendirin

Pazarda çok sayıda gelişmiş siber güvenlik çözümü olmasına rağmen, uç nokta korumanızın sizin için hayati bir rolü olduğunu unutmak oldukça kolaydır. Peki uç noktalar neden bu kadar önemli? Uç noktalar; sadece bir işletmenin altyapısına (siber suçluların öncelikli hedefi) giden en yaygın giriş noktaları değil, aynı zamanda karmaşık olayların etkili bir şekilde araştırılması için ihtiyaç duyulan verilere ilişkin önemli kaynaklardır.

Bu nedenle her işletmenin, dosyasız tehditler ve fidye yazılımlar da dahil olmak üzere emtia tehditlerinin neden olduğu yüksek sayıdaki olası olaylara karşı otomatik koruma sunan bir EPP seçmesi gerekiyor.

Bu tür bir kurulum, görece sınırlı sayıda uzman güvenlik bilgisine veya personeline ihtiyaç duyduğu için, özel bir güvenlik ekibi olmayan KOBİ'lerin veya küçük kuruluşların veya oldukça düşük düzeyde siber güvenlik uzmanlığı olan işletmelerin uç nokta güvenliği ihtiyaçlarını karşılar.

Ayrıca bu, orta ve büyük ölçekli kuruluşlar için oldukça önemli bir temel aşamadır; çünkü çözüm, çok sayıdaki küçük tehditlerle otomatik olarak ilgilendiği için bu kuruluşların ihtiyaç duydukları çok daha gelişmiş savunmaya odaklanmaları konusunda güvenlik ekiplerinin önünü açabilir.

Sahip olmasını beklemeniz gereken özellikleri size sunup sunmadığı konusunda EPP'nizi değerlendirirken şunları göz önünde bulundurmanız gerekir:

Ne kadar etkili?

Ne kadar yanlış pozitif alıyorsunuz?

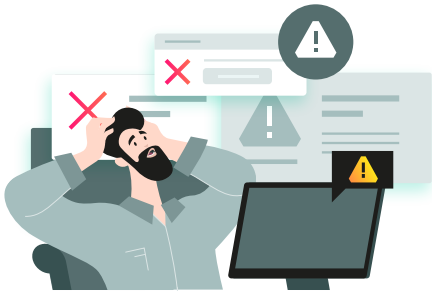
Web, uygulama ve cihaz kontrolleri gibi etkili saldırı alanı daralması sunuyor mu?

Rutin görevlerin otomatikleştirilmesine katkı sağlıyor mu?

Kullanımı kolay mı ve BT ekibinizdeki maliyetleriniz ile genel giderlerinizi en aza indirmeye yardımcı oluyor mu?

Güvenlik açığı değerlendirmesi ve yama yönetimi gibi kritik görevlerde yardımcı oluyor mu?

## 2. Adım: Uç nokta savunmalarınızdaki kritik boşlukları tespit edin



EPP'niz çok çeşitli emtia tehditlerine karşı size koruma sağlayacak olsa da, EPP'nizi atlatan yeni, bilinmeyen ve elden kaçabilen tehditlere karşı da savunmanızı gözden geçirmelisiniz.

Bir siber suçlunun saldırı düzenlemesinin gün geçtikçe daha ucuz hale gelmesi daha fazla işletmeyi risk altına sokuyor. Bu tür saldırıların artmasının yanında, saldırganların uç nokta güvenliğini etkili bir şekilde atlatmak için çeşitli teknikleri birleştirmesi, test etmesi ve kullanması nedeniyle çok daha etkili bir hale de geldiler.

Uzaktan çalışmadaki artışın bir sonucu olarak kurumsal çevrenin ortadan kalkması gibi değişiklikler nedeniyle bu tür tehditlerin acilen çözüme kavuşturulması artık daha da kritik bir hale geliyor.

Savunmanızı geleneksel EPP'lerin ötesine genişletmeniz gereken diğer belirtiler ise şunları içeriyor:

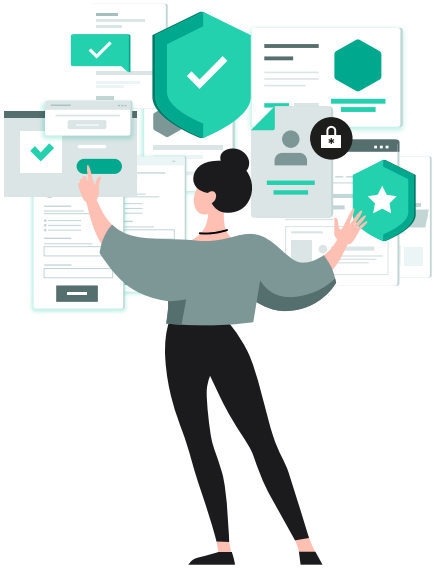
- EPP'niz artan yeni, bilinmeyen ve elden kaçabilen tehdit sayısını durdurmakta başarısız kalıyor.
- Uç noktalarınızda gerçekte neler olduğu konusunda sınırlı bir görünürlüğe sahipsiniz. Bu sınırlı görünürlüğe; kök neden analizleri, araştırma ve gerçek zamanlı tehdit yanıtı süreçlerini yürütememeniz veya bunu yavaş, karmaşık ve hata yapmaya yatkın olan bir olay temelinde standart işletim sistemi (OS) araçları ile manuel olarak yapmanız da dahil.
- Giderek artan gelişmiş tehditlerle mücadele etmede ihtiyaç duyulan BT güvenlik uzmanı becerilerine veya kapasitesine sahip değilsiniz.
- Büyük bir güvenlik olayı sebebiyle olası para cezaları ile karşılaşmaktan veya işletmenizin itibarına yönelik tehditlerin söz konusu olmasından endişeleniyorsunuz.

**İstemediğiniz birçok işlev için ödeme yapmak yerine gerçekten ihtiyacınız olan tüm işlevlerden en iyi şekilde yararlanın**

Bu tür tehditlere karşı savunma yapabileceğiniz etkili bir çözüm uygulamak için; şirketinizin boyutu, kurumsal profili, güvenlik konusundaki hazırlık seviyesi, mevcut kaynakları ve uzmanlığı ve özellikle de BT veya BT güvenlik ekibinizin güvenlik beceri düzeyi (veya 'olgunluğu') dahil işletmenizin özelliklerini gözden geçirmeniz gerekir.

Aynı zamanda istemediğiniz birçok işlev için ödeme yapmak yerine gerçekten ihtiyacınız olan tüm işlevlerden en iyi şekilde yararlanmanızı sağlayacak bir çözüm ve ardından da bu alanlarda çalışmak için ihtiyaç duyulan becerilere sahip BT güvenliği uzmanlarını işe almak istersiniz.

# 3. Adım: Neyi başarmak istediğinize dair net olun



Gartner[3]'a göre EDR araçları, güvenlik ve risk yönetimi teknik uzmanlarına ortamlarının güvenliği hakkında şu iki önemli soruyu cevaplamaları konusunda bir yöntem sunuyor:

- Burada ne oldu?
- Şu an ne oluyor?

Birçok işletme, sınırlı uzmanlığa (veya küçük bir BT güvenliği departmanına ve bunu genişletme planı olmamasına) sahip olmasına rağmen altyapılarında neler olduğunu anlamaya ve herhangi bir hasar meydana gelmeden önce elden kaçabilen tehditlere karşı yanıt verebilmeye ihtiyaç duyuyor.

Uygun EDR becerilerinin EPP'ye eklenmesi, daha gelişmiş ve elden kaçabilen tehditlere karşı oldukça etkili bir savunma sağlayabilir. Bu, BT güvenliği uzmanlarına etkili araştırma için gerekli olan bilgi ve verileri; Risk Göstergeleri (IoCs) oluşturarak, bu göstergeleri içe aktararak ve tüm uç noktalarda bu göstergeler için taramalar gerçekleştirerek kök neden analizi için gerekli olan araçları sağlayacaktır. Ve ayrıca, dosyaları karantinaya alma, ana bilgisayar izolasyonu, bir süreci durdurma, bir nesneyi silme vb. gibi otomatik ve/veya hızlı, doğru yanıtları mümkün kılacaktır.

# 4. Adım: İhtiyaçlarınıza en uygun korumayı belirleyin

Birçok işletme, özellikle BT güvenliği alanında uzmanlaşmış kişileri işe almayabiliyor. Bazıları, BT güvenliği departmanlarını daha yeni kurmaya başlamış bile olabilir. Diğerlerinin ise halihazırda tamamen gelişmiş ve nitelikli BT güvenliği ekipleri olabilir. Bu nedenle bu tür işletmelerin, tehdit savunmaları konusundaki mevcut uzmanlıklarının kalitesi ve bu göreve ayırabilecekleri zaman büyük ölçüde farklılık gösterir.

Özel BT güvenliği personeli olmayan veya rutin görevlerinden başlarını kaldıramayan BT güvenliği personeline sahip olan işletmelerin, bu tür farklılaşan koşullarla mücadele etmek için elden kaçabilen güncel tehditlere karşı stratejik otomasyon kullanımı uygulamaya ihtiyaçları olacaktır.

Bu da, bu tür tehditlere karşı koruma sağlarken, EPP'lerine uygun seviyelerde otomasyon (tamamen veya kısmen) da sağlayan ek EDR araçları ile desteklemeleri anlamına gelir.

3 Gartner – Uç Nokta Tespiti ve Yanıtı Teknolojileri ve Çözümleri için Çözüm Karşılaştırması – Ocak 2020

**Zamandan tasarruf ettiren ve sıkıntıları azaltan, mümkün olan en kolay kullanıma ve sadeliğe sahip araçlar**

Alternatif olarak, gerekli zamana veya becerilere sahip olamayabilecekleri aşırı derecede karmaşık bir EDR çözümüne yatırım yapmalarındansa, bir sağlayıcı, bir yönetilen servis sağlayıcısı (MSP) veya bir yönetilen güvenlik servis sağlayıcısı (MSSP) tarafından sunulan yönetilen tespit ve yanıt (MDR) çözümü; sektör uzmanları tarafından 7/24 güvenlik izleme, otomatik ve yönetilen tehdit avı, rehberli ve uzaktan yanıt senaryoları gibi becerilere erişmesine imkan verir.

Üçüncü seçenek ise EDR ve MDR'yi birleştirmektir. Birçok işletme, tehdit avı için gerekli olan uzmanlığa sahip değildir; bu nedenle, kurum içi tespit ve yanıt becerilerini uygularken bu uzmanlığı dışarıdan karşılamak sıklıkla ideal bir çözüm olarak düşünülür. Bu, özellikle de tespit ve yanıt uzmanını desteklemek için gerekli kaynağa, iş gücüne ve/veya becerilere sahip olmayan ancak kendi siber güvenlik ekibini geliştirmek isteyen işletmeler için faydalı olabilir.

Sizin durumunuza en çok uyan hangisi olursa olsun, size zaman kazandırıp endişelerinizi azaltırken aynı zamanda olabildiğince basit ve anlaşılır olan araçlar istersiniz. Aynı zamanda uyarı yorgunluğunu en aza indirmek için, yüksek sayıdaki potansiyel tehditle de otomatik olarak mücadele eden bir çözüm istersiniz.

# 5. Adım: Kullanım senaryolarınızı gözden geçirin

İhtiyaçlarınıza en uygun korumayı belirlerken gereksinimlerinizi açıkça belirlemelisiniz. Bu da, bunu yerine getirmede ihtiyacınız olan kullanım senaryoları ve almayı beklediğiniz sonuçlar gibi söz konusu çözümün performansı ve olağan kullanımının kritik özelliklerini gözden geçirmek anlamına geliyor.

Örneğin, bir güvenlik uyarısı aldığınızda, EDR ve/veya MDR şu gibi önemli soruları yanıtlamanızı sağlamalıdır:

Uyarının bağlamı nedir?

Uyarıyla ilgili halihazırda hangi eylemler gerçekleştirildi?

Tespit edilen tehdit hala aktif mi?

Diğer ana bilgisayarlar saldırı altında mı?

Saldırı hangi yolu izledi?

Tehdidin kök nedeni nedir?

Ayrıca tehditin tüm etki alanını anlamanıza da yardımcı olmalıdır. Örneğin:

Küresel bir tehdit altındaysanız, yönetim ekibiniz muhtemelen halihazırda saldırı altında olmadığınızdan emin olmak isteyecektir; bunu sağlamak adına çevrimiçi bir risk göstergesi bulacak, bir tarama gerçekleştirecek ve ekibinizin endişelerini doğru bir şekilde cevaplayacak beceriye ihtiyaç duyarsınız.

Düzenleyici bir kurum sizden belirli bir risk göstergesi için tarama gerçekleştirmenizi istiyorsa, güvenilir kaynaklardan risk göstergelerini içe aktarabilmeniz ve bir saldırının göstergeleri için periyodik taramalar gerçekleştirebilmeniz gerekir.

Bir uyarıyı kapsamlı bir şekilde araştırdıysanız ve diğer ana bilgisayarların da etkilenip etkilenmediğini öğrenmek için tüm ağ boyunca taramalar gerçekleştirmek yerine keşfedilen tehdit üzerinde risk göstergeleri oluşturduysanız, bunun sizin için otomatik olarak yapılması gerekir.

**Benzer şekilde, çabuk yayılan, hızlı ilerleyen tehditleri aşağıdakilerle hızlı bir şekilde yanıtlayabilmeniz gerekir:**

- Ana bilgisayarı izole ederek, dosyayı karantinaya alarak veya inceleme sırasında dosyaların yürütülmesini önleyerek tehdidin kontrol altına alınmasıyla.
- Keşfedildikleri anda elden kaçabilen tehditlere yanıt vermenizi sağlayan, risk göstergeleri taramalarına dayalı otomatik uç nokta yanıtı ile.
- Keşfedildikleri anda elden kaçabilen tehditlere yanıt vermenizi sağlayan, risk göstergeleri taramalarına dayalı otomatik uç nokta yanıtı ile.

**Dolayısıyla, çözümünüzden beklemeniz gereken önemli sonuçlar arasında şunların yer alması gerekir:**

- Daha sık görülen ve daha yıkıcı elden kaçabilen tehditlere karşı koruma.
- Basit ve otomatik bir araçla zamandan ve kaynaklardan tasarruf sağlama.
- Tüm ağınız üzerindeki karmaşık tehditlerin tam etki alanını gösterme.
- Her bir tehditin kök nedenini ve nasıl ortaya çıktığını anlamanızı sağlama.
- Hızlı otomatik yanıt sayesinde daha fazla hasardan kaçınma.

## Peki ya sınırlı kurum içi güvenlik uzmanlığına sahipseniz?

Diyelim ki kurum içi güvenlik uzmanlığınız sınırlı ya da sadece bir veya iki kişiden oluşan küçük bir güvenlik uzmanı ekibiniz var. Ayrıca EPP'nizi EDR ve/veya MDR ile destekleyip desteklememe konusunda karar vermeye çalıştığınızı farz edelim. Bu durumda ne tür faydalar sağlamayı bekleyebilirsiniz ve sizin için doğru olan hangileridir?

# 6. Adım: Hem EDR'yi hem MDR'yi dikkatle inceleyin

Daha pratik bir yaklaşımı tercih ediyorsanız (ve BT ekibiniz yeterli miktarda BT güvenliği becerisine sahipse), EDR; yeni, bilinmeyen ve elden kaçabilen tehditler nedeniyle ortaya çıkan riskleri ortadan kaldırarak ve güvenlik personelinize tehdit incelemesi, kök neden analizi ve yanıt için ihtiyaç duyulan görünürlüğü sağlayarak işlerinizin aksamasını ve ortaya çıkacak hasarı önlemenize yardımcı olabilir.

Bu, güvenlik ekibinizin birden çok araçla ve konsolla uğraşmak zorunda kalmadan daha verimli bir şekilde çalışmasını sağlayarak maliyet verimliliğini artırmasının yanı sıra kapsamlı bir süreç dizisini de otomatik hale getirerek kapasitenizi en üst düzeye çıkarabilir. Bunlara ek olarak, tehditleri izlemenizi ve tespit etmenizi, saldırıları yanıtlamanızı ve önlemenizi kolaylaştırarak içinizin de rahatlamasını sağlar.

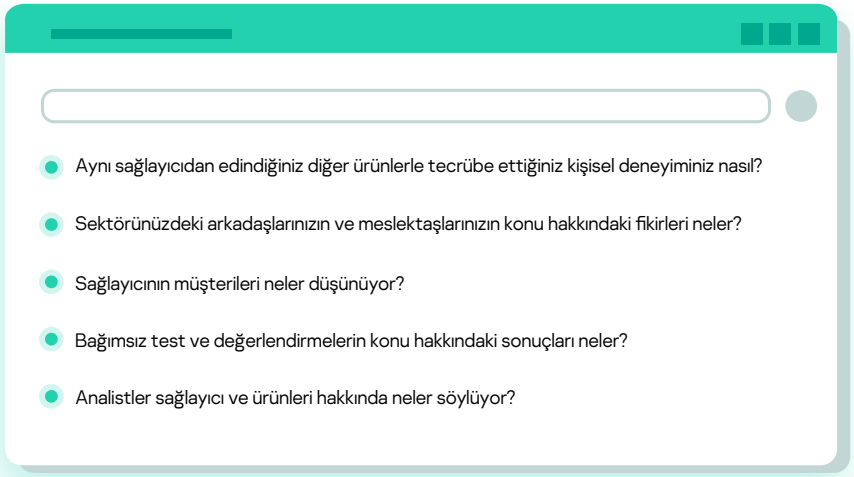
Önemli tespit ve yanıt görevlerine ilişkin yükü azaltarak kurum içi BT güvenliği kapasitenizi genişletmek istiyorsanız, MDR; aksi halde otomatik güvenlik bariyerlerini atlatabilecek olan tehditlere karşı gelişmiş ve sürekli bir koruma sunar. Bu, siber güvenlik alanındaki nitelikli personel eksikliği probleminizi çözerek işletmenizi güçlendirmenize yardımcı olabilir; ayrıca yüksek maliyetlere katlanmadan 7/24 Güvenlik Operasyon Merkezi'nin (SOC) sağladığı tüm önemli avantajları size sunabilir.

Bununla birlikte MDR, şirket içi kaynakları gerçekten BT güvenlik ekibinizin katılımını gerektiren kritik görevlere odaklayarak maliyet verimliliğini artırabilir ve analiz verimini önemli ölçüde artırmak ve ortalama yanıt süresini en aza indirmek için gelişmiş makine öğrenimi modellerinden yararlanarak kapasiteyi en üst düzeye çıkarabilir. Aynı zamanda otomatik ve yönetilen tehdit avı ile birlikte sektör uzmanları tarafından sürekli bir güvenlik izlemesi sunar. Bu izlemenin içerisinde; karmaşık ve kötü amaçlı yazılım kullanmayan tehditler ile saldırılarında yasal işletim sistemi araçlarını kullanan, tespit edilmesi zor ve tehlikeli olan tehditlerin analizi de yer alıyor.

Öte yandan, EDR ve MDR'yi birleştirmek; ilgili EDR sınıfı özelliklerini kendi ihtiyaçlarınıza uyarlamanıza imkan verir. Örneğin, kurum içi uç nokta tespit ve yanıt becerilerini uygularken tehdit avını (gerekli uzmanlığına sahip olmayabileceğiniz) dışarıdan sağlamak gibi.

## Peki ya büyük resme bakarsak?


EDR ve/veya MDR konusundaki tercihlerinizi belirledikten sonra, mevcut olan çeşitli çözümlerin pazarda nasıl değerlendirildiğini incelemek istersiniz. Siber güvenlik kadar hayati önem taşıyan bir ürün ararken, bağımsız uzmanların ve mevcut kullanıcıların değerlendirmeleri herhangi bir potansiyel sağlayıcının pazarlama amaçlı iddialarından önemli olmalıdır. Örnek vermek gerekirse:




# 7. Adım: Daha geniş güvenlik ortamınızı düşünün

Birçok işletmede, EPP, EDR ve/veya MDR çözümlerinin çok daha geniş bir güvenlik çerçevesi ile entegre olması ve bunun bir parçası olarak çalışması gerekir.

Bu çözümlere ek olarak, örneğin, aşağıdakilerden de faydalanabilirsiniz:

**Otomatik bir korumalı alan** – Uç nokta güvenliğinizin varlığında hareketsiz kalan ancak bir ana bilgisayar savunmasız hale geldiğinde etkinleşen ve bu nedenle de kontrollü, izole bir ortamda analiz edilmesi gereken tehditleri ortaya çıkararak uç noktalarınıza gelişmiş bir tespit seviyesi katar.

**Tehdit istihbaratı** – Şüpheli dosyalardaki, URL'lerdeki, IP'lerdeki ve etki alanlarındaki siber tehditler gibi sorunları daha iyi yönetmenizi ve tehditleri daha hızlı ve daha kapsamlı şekilde araştırmanızı sağlar.

**Güvenlik farkındalığı eğitimi** – çalışanlarınıza yönelik olan bu eğitim, özellikle siber güvenlik olaylarının büyük bir çoğunluğunun insan hatasından kaynaklandığı durumlarda, siber güvenlik farkındalığındaki boşlukları gidermenize ve çalışan davranışlarını değiştirmenize yardımcı olur.

Aynı zamanda çözümünüzün nasıl yönetileceğini de gözden geçirmek istersiniz: Örneğin, size tüm çeşitli bileşenler ve web, şirket içi ve kapalı yönetim seçenekleri dahil olmak üzere birleşik ve tek bir ekranda birleştirilmiş bulut destekli bir konsol sunması gibi.

# 8. Adım: Sağlayıcınıza aşağıdakilerin tümünü sağlayıp sağlamadıklarını sorun:

Farklı sağlayıcılar, (bazen büyük ölçüde) farklı yeteneklere sahip EDR ve MDR çözümleri sunar. Temel kural olarak, kapsamlı bir çözümün ideal olarak şunları içermesi gerekir.

- Hızlı ve sorunsuz dağıtım
- Alışmak için uzun süre veya yeniden eğitim gerektirmeyen kolay ve sezgisel araçlar
- Siber güvenlik araçlarınızı yapılandırmanız ve olaylara tek bir yerden tepki vermeniz için birleşik bir yönetim konsolu
- Muhtemel tüm dağıtım seçenekleri ile özel ihtiyaçlarınızı ve gereksinimlerinizi karşılayabilme: bulut, şirket içi, hibrit, kapalı
- Tehdit görünürlüğü
- Daha hızlı ve daha kolay analiz için görselleştirme ve detaya inme özelliklerini içeren kök neden analizi
- Risk göstergeleri içe aktarma, oluşturma ve tarama
- Hızlı ve tercihen otomatik yanıt özellikleri
- Rehberli yanıt senaryoları
- Sağlayıcı/yönetilen güvenlik hizmeti sağlayıcısı uzmanları tarafından desteklenen otomatik tehdit avı
- Sıkı bir şekilde entegre edilen uç nokta koruması ve uç nokta tespit ve yanıt işlevselliği
- Korumalı alan kapasitesi
- Entegre dosyasız koruma
- Kötüye kullanım önleme teknolojisi
- Fidye yazılımlarına karşı koruma
- Güvenlik açığı ve yama yönetim işlevi
- Uygulama, web ve cihaz kontrolü ile sistem güçlendirici diğer yöntemler
- Kullanıcı ve ağ yavaşlamalarını önlemek için yüksek performans
- Yerel dilinizde, etkili teknik destek

# Kaspersky Optimum Security size nasıl yardımcı olur?

Kaspersky, bağımsız testlerde diğer sağlayıcılara kıyasla yüksek koruma kalitesini istikrarlı biçimde ortaya koyar.

2019 yılında, Uç Nokta Koruma Platformları[4] kategorisinde üçüncü kez Gartner Peer Insights Customers' Choice ödülünü alarak üst üste yedi yıl en çok test edilen ve en çok ödül alan güvenlik sağlayıcısı olduk.

2020 yılında ise, hizmet ve destek bakımından en yüksek dereceyi alan sağlayıcı olarak dünya genelinde Uç Nokta Tespit ve Yanıt çözümleri[5] kategorisinde Gartner Peer Insights Customers' Choice takdirini alma hakkına sahip olan altı sağlayıcıdan biri olmayı başardık.

Yakın zamanda aldığımız diğer ödüller arasında şunlar yer alıyor:

- 2020 NSS Labs Gelişmiş Uç Nokta Koruması (AEP) grup testinde AA seviyesinde ürün derecelendirmesi
- AV-Comparatives: Enhanced Real World Testi'nde gelişmiş siber tehditlere karşı korumada alınabilecek en yüksek sonuç
- 2020 yılı SE Labs En İyi Kurumsal Uç Nokta ödülü

Kaspersky Optimum Security işletmenizi, kaynakların bilincinde olarak yeni, bilinmeyen ve kaçamak tehditlere karşı korur. Bu sayede, 7/24 güvenlik izleme, otomatik tehdit avı ile rehberli ve uzaktan yanıt senaryoları konusunda Kaspersky uzmanlarının desteği ile güçlendirilmiş etkili bir tehdit önleme, tespit ve yanıt çözümünü hızlı ve kolay bir şekilde uygulayabilirsiniz.

Bir bulut konsolu ile yönetilen, korumalı alan, tehdit istihbaratı portalı ve güvenlik farkındalığı eğitimi ile desteklenen EPP, EDR ve MDR arıyorsanız, Kaspersky Optimum Security; birleşik bir çözüm ile uç noktalarınızın tamamı için tam koruma sağlar ve size otomatik önleme, tespit ve yanıt, yönetilen koruma ve siber güvenlik eğitimi sunar.

## Gelişmiş tehdit koruması

- Gelişmiş önleme ve tespit mekanizmaları (makine öğrenimi, davranış analizi, korumalı alan, Saldırı Göstergeleri'ne (IoA) sahip otomatik tehdit avı) elden kaçabilen tehlikeli tehditlere karşı korumayı en yüksek seviyeye çıkarır; Kaspersky Endpoint Security for Business ile emtia tehditlerine karşı güçlü EPP koruması oluşturur
- Gelişmiş tehdit görünürlüğü, tespit edilen tehditler hakkında bağlam ve detay bilgileri sağlarken, sade kök neden analizi ve görselleştirme araçları her bir tehditi ve nasıl geliştiğini hızlı ve etkili bir şekilde araştırmanıza ve anlamanıza olanak verir.
- Otomatik tehdit avı; sektör lideri uzmanlar tarafından 7/24 sürekli izleme ile tehdit tespit ve yanıtı erken ve etkili bir şekilde oluşturmanıza ve geliştirmenize yardımcı olur.
- 'Tek-tık' ile hızlı ve uç nokta arası otomatik yanıt seçenekleri ve tüm altyapı genelinde risk göstergeleri taramaları, hızlı yayılan tehditlere hızla yanıt vermenize yardımcı olur.
- Rehberli ve uzaktan yanıt senaryoları güvenlik ekiplerinize yeni, bilinmeyen ve elden kaçabilen tehditlere karşı uzman analizleri ve yanıtlar sağlar.
- Çalışanların; siber tehditler, siber suçluların kullandığı yöntemler ve saldırıların gerçekleşmeden önce önlenmesine nasıl yardımcı olabilecekleri konularındaki farkındalığını yükseltmek, insan hatasından ve sosyal mühendislikten kaynaklanan riskleri azaltır.

## Hızlı, ölçeklenebilir ve kullanıma hazır koruma

- Tüm iş istasyonlarında, dizüstü bilgisayarlarda ve sunucularda, fiziksel ve sanal makinelerde, herkese açık bulutlarda ve konteynerlarda çalışır.
- Birleştirilmiş, çok katmanlı bir uç nokta güvenliği, olayları önceliklendirir ve kullanışlı bir web portalı sunulan tehdit istihbaratı ile tehdit keşfini ve araştırmasını hızlandırır.
- Fidye yazılımlarını, güvenlik açıklarını, dosyasız ve diğer kötü amaçlı yazılım saldırılarını önlediği kanıtlanmış sektör lideri teknolojileri kullanarak bilinen ve yeni ortaya çıkan tehditleri durdurur.

4 Gartner Peer Insights 'Voice of the Customer': Uç Nokta Koruma Platformları, 10 Aralık 2019
5 Gartner Peer Insights 'Voice of the Customer': Uç Nokta Tespit ve Yanıt Çözümleri, 1 Mayıs 2020

# Ek personel veya uzman ihtiyacını en aza indirir

- Bulut özellikli tek bir konsoldaki basit analiz ve yanıt süreçleri, güvenlik personelinin araştırma ve iyileştirme konularında harcayacakları zaman ve eforu optimize etmelerine yardımcı olur.
- Birleşik konsol, başlıca Kaspersky güvenlik uygulamalarının tek bir ekrandan yönetilmesini mümkün kılar. Siber güvenlik araçları yapılandırılabilir ve tek bir noktadan olaylara tepki verebilir; bulut, şirket içi, hibrit ve hava aralıklı olanlar da dahil mümkün olan tüm dağıtım seçenekleri ile belirli ihtiyaçları karşılayabilir.
- 7/24 güvenlik izlemesi, BT güvenliği konusunda personel eksikliği yaşayan işletmeler için bile sürekli koruma sağlar.

**Neden Kaspersky Optimum Security'ye yatırım yapmalısınız?**
**Kaspersky Optimum Security** ile sizleri belirlenmesi güç bir saldırıya ilişkin ciddi riski altında olduğunuz noktadan alıp uç nokta güvenliğiniz konusunda kendinize olan güveninizi yenilediğiniz bir noktaya taşıyabiliriz. Ortamınızda neler olduğu konusunda şüphe duymak yerine, nerede olursa olsun tüm uç noktalarınız üzerinde görünürlüğe ve kontrole sahip olursunuz. Karmaşıklığı nedeniyle güvenliğinizi güncelleme konusunda tereddüt etmeniz yerine, kaynaklarınızı optimize etmenize yardımcı olan konsolide ve sadeleştirilmiş bir çözüme sahip olursunuz.

go.kaspersky.com/optimum adresini ziyaret ederek, ek kaynak ihtiyacını en aza indirirken aynı zamanda işletmenizin ihtiyaç duyduğu gelişmiş korumayı nasıl elde edebileceğiniz hakkında daha fazla bilgi alabilirsiniz.

Siber Tehdit Haberleri: www.securelist.com
BT Güvenlik Haberleri: www.kaspersky.com/blog
Tehdit İstihbaratı Portalı: opentip.kaspersky.com
Bir bakışta teknolojiler: www.kaspersky.com/TechnoWiki
Ödüller ve takdirler: media.kaspersky.com/en/awards
İnteraktif Portfolyo Aracı: kaspersky.com/int_portfolio

**www.kaspersky.com.tr**

kaspersky GELECEĞİ YAKALAYIN