kaspersky GELECEĞİ YAKALAYIN

Kaspersky Optimum Security

Yönetilen koruma ve bulut destekli uç nokta tespit ve yanıt ile siber güvenliğinizde optimum seviyeyi yakalayın

Sorun

Kısıtlı olan zamanınızı ve kaynaklarınızı daha fazla zorlamadan yeni, bilinmeyen ve elden kaçabilen tehditlere karşı işletmenizi etkili bir şekilde savunabilmeniz gerekir.

Başarılı siber saldırıların %30'unde yasal sistem araçları kullanılıyor[1]

Gelişmiş saldırılar artıyor

Günümüzün elden kaçabilen tehditleri, geleneksel uç nokta korumasını etkili şekilde atlatabilmeleri için tasarlanıyor. Bu durum, saldırıların tespit edilmesini, analiz edilmesini ve bu saldırılara yanıt verilmesini gittikçe zorlaştırdığı için işletmeler açısından eskiye göre çok daha önemli riskleri de beraberinde getiriyor. Tespit edilmemiş bir tehdit altyapınıza sızarsa, işletmenizin kâr-zarar dengesini de etkileyen şu gibi önemli kayıplarla karşı karşıya kalabilirsiniz:

- Kritik iş süreçlerinin kesintiye uğraması,
- Ciddi düzeyde itibar ve müşteri kaybı,
- Para cezaları, yaptırımlar ve kazanç kayıpları.

Uç nokta korumasının güçlendirilmesi gerekiyor

Günümüzün elden kaçabilen tehditleri, suçluların yasal sistem araçları ve diğer kullanıma hazır yöntemleri ve teknolojileri kullanmaları nedeniyle çok daha etkili bir hale geldi. Suçluların saldırılarında bunları kullanması; alt yapılarınıza erişim sağlamalarına, bu erişimi sürdürmelerine, altyapınızda daha hızlı ve tespit edilmeyen kötü amaçlı eylemler gerçekleştirmelerine fırsat veriyor.

Kurumsal çevrenin ortadan kalkması ve uzaktan çalışmanın yaygınlaşması ile bu durum daha da kötü bir hal alırken, altyapınıza girmek isteyen saldırganlar için geleneksel olarak en çekici giriş yolu olan uç noktaları daha ön plana çıkarıyor.

Kaynaklar ise yetersiz kalıyor

Günümüzde artık uç nokta güvenliğinin ihtiyaç duyduğu bir şey olan ek korumayı sağlamak için, işletmeniz içerisinde yeterli düzeyde olay müdahalesi becerilerinin geliştirilmiş olması gerekiyor.

Ancak bu tür bir projeye ilişkin maliyetler hızlı bir şekilde kontrolden çıkabilir:

- Yazılım ve donanım maliyetleri artabilir,
- Yalıtılmış ve ayrı parçalara ayrılmış, güvenlik araçları ve süreçleri, güvenlik verimliliğinin zedelenmesi anlamına gelebilir,
- Rutin görevlerle çok fazla zaman kaybedilebilir.

Çözüm

Kaspersky Optimum Security, Kaspersky uzmanlarının desteği ve rehberliği eşliğinde 7/24 güvenlik izleme, otomatik yanıt ve tehdit avı ile güçlendirilmiş etkili bir tehdit tespit ve yanıt çözümü sunar.

Saldırıların %45'i, şüpheli dosyalar veya şüpheli uç nokta faaliyetleri sayesinde tespit edildi[1]

Gelişmiş tehdit engelleme

Sahip olduğunuz korumayı riske atmadan; basitleştirme ile etkili olma, insan zekası ile otomasyon, verimlilik ile işlevsellik arasındaki optimum dengeye ulaşın!

Kaspersky Optimum Security, savunmalarınızı yeni, bilinmeyen ve elden kaçabilen tehditlere karşı güçlendirerek para, müşteri ve itibar kaybetme riskinizi azaltmanıza yardımcı olur. Böylece, günümüzün hızla gelişen tehdit ortamına karşı koymaya hazır hale gelirsiniz.

Hızlı ve ölçeklenebilir hazır çözümler

Otomatik önleme yöntemleri, uç nokta korumasının temelini oluşturur. Ancak çok daha tehlikeli elden kaçabilen tehditlerle başa çıkabilmek istiyorsanız, bu yöntemleri gelişmiş araçlarla tamamlamanız gerekir.

Kaspersky Optimum Security, gelişmiş tespit ve hızlı yanıt becerileri sağlar ve bunların hepsini size bulut üzerinden sunar. Bu sayede, siber güvenlik mühendisleriniz, eskiden başa çıkabilmek için uykularını kaçıran tehditlerle bile hızla ve kesin şekilde mücadele edebilir.

Optimum yatırım seviyeleri

Daha fazla personeli işe almanıza, mevcut çalışanlarınıza tekrar tekrar eğitim vermenize veya karmaşık dağıtım süreçleri nedeniyle işlerinizin durma noktasına gelmesine gerek yok: Kaspersky Optimum Security, önemli olay müdahalesi süreçlerini benzersiz ihtiyaçlarınıza göre basitleştirir ve bu süreçlerin otomatik hale getirilmesine yardımcı olur.

İhtiyaçlarınıza hem şirket içi hem de bulut seçeneklerine ile uyum sağlarken, BT sistemi karmaşıklığını azaltmanıza, kullanıcı verimliliğini artırmanıza ve uygulama maliyetlerini şeffaf hale getirmenize yardımcı olan ölçeklenebilir bir kullanıma hazır güvenlik araç seti sunar.

Önemli avantajlar

- Çağın hep ötesinde olun ve işletmenizi, güncel ölümcül elden kaçabilen tehdit dalgası nedeniyle oluşan gerçek kesinti ve zarar riskine karşı savunun.
- Kullanımı kolay bir Uç Nokta Tespit ve Yanıt (EDR) araç setiyle kendi olay müdahale becerinizi geliştirin.
- Çalışanlarınızı eğiterek ve güvenlik farkındalıklarını arttırarak kötü amaçlı dosyaların bulaşması riskini önemli ölçüde azaltın.
- İşlemlerin otomasyonu ve yönetilen işlevsellik ile değerli kaynaklarınızı koruyun.
- Çeşitli özellikleri tek bir buluttan veya şirket içi konsoldan yönetilen bir çözüm ile harcadığınız zamandan ve emekten tasarruf edin.

Temel özellikler

Kaspersky Optimum Security, elden kaçabilen tehditlere karşı koruma sağlayabilmek için temelinde tespit, analiz ve yanıt bulunan çok çeşitli temel işlevler sunar.

Gelişmiş tespit

- Makine öğrenimine dayalı davranış analizi algoritmaları ile şüpheli davranışları hızlı ve doğru bir şekilde ortaya çıkarır.
- Kaspersky uzmanları tarafından desteklenen özel Saldırı Göstergelerine dayalı otomatik tehdit avı ile gizlenen karmaşık tehditleri bulur.
- Saldırı yüzeyini daraltan araçlarının yapılandırmasını kullanıcı profillerine göre otomatik olarak düzenleyen adaptif anormallik kontrolü sunar.

Basitleştirilmiş inceleme

- Bir olayla ilişkili bilgilerin tamamı otomatik olarak tek bir olay kartında toplanır.
- Görselleştirme ve anlaşılır inceleme süreci ile yaşanan olayı tek bir ortamda hızlı ve etkili bir şekilde analiz etmenizi ve sonraki davranış biçimi hakkında karar vermenizi sağlar.
- Ayrıca, size özel önerileri sunmak için Saldırı Göstergelerinin yaptığı tüm tespitler Kaspersky tarafından önceliklendirilir ve incelenir.

Otomatik yanıt

- 'Tek-tık' ile yanıt özelliği, münferit bir olayı hızlıca kontrol altına almanızı sağlar.
- Kaspersky uzmanlarının deneyimlerine dayanan rehberli yanıt, çok daha karmaşık ve tehlikeli tehditlerin bile üstesinden gelebileceğiniz anlamına gelir.
- Otomatik uç noktalar arası yanıt, ağda analiz edilen veya içe aktarılan tehditleri bulmanıza ve yanıtlamanıza yardımcı olur.

Nasıl uygulayabilirsiniz?

Kaspersky Optimum Security, bir saldırının çeşitli aşamalarında tehditleri önlemek, tespit etmek ve yanıtlamak için birlikte etkili bir şekilde kullanılabilen bir dizi araç ve önemli becerilere sahip olduğundan:

Sızma

Kullanıcı, bir kimlik avı e-postası alır veya kötü amaçlı bir web kaynağına erişerek ana bilgisayarına virüs bulaştırır.

Kurulum

İlk bulaşma, gerekli bileşenlere dağılır, K&K[1] ile iletişime geçer ve etrafını keşfeder.

Kök erişimi

Kalıcılık kazanmak ve gerektiğinde yatay hareketi başlatmak için yasal ve sistemde yerel olarak çalışabilenler de dahil bir dizi araç kullanılır.

Çalışanların güvenlik farkındalığı

Saldırı yüzeyinin daralması

Otomatik tehdit önleme

Makine öğrenimi temelli davranış analizi ve korumalı alanı da içeren gelişmiş tespit mekanizmaları

IoA'ler[2] ile otomatik tehdit avı

Kök neden analizi ve IoC[3] taraması

Otomatik, rehberli ve uzaktan yanıt senaryoları

[1] Komuta ve kontrol
[2] Saldırı Göstergeleri
[3] Risk Göstergeleri

Daha fazla koruma

Güvenliğinizin farklı yönlerini - tespit, inceleme ve farkındalık - hedefleyen çeşitli araçlarla savunmalarınızı daha da güçlendirebilirsiniz.

Başarılı saldırıların %31'inin kötü amaçlı e-posta kaynaklı olması, bunların birçoğunun çalışanlar tarafından önlenemediği anlamına geliyor[1]

Ek tespit katmanı

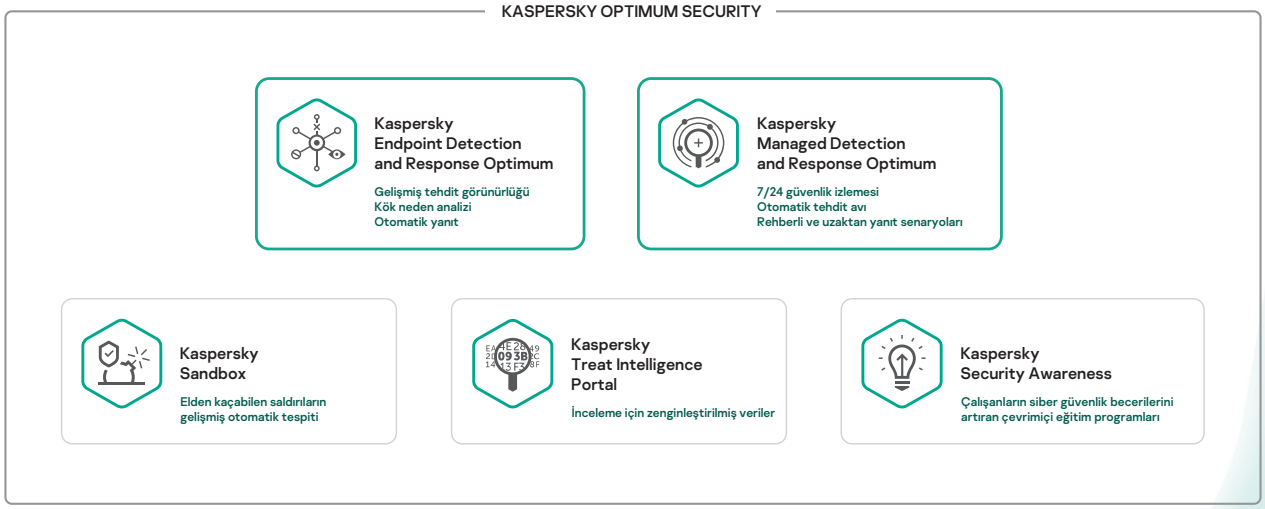
Tehditleri izole bir ortamda otomatik olarak analiz eden ve patentli tespit algoritmaları ile elden kaçmasını önleyen teknikler kullanan **Kaspersky Sandbox** ile yeni ve bilinmeyen tehditleri çok daha hızlı ve güvenilir bir şekilde ortaya çıkarın. Yapılandırılmış yanıtlar, keşfedilen tehditlere otomatik olarak uygulanırken, ilk dağıtım sürecinin dışında herhangi bir yönetime ihtiyaç duymadan tespit becerilerinizi önemli ölçüde artırır.

İncelemelerde sağlanan ek avantaj

Tehditle ilişkili dosyalar, hesaba dayalı adreslemeler, IP'ler ve URL'lere ilişkin güncel bilgilerle, siber güvenlik uzmanlarınızın tehditleri daha kapsamlı ve hızlı bir şekilde analiz etmesine ve anlamasına yardımcı olur. Kullanımı kolay **Kaspersky Threat Intelligence Portal** ile ek maliyet gerektirmeden daha fazla bilgiye ulaşmanızı sağlar.

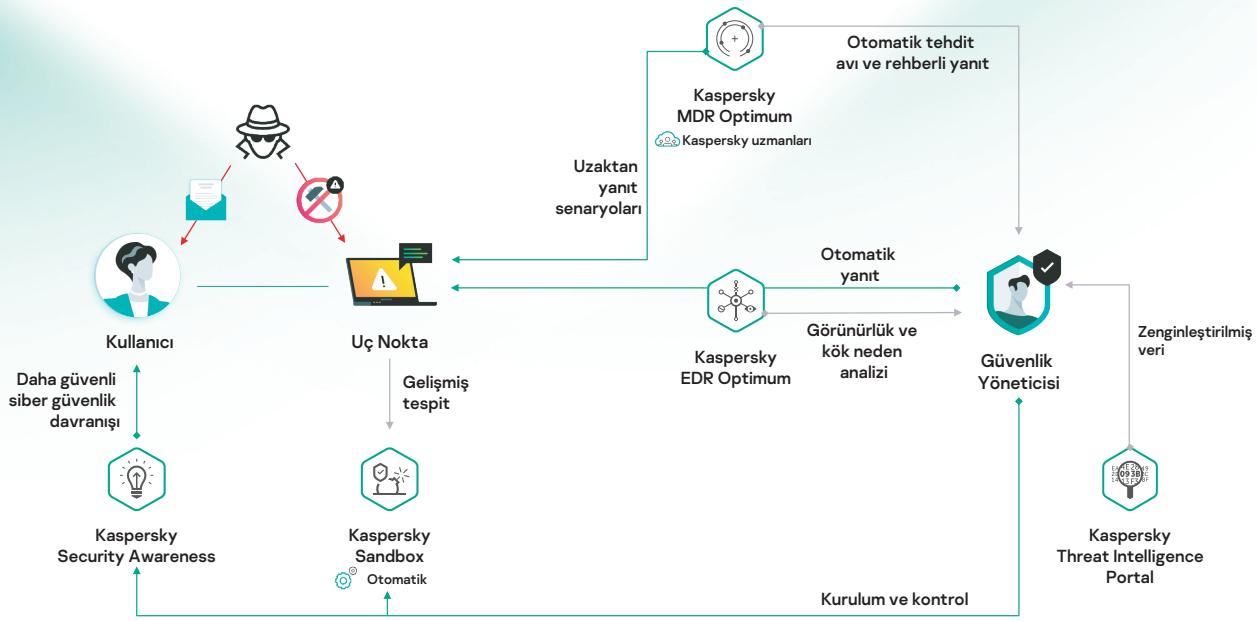
Güvenliğinizin temelinde çalışanlar bulunur

Saldırı yüzeyinizi daraltmanın ve olay sayısını azaltmanın kilit noktası, dikkatsizlik veya basit bir bilgi eksikliği nedeniyle altyapınızda ortaya çıkmasına neden olabilecekleri siber tehditler konusunda farkındalık sahibi olmaları için çalışanlarınıza eğitim vermektir. **Kaspersky Security Awareness**, altyapınızı korumaları için tüm çalışanlarınız ihtiyaç duyduğu bilgi ve becerileri geliştirir; bu sayede çalışanlarınız, siber anlamda güvenli bir ortamın devamlılığı için sizinle birlikte aktif olarak görev alırlar.



Nasıl çalışır?

Kaspersky Optimum Security'nin kullanımını, 7/24 koruma sağlamak için yönetilen bir çözüm şeklinde, kullanımı kolay bir EDR araç seti olarak veya her ikisinin bir kombinasyonu olacak şekilde, nasıl kullanacağınıza bağlı olarak siz seçebilir; kurum içi tespit ve yanıt becerilerinizi geliştirirken, Kaspersky uzmanlarının bilgi ve tecrübelerinden yararlanabilirsiniz. Kaspersky Optimum Security, birçok ürünü tek bir çözümde bir araya getirir:



Kullanım

Kaspersky Optimum Security'yi tek bir konsol aracılığıyla kolayca yönetebilir, bu sayede kısıtlı olan zamanınızı ve kaynaklarınızı en verimli şekilde kullanabilirsiniz.

Katılımcıların %56'sı, işletmelerinin siber güvenlik alanındaki personel eksikliği nedeniyle risk altında olduklarını belirtiyor[2]

Her şey tek bir pakette

- Kaspersky güvenlik ekosisteminin bir parçası olarak savunmalarınızı temel güvenlik seviyesinden optimize edilmiş gelişmiş özelliklere sahip güvenlik seviyesine getirir.
- Kaspersky Optimum Security'nin sahip olduğu farklı bir çok özellik, tek bir bulut konsol aracılığıyla yönetilebilir.
- Çok katmanlı korumaya sahip bir çözüm olarak yaygın ve elden kaçabilen tehditlerin yanı sıra insan kaynaklı hata olasılıklarını da ele alır.

Kolay yönetim

- Bulut yönetim konsolu, dünyanın neresinde olursanız olun hızlı ve etkili kontrol imkanı sunar.
- Şirket içi ve bulut tabanlı seçenekler size aynı yönetici deneyimini sunar.
- Halihazırda Kaspersky çözümlerini kullanıp kullanmadığınızdan bağımsız olarak hızlı ve sorunsuz bir dağıtım sunar.
- Tüm araçlar, uzun süreli alışma süreci veya yeniden eğitim gerektirmeden kolaylıkla ve sezgisel olarak kontrol edilip yönetilebilir.

Zaman ve kaynaklardan tasarruf edin

- Yönetilen koruma, BT güvenliğinde personel veya uzmanlık eksikliği yaşayan işletmelerin bu konuda güvenlik yatırımı yapmalarına gerek kalmadan tespit ve yanıt becerilerini geliştirmelerine yardımcı olur.
- Önemli siber güvenlik süreçlerinin otomatikleştirilmesiyle, olay müdahalesi daha hızlı, daha doğru ve daha verimli bir hale gelir.
- Çalışanların daha yüksek bir güvenlik farkındalığına sahip olması, daha az tehdidin savunmalarınıza sızması ve daha az olayın ortaya çıkması ile daha az işlem yapmanız anlamına gelir.

Kaspersky'nin aşamalı yaklaşımı

Kaspersky Security Foundations ile savunmalarınızı güvenilir bir koruma üzerine inşa edebilir; Kaspersky Optimum Security ile temel olay yanıtınızı sorunsuz bir şekilde yükseltebilir; ve son olarak, Kaspersky Expert Security ile en gelişmiş saldırılara karşı koruma sağlamayı hedefleyen güçlü araçları geliştirebilirsiniz.

Sizin için uygun olan seviyeyi seçebilirsiniz:

Kaspersky Security Foundations

Tehditlerin büyük bir kısmını otomatik olarak engeller:

- Tüm siber saldırıların büyük bir kısmını oluşturan yaygın tehditler nedeniyle ortaya çıkan olayları çok vektörlü ve otomatik olarak önler.
- Her boyutta ve karmaşıklıktaki işletmeler için entegre bir savunma stratejisi oluşturmadaki temel aşamadır.
- Küçük BT ekiplerine sahip olan ve güvenlik uzmanlığı gelişmekte olan işletmeler için güvenilir uç nokta koruması sağlar.

Kaspersky Optimum Security

Aşağıdaki koşulların olduğu durumlarda işletmelerin savunmalarını elden kaçabilen tehditlere karşı güçlendirir:

- Temel düzeyde siber güvenlik uzmanlığı olan küçük bir BT güvenlik ekibine sahip,
- Boyut ve karmaşıklık olarak büyümekte olan bir BT ortamına sahip olan ve bu nedenle saldırı yüzeyi artan,
- Gelişmiş koruma ihtiyacının aksine, siber güvenlik kaynaklarında eksiklik yaşayan,
- Olay yanıt becerisi geliştirmenin git gide önemli kazandığı.

Kaspersky Expert Security

Aşağıdaki koşulların olduğu durumlarda karşılaşılabilecek hedefli ve APT benzeri saldırılara hazırlar:

- BT ortamının karmaşık ve dağıtık olması
- Gelişmiş bir BT güvenlik ekibinin veya bir Güvenlik Operasyon Merkezinin mevcut olması
- Güvenlik olaylarının ve veri sızıntılarının yüksek maliyetleri nedeniyle düşük risk iştahı
- Mevzuata uyumluluk konusu

Kaspersky Optimum Security'nin, güvenlik ekibinize ve kaynaklarınıza kolaylık sağlarken siber tehditleri nasıl ele aldığı hakkında daha fazla bilgi almak için lütfen http://go.kaspersky.com/optimum adresini ziyaret ediniz.

1 Kaspersky Incident Response Analyst Report 2019, Kaspersky, 2020
2 (ISC)2 Cybersecurity workforce study, (ISC)2, 2020

Siber Tehdit Haberleri: www.securelist.com
BT Güvenliği Haberleri: business.kaspersky.com

www.kaspersky.com.tr