KASPERSKY lab

Yeni nesil uç nokta koruması

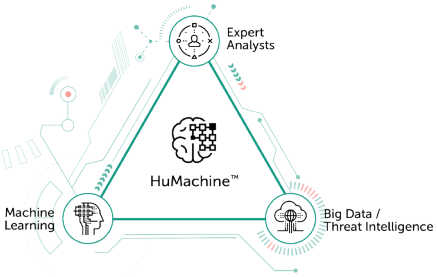
www.kaspersky.com.tr/business
#truecybersecurity

Kaspersky®
Endpoint Security
for Business

İş sürekliliği stratejinizin bir parçası olarak güvenlik

Teknoloji, işletmeler için dönüştürücü bir güçtür. İşletmeler teknolojiye ayak uydurmak zorundadır aksi takdirde çağın gerisinde kalırlar. Ancak teknoloji, kapılarını suçlulara da açar. Saldırganların ilk hedefi ve sorunların çoğunun kaynağı uç noktalardır. Geçtiğimiz yıl, işletmelerin %38'inden fazlası siber saldırıya maruz kalırken korunan uç noktalara yapılan saldırıların %39'u başarılı oldu. Bu ortamda, şirketlerin onlara saldıran siber suçlulardan daha akıllı olması gerekir.

Siber saldırıların ardında insanlar olduğu müddetçe bu saldırılara karşı koymak için yenilikçi teknolojiler kullanan insan zekasına ihtiyaç vardır. Kaspersky Lab koruması, sektördeki en iyi uzmanların bilgisiyle desteklenen makine öğrenimi algoritmalarına ve global tehdit istihbaratımıza dayalıdır. Bu eşsiz birleşime HuMachine™ adını verdik. Bu teknoloji tüm ürünlerimizin DNA'sında bulunur.



Kaspersky Lab, 2017 yılında **Gartner Peer Insights Uç Nokta Koruma Platformları: Platin Müşteri Seçimi Ödülü'nü** kazandı. Bu ödül, rekabetçi Uç Nokta Koruma Platformları piyasasında alınabilecek en üst düzey ödüllerdendir. Uç nokta uygulamalarımız, diğer satıcılara kıyasla bağımsız testlerde en çok ilk üçe girme yüzdesine (%90) sahiptir.

Geleceğe yatırım yapın

Küçük ve orta büyüklükteki işletmeler için tek bir veri ihlalinin ortalama finansal etkisi 86.500 USD iken bu rakam kurumsal şirketlerde 992.000 USD'ye ulaşıyor. Yeni nesil antivirüs artık yeterli değil. Hem birden çok teknolojik katmanda hem de kurumsal BT altyapısının işlevsel katmanlarında güvenliği sağlayan çok boyutlu bir çözüm ihtiyacınız olan korumayı sağlayabilir. Gerçek uç nokta güvenliği, işletmeleri her türlü platformda tüm siber tehditlere karşı korumak için çeşitli akıllı teknikleri ve teknolojileri bir araya getirir. Tüm BT ağınızı koruyabilirseniz iş sürekliliğinizden emin olursunuz.

HuMachine™ tabanlı uygulamalarla en çok değer verdiğiniz şeyleri koruyun

BT güvenliği için ayırdığınız bütçe, işletmenizle aynı oranda büyümeyebilir. Kaynaklar, bugünün ve yarının zorluklarını karşılayacak şekilde optimize edilmelidir.
HuMachine™ zekasından yararlanan Kaspersky Endpoint Security for Business; fidye yazılımlarına, güvenlik açıklarına ve en gelişmiş siber tehditlere karşı koruma sağlar. Kaynak açısından optimize edilen çözüm; güçlü güvenlik kontrolleri, otomatik güvenlik açığı ve düzeltme eki yönetimi ve entegre şifreleme özelliklerine sahiptir. Tüm bu özellikler, kurumsal ağ genelinde tek bir konsoldan yönetilebilir.

Çevik ve uyarlanabilir güvenlik

Bu ürün, tüm BT ortamlarında çalışmak üzere tasarlanmıştır. Başarısını kanıtlamış, çok çeşitli Yeni Nesil teknolojiler kullanır. Yerleşik sensörler ve Uç Nokta Tespiti ve Yanıtı (EDR) teknolojisi, büyük miktarlardaki verilerin yakalanmasını ve analiz edilmesini sağlayarak en zor anlaşılan ve karmaşık siber saldırıların bile keşfedilmesine yardımcı olur.

Dış kaynaklı BT için geleceğe yönelik güvenlik

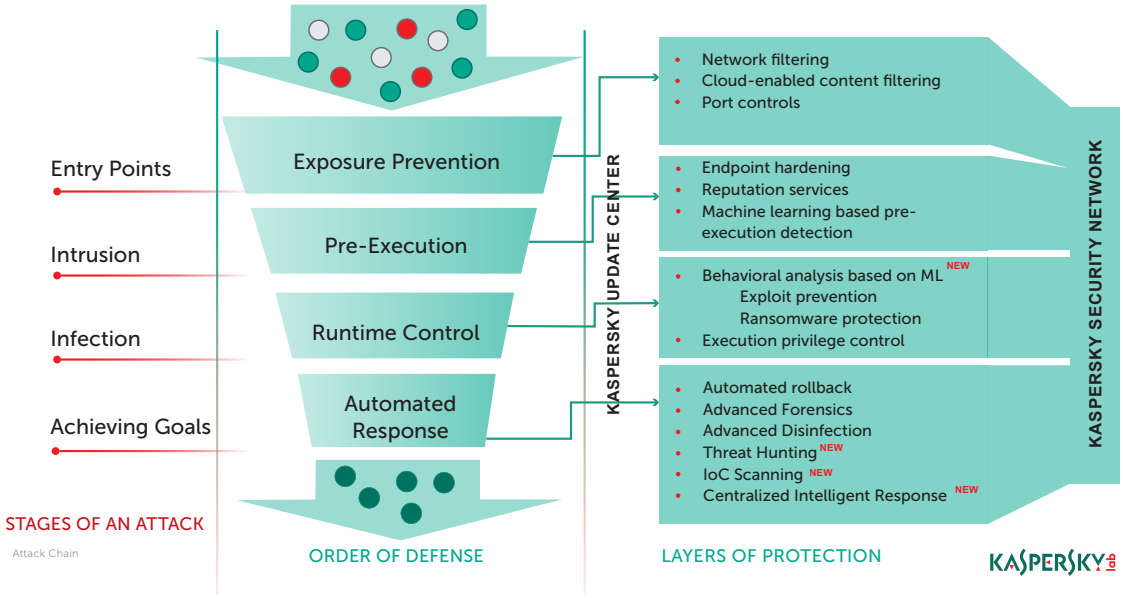
Tehdit önleme, mobil güvenlik, veri şifreleme ve güvenlik açığı ve düzeltme eki yönetimi ile birlikte yerleşik çok kiracılı olma özelliği, Yönetilen Hizmet Sağlayıcılarının BT güvenliğini sundukları hizmetler arasına ekleyerek güçlenmelerini sağlar.

Daha az yer kaplayarak yüksek performans sunar

En çok test edilen ve ödül alan HuMachine tabanlı güvenliğimiz, bilgisayar kaynaklarını minimum düzeyde etkileyerek optimum koruma sağlar. İmzasız bileşenler, tehditlerin sıklıkla güncellemeye gerek kalmadan algılanmasını sağlar.

Kapsamlı koruma

Kaspersky Endpoint Security for Business; tehditler gelişmiş koruma katmanlarına ulaşmadan birçoğunun etkisiz hale getirilmesi için Yeni Nesil teknolojiler (uç noktaların güçlendirilmesi, makine öğrenimine dayalı davranış analizi, güvenlik açıklarını önleme vb.) kullanır. Uç noktalara kadar ulaşan şüpheli dosyalar, tespit edilir ve engellenir.



Çok katmanlı yaklaşımımıza sahip gelişmiş teknolojilerin bu birleşimi, performans ve verimli koruma arasında mükemmel bir denge sağlar. Bu özelliğimiz, ürünlerimizin sektördeki en yüksek tespit oranlarına ulaşması konusunda çok önemli bir rol oynar. Yüksek tespit oranlarımız, bağımsız testlerde sürekli olarak kanıtlanır.

Aşağıdakiler için çok katmanlı koruma sağlar:

- Windows, Linux veya Mac
- Android ve diğer mobil cihazlar
- Çıkarılabilir depolama birimleri
- Windows ve Linux Sunucuları
- E-posta sunucuları
- Web ağ geçitleri
- İşbirliği sunucuları

Aşağıdakilere karşı benzersiz bir savunma sağlar:

- Yazılım açıklarından yararlanan yazılımlar
- Fidye yazılımı
- Mobil kötü amaçlı yazılımlar
- Bilinmeyen tehditler
- Dosyasız (fileless) tehditler
- PowerShell & diğer komut dosyası tabanlı saldırılar
- Web tehditleri
- E-posta ile yayılan tehditler
- Kimlik avı saldırıları
- İstenmeyen e-postalar

Fidye Yazılımlarına ve Açıklardan Yararlanan Yazılımlara Karşı Koruma

Gerçek zamanlı tehdit istihbaratı ve makine öğreniminin benzersiz kaynaklarını temel alan teknolojilerimiz, sürekli gelişir. Uç noktalarınızı en yeni güvenlik açıklarından koruyun. Gelişmiş tehditlere ve fidye yazılımlara karşı verilerinizin ve paylaşılan klasörlerinizin güvenliğini sağlayın.

Hesapların ele geçirilmesini engelleyin

Davranış Algılama özelliği, sistem açısından kritik süreçleri korumanın yanı sıra kullanıcı ve yönetici kimlik bilgilerinin sızdırılmasını engelleyen bir Bellek Koruma mekanizmasına sahiptir.

Uygulamalar nedeniyle saldırıya maruz kalma ihtimalinizi azaltın

Dinamik Beyaz Listeye Alma ve Uygulama Kontrolü özellikleri, hangi yazılımların çalıştırılabileceğiyle ilgili tüm kontrolü size vererek sıfır gün saldırılarına maruz kalma ihtimalini azaltır. Uygulama Kontrolü, çeşitli yorumlayıcılar aracılığıyla yürütülebilir dosyaların, DLL'lerin ve kontrol betik dosyalarının başlatılmasını engeller. Davranış Algılama ve Güvenlik Açıklarından Yararlanan Programları Önleme özelliği, uygulamanın davranışını izler, olası kötü niyetli etkinliği engeller ve yasal uygulamalardaki güvenlik açıklarından yararlanılmasını ve kötü amaçlı yazılımlar tarafından kullanılmasını engeller. Onaylı ve güvenilir uygulamalarınız ise sorunsuz bir şekilde çalışmaya devam eder.

Rootkitleri etkisiz hale getirir

Saldırganlar, etkinliklerini güvenlik çözümlerinden gizlemek için rootkitleri ve bootkitleri kullanır. Kaspersky Lab'in çok katmanlı Yeni Nesil korumasının bir parçası olan rootkitleri önleme teknolojisi, en iyi gizlenen virüsleri bile tespit etmeye ve etkisiz hale getirmeye yardımcı olur.

En gizli saldırıları ve izinsiz girişleri bile tespit edebilirsiniz

Yerleşik sensörler ile Uç Nokta Tespiti ve Yanıt teknolojisi, büyük miktarlardaki verilerin yakalanmasını ve analiz edilmesini sağlayarak zor anlaşılan ve en karmaşık siber saldırıların bile keşfedilmesine yardımcı olur. İzinsiz girişlerle ilgili risk göstergeleri (IOC) gibi kanıtlar için gelişmiş tehdit avı özellikleri sunar.

Ağ aracılığıyla saldırıya maruz kalma ihtimalinizi azaltın

Arabellek aşımı saldırısı kullanan kötü amaçlı yazılımlar, bellekte çalışan bir işlemi değiştirebilir ve bu yolla kötü amaçlı kodları çalıştırabilir. Ağ Tehdit Koruması, ağ saldırılarını ve güvenlik açıklarından yararlanan yazılımları tanımlar ve henüz size ulaşamadan engeller.

Bakım ve Destek

Dünya genelinde 200'den fazla ülkede 35 ofisimizle hizmet veriyoruz. 7/24 global destek anlayışımız Maintenance Service Agreement (MSA) destek paketlerimize de yansımıştır. Profesyonel Hizmetler ekiplerimiz, Kaspersky Lab çözümünüzden maksimum faydayı elde etmenizi sağlamak için sürekli nöbettedir. Kritik güvenlik olayları desteğinin yanı sıra dağıtım sırasında size yardımcı olur.

Ücretsiz deneme

Yalnızca Gerçek Siber Güvenlik işletmenizi her türlü tehditten korumak için kullanım kolaylığını **HuMachine™** istihbaratının hızıyla birleştirir. Bu sayfayı ziyaret ederek **Kaspersky Endpoint Security for Business** çözümünün 30 günlük ücretsiz tam sürümünü deneyin. Deneme süresinin sonunda ürünü satın almaya karar verirseniz lisans ücretini ödemeniz yeterlidir. Uygulama, deneme sırasında uç noktalarınızda çalışmaya başladığı için hiçbir ek işlem yapmanıza gerek yoktur.

Uç nokta korumasının ötesinde – şu anda ve gelecekte

Envanteri ve düzeltme ekleri uygulamayı kolaylaştırır

Donanım ve yazılım envanteriyle ilgili ayrıntıları keşfetmek ve güvenlik açıkları için zamanında düzeltme eki uygulanmasını yönetmek, zaman kaybına neden olan zor bir iştir. Siber suçlular, tek bir uç noktadan BT altyapısına saldırmak için genellikle düzeltme eki uygulanmamış güvenlik açıklarından yararlanır. Bu çözüm, yeni üçüncü taraf yazılımların uzaktan dağıtımının ötesinde güvenlik açıklarıyla ilgili sürekli olarak toplanan istihbarata dayalı otomatik güvenlik açığı değerlendirmesi ve düzeltme eki yönetimi özellikleri sunar. Bu sayede saldırılara açık yazılımların güncelliğini koruyarak BT yöneticilerinizin diğer görevlerine vakit ayırmasına yardımcı olur.

Şifreleme yoluyla güvenli veri paylaşımı

Kullanıcı için şeffaf FIPS 140-2 sertifikalı şifreleme, taşınabilir cihazlarda ve şirket içindeki cihazlarda bulunan gizli veriler için tam koruma sağlar. Entegre teknoloji sayesinde merkezi olarak dosya, disk ve cihaz düzeyinde kurumsal verilerin şifrelenmesini ve ağınızdaki veri paylaşımının güvenliğini sağlayabilirsiniz.

Mobil ve uzaktan senaryolar için destek

Veriler her zaman erişilebilir hale gelir ve ortamınızda serbestçe hareket edebilir. Mobil güvenlik, özellikle hareket halindeki verileri hedef alan tehditlere karşı koruma sağlamanın yanı sıra cihazlardaki zayıflıkları altyapıya sızmak için sıçrama tahtası olarak kullanma girişimlerini engeller. Cihaz Kontrolü, onaylanmamış veya şifrelenmemiş taşınabilir cihazlardaki veri kaybının ve cihazlardan virüslü verilerin indirilmesinin sonuçlarına karşı önlem almanızı sağlar.

Tüm platformlara yönelik yönetimle verimliliği optimize edin

Tek bir konsol, nerede olursa olsun ve hangi görevi üstlenirse üstlensin tüm iş istasyonları, sunucular ve mobil cihazlar üzerinde tam görünürlük ve kontrol sağlar. Neredeyse sonsuz düzeyde ölçeklenebilir olan bu çözüm; lisans, uzaktan sorun giderme ve ağ kontrollerine erişim sağlar. Merkezi yönetim; Active Directory entegrasyonu, rol tabanlı model ve entegre panolarla tamamlanır.

Hassas verilere ve kayıt cihazlarına erişimi düzenleyin

Çözümümüz, atanan güven düzeylerine göre uygulama ayrıcalıklarını ve şifrelenmiş veriler gibi kaynaklara erişimi sınırlar. Host Intrusion Prevention System (HIPS), yerel ve bulut (KSN) bilinirlik veri tabanlarıyla birlikte çalışarak uygulamaları kontrol eder ve kritik sistem kaynaklarına, ses ve video kayıt cihazlarına erişimi kısıtlar.

Web tehditlerini uç noktalarınıza ulaşmadan önce durdurun

Gelen tehditlerin büyük çoğunluğunu ağ geçidi düzeyinde durdurarak uç noktalara ulaşmalarını engelliyoruz. Bu sayede insan faktörü ve iş istasyonu güvenlik özellikleri etkisini önemli ölçüde azaltıyoruz.

Güvenli bir ağ geçidi, mobilitenin çalışma süreçlerine nüfuz etmesine rağmen kurumsal güvenlik senaryolarının büyük çoğunluğu için ilk savunma hattıdır. Güvenlik teknolojilerimiz, ağ geçitlerinden akan trafiği filtreleyerek gelen tehditleri uç noktalarınıza ve sunucularınıza ulaşmadan önce otomatik olarak engeller. Bu sayede güvenlik açıklarından yararlanılma ihtimali ve BT güvenlik personelinin işletim maliyetleri önemli ölçüde azalır.

Verimliliği artırın ve tehditleri azaltın

Kaspersky Lab'in istenmeyen postalara karşı bulut destekli Yeni Nesil koruması, hatalı pozitifler nedeniyle değerli e-postaların silinmesini minimum düzeye indirirken en gelişmiş ve bilinmeyen e-posta saldırılarını bile tespit eder. İstenmeyen e-postaları, size ulaşmadan önce durdurarak bu postalar için harcanan zamanın ve kaynakların yanı sıra ilgili risklerin de azalmasına yardımcı olur. Bu sayede sistem ve insan kaynaklarınızdan tasarruf edebilirsiniz. Koruma işlevi, gelen e-postalardaki kötü amaçlı ekleri, bilinen ve bilinmeyen kötü amaçlı yazılımları filtrelemek için makine öğrenimi ve bulut destekli tehdit istihbaratı dahil olmak üzere birden çok proaktif güvenlik katmanı içerir.

Güvenli işbirliğini etkinleştirin

Microsoft Sharepoint® güvenlik hizmetimiz, işletmenizin işbirliği ilkelerini uygulaması ve şirket ağınızda uygunsuz içeriklerin depolanmasını önlemek için kötü amaçlı yazılımdan koruma, içerik filtreleme ve dosya filtreleme özelliklerini içerir.

Kaspersky Endpoint Security for Business, yöneticilerin BT ortamlarını görmesini, izlemesini, kontrol etmesini ve korumasını sağlar. Yeni Nesil araçlarımız ve teknolojilerimiz, işinizin her aşamasında artan güvenlik ve BT ihtiyaçlarınızı karşılamak için farklı düzeylerdeki ürünlerle dengelenmiştir.

Kaspersky® Total Security for Business

Yeni ve eski sistemlerin birleşiminden oluşan gelişmiş BT ortamlarına sahip işletmeler, güvenlik ayarlarını farklı sistemler için incelikli bir şekilde ayarlamalıdır. Uç noktalar, altyapı ve işbirliği sunucuları için en kapsamlı güvenlik çözümümüz, tam olarak bunu yapmanızı sağlar. Böylece BT varlığınıza göre yapılandırabileceğiniz sıkı güvenlik önlemlerine sahip olabilirsiniz.

Kaspersky® Endpoint Security for Business Advanced

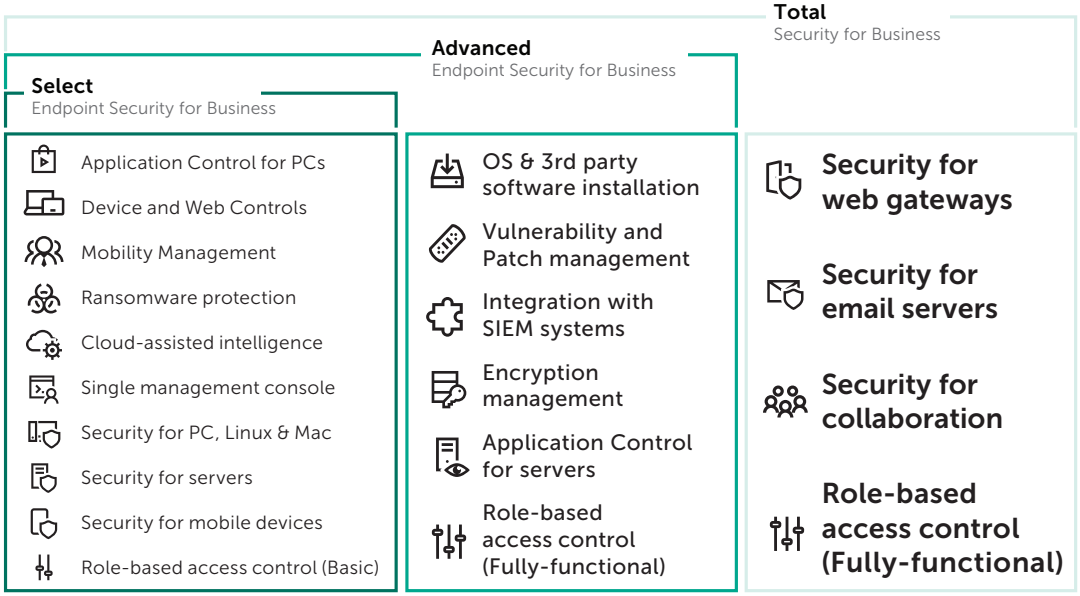
İşletmenizi korumak için daha fazla çalışan bir güvenlik çözümü istiyorsanız **Kaspersky Endpoint Security for Business Advanced** çözümünü seçin. Tüm uç nokta ve sunucularınızın güvenliğini sağlamanın yanı sıra hassas verileri korumak ve güvenlik açıklarını ortadan kaldırmak için ek güvenlik katmanları sunar ve sistem yönetim görevlerinin basitleştirilmesine yardımcı olur.

Kaspersky® Endpoint Security for Business Select

İşletmenizdeki operasyonlar dijital ortama taşındıkça her sunucu, dizüstü bilgisayar ve mobil cihazı korumanız gerekir. İşletmenizdeki her uç noktayı tek bir esnek yönetim konsolunda tek bir çözümle korumanıza yardımcı olan Yeni Nesil güvenlik hizmetleri sunuyoruz.

Sizin için doğru sürüm hangisi?

Kaspersky Endpoint Security for Business, her türlü benzersiz ve sürekli gelişen BT ihtiyacınız için ideal çözümü sunar.



İhtiyacınız olduğunda daha fazla güvenlik özelliği ekleyin

Yazılım güvenlik açıklarını ve düzeltme eki yönetimini otomatikleştirmek ve merkezileştirmek, fidye yazılımı dahil olmak üzere birçok tehlikeli tehdide karşı koruma sağlar. **Kaspersky Endpoint Security for Business Select** müşterilerimiz için bu otomasyon **Kaspersky Vulnerability and Patch Management Eklentisi** ile kullanılabilir.

Ayrıca Select müşterilerimiz için **Kaspersky Encryption Eklentisi**, Tam Disk ve Dosya Düzeyinde Şifreleme sağlar. Bu eklenti, güçlü şifreleme algoritmaları kullanır ve iki adımlı doğrulama için akıllı kartların/belirteçlerin yanı sıra şifreli dosyalara anında erişim için Tek Seferlik Oturum Açma desteği sunar. Bu sayede yerel olarak ve çıkarılabilir sürücülerde depolanan dosyaları ve klasörleri şifreleyebilirsiniz.

Daha fazla karmaşıklığa neden olmadan ek güvenlik özellikleri için Kaspersky Security Center'dan gerekli özellik setini etkinleştirmeniz yeterlidir.

Geçerli uç nokta korumanızı neden yükseltmelisiniz?

Her zaman en yeni teknolojilere sahip olun. Hızlı ve kolay: tek bir sunucu, tek bir konsol, tek bir aracı

Her türlü iş sürecini daha derin entegrasyon ile destekleyin: Kurum içinde geliştirilen tek kod tabanı

Gizli maliyetlerden ve ayrı lisanslardan kaçının: Tek bir ürünü satın alarak istediğiniz tüm işlevlere sahip olun

Gelişmiş denetim ve kontrol becerisi: Rol tabanlı erişimle birleştirilmiş yönetim

Kaspersky Lab olarak tüm teknolojilerimizi kendi şirketimizde geliştiriyoruz. Bu nedenle uygulamalarımız daha dengeli ve verimlidir. Kendi Ar-Ge modelimize bağlıyız ve birçok teknolojik yeniliği ürünlerimize dahil ediyoruz. Aşağıda bu yeniliklerle ilgili birkaç örnek görebilirsiniz:

- Çok Katmanlı Makine Öğrenimi: uç noktalarda ve bulutta ölüm zincirinin farklı aşamalarında Makine Öğrenimi yöntemlerini kullanma.
- Uç nokta koruması ile Uç Nokta Tespit ve Yanıtı ya da Hedefli Tehditlere Karşı Koruma çözümlerimiz arasındaki entegrasyonun bir sonucu olarak etkin tehdit avı.
- Bileşenleri korumak için benzersiz bulut modu, bilgisayar kaynaklarını ve internet bant genişliği kullanımını minimum düzeyde etkileyerek optimum koruma sağlar.
- Microsoft Windows Server kapsayıcıları, dış trafik güvenliği ve güvenlik duvarı yönetimi için destek.
- Gelişmiş Cihaz Kontrolü ve Köprü Kurmaya Karşı Koruma işlevi.
- Güvenilen Sertifikalar kategorisi ile Gelişmiş Uygulama Kontrolü ve ilkeler için Test Modu.
- Yeni ve kolay anlaşılır kullanıcı arabirimi, koruma durumunu ve Kaspersky Lab'in en yeni teknolojilerinin verimliliğini göstererek çok katmanlı korumayı görselleştirir.

Gerçek Siber Güvenlik: DNA'mızda var

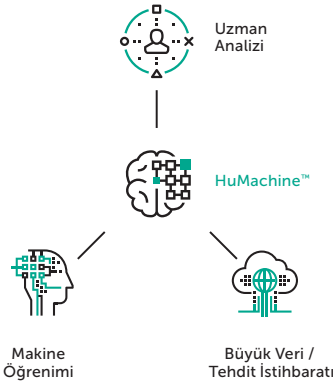
Kaspersky Lab, DNA'mızda bulunan dünya lideri tehdit istihbaratını kullanarak güçlü siber güvenlik çözümleri sunar. Bu DNA yaptığımız her işi etkiler. Bağımsız bir şirket olarak daha çeviğiz, farklı düşünürüz ve daha hızlı hareket ederiz.

- **Uzmanlığımız, CEO'muz Eugene Kaspersky'den başlar.**
- **Global Araştırma ve Analiz Ekibi'miz(GReAT)**, BT güvenliği uzmanlarından oluşan seçkin bir gruptur ve dünyadaki en tehlikeli kötü amaçlı tehditleri ve hedefli saldırıları ortaya çıkarma konusunda liderdir.
- Çığır açan **Global Şeffaflık Girişimimiz**, müşterilerimizi, tehditlerin kökenine ve amacına bakmaksızın tüm siber tehditlerden korumak için verdiğimiz söze bağlılığımızı gösterir.

Gerçek Siber Güvenlik ile Avrupa Birliği Genel Veri Koruma Yönetmeliği'ne uyumluluğunu güçlendirin
Kaspersky Lab, Avrupa Birliği Genel Veri Koruma Yönetmeliği'ndeki siber güvenlikle ilgili konular hakkında farkındalığı artırır. Çözümlerimiz, müşterilerimizin veri ihlali riskini azaltmalarına ve güvenlik olaylarını önlemelerine yardımcı olur. Ayrıca izlenen altyapıda daha gelişmiş bir görünürlük sağlayarak müşterilerimizin Veri Koruma Görevlilerine yardımcı oluruz.

Büyük Resim - Kaspersky Kurumsal BT Güvenlik Çözümleri

Uç nokta koruması ne kadar önemli olsa da yalnızca bir başlangıçtır. İster türünün en iyisi ister tek kaynaklı bir güvenlik stratejisi kullanın, Kaspersky Lab birbirine bağlı veya bağımsız çalışabilen çok çeşitli ürünler sunar. Bu sayede performanstan, verimlilikten veya seçim özgürlüğünüzden taviz vermeden istediğiniz stratejiyi özenle seçebilirsiniz. Web sitemizden daha fazla bilgi edinebilirsiniz.



Kaspersky Lab
Size en yakın iş ortağımızı bulun: https://www.kasperskypartners.com/et.cfm?eid=global
Kaspersky for Business: https://www.kaspersky.com.tr/small-to-medium-business-security
Gerçek Siber Güvenlik: https://www.kaspersky.com.tr/true-cybersecurity
BT Güvenlik Haberleri: https://www.kaspersky.com.tr/blog/

#truecybersecurity
#HuMachine

www.kaspersky.com.tr