kaspersky GELECEĞİ YAKALAYIN

Kaspersky Endpoint Security for Business

Teknoloji iş için dönüştürücü bir güçtür – hızınızı koruyun veya yavaşlayın. Ancak teknoloji aynı zamanda suçlulara da kapılar açıyor ve uç noktaları birincil hedef haline geliyor. Bu nedenle, işinizin en çok değer verdiği şeyleri korumak için titiz ve güvenilir çözümler üreterek sizi hedef alan siber suçlulardan daha akıllı olmanız gerekir.

Zorluklar

Saldırılardan kaynaklanan artan baskı

Şimdi siber suç araçları o kadar ucuz ki, güvenlik olaylarında ve risklerinde dramatik bir artış görüyoruz. Fidye yazılımı, finansal casus yazılım, kimlik avı ve diğer tehditler, özellikle dijital dönüşümün sancıları içindeyseniz, kuruluşunuzu ciddi kayıplarla vurabilir.

Korumak için heterojen bir altyapı

Uzaktan çalışma, bulut hizmetleri ve çevik süreçlerin yaygınlaşması, tüm güvenlik stratejilerinin iş için kullanılan kişisel cihazlar da dahil olmak üzere dizüstü bilgisayarlar, iş istasyonları, sunucular ve cep telefonları dahil olmak üzere uç nokta cihazlarınızın tamamını kapsamasını gerektirmektedir. Desteklediğiniz tüm çeşitli işletim sistemleri hakkında da düşünmeniz gerekir.

Üstesinden gelinmesi gereken yüksek düzeyde karmaşıklık

Karmaşık bir BT altyapısı ve onu desteklemek ve korumak için gerekli uzmanlığın hepsinin bir maliyeti vardır. Zaman, bütçe, personel ve belirli beceriler açısından değişen kurumsal güvenlik gereksinimlerinizi karşılamak için doğru çözümlere etkili bir şekilde yatırım yapmanız gerekir.

Çözüm

Hızlı uyarlanabilir güvenlik

Şunları yapabilmeniz gerekir:

- Performansınızı etkilemeden verilerinizi, çalışanlarınızı ve altyapınızı tam olarak korumak.
- Size doğru gelen yeni ve ortaya çıkan tehditleri tespit etmek ve bunlara karşı koymak için en son ve en güvenilir tehdit istihbaratına güvenmek.
- Tehdit davranış kalıplarını tanımak, böylece bilinmeyen tehditler bile etkisiz hale getirilebilir.
- Hangi uygulamaların, web sitelerinin ve cihazların uç noktalarınız ve kullanıcılarınızla etkileşime girebileceğini kontrol ederek saldırı yüzeyinizi azaltmak.

Her platform için tek bir çözüm

Arayacaklarınız şunlardır:

- Nerede olursa olsun ve sahibi siz olun ya da olmayın, verilerinizi taşıyan her iş istasyonu, sunucu ve mobil cihaz için mümkün olan en iyi güvenlik. Tehdit giriş noktalarını ve ekibinize daha fazla iş çıkarmadan web ve e-posta ağ geçitlerini nasıl koruyacağınızı da düşünün.
- Windows, Mac, Linux, iOS ve Android dahil olmak üzere karışık ortamınızdaki tüm işletim sistemlerini tek bir konsoldan çalışarak tek bir çözümle kapsayabileceğinizin güvencesi.

Esnek yönetim ve görev otomasyonu

Ve aşağıdakilerle kaynaklarınızı en üst düzeye çıkarmak isteyeceksiniz:

- Yüksek düzeyde otomasyon - özellikle yama ve işletim sistemi dağıtımı gibi temel ancak rutin görevler için. Ekibinizin zaman ve uzmanlığı boşa harcanmayacak kadar değerlidir.
- Uzaktan yönetim özellikleri - ister ev ofislerinde iş istasyonları kurun, ister şifreleme seçenekleriyle verileri güvence altına alın.
- Merkezileştirme. Konsollar arasında dolaşmak yok - çevrenizde veya bulutta basit, entegre tek ekran yönetimine ihtiyacınız var.

Veri ihlallerinin maliyeti

KOBİ'ler için $105 bin

İşletmeler için $927 bin

$101k	▲ $105 bin	$1.09m	▼ $927k
2020	2021	2020	2021

Kaynak: Kaspersky BT güvenlik ekonomisi raporu 2021

Üç Kademeli özellik paketi

Kaspersky Endpoint Security for Business'daki araçlar ve teknolojiler, işiniz büyüdükçe gelişen güvenlik ve BT ihtiyaçlarını karşılamak için aşamalı kademelerde akıllıca dengelenir.

En çok ödül alan... ve müşterilerimizin memnun kaldığı güvenlik

Kaspersky ürünleri, 2013 ve 2021 yılları arasında 741 bağımsız test ve incelemede yer almıştır. Ürünlerimiz 518 kez birincilik ödülüne layık görüldü. Daha fazla ayrıntı için bkz. www.kaspersky.com/top3

Fidye yazılımı tehditleri

Bu saldırılar, son yılların en dikkate değer saldırılarından bazıları büyük markaları vurarak bireylere veya şirketlere yapılmıştır.

Daha önce fidye yazılımı saldırısına uğrayan şirketlerin yöneticilerinin %88'i, tekrar saldırıya uğramaları halinde ödeme yapacaklarını söyledi.

Fidye yazılımları, dünya genelinde işletmeler için giderek büyüyen bir sorun olup, fidye yazılımlarının kullanıldığı saldırıların sayısı yalnızca 2021 yılında neredeyse iki katına çıkmıştır. Bu durum kısmen, daha fazla insanın evden çalışmasına neden olan pandemiye bağlanabilir. Ancak, kalacak gibi görünen bir hibrit çalışma modeliyle, bir fidye yazılımı saldırısı olasılığı devam ediyor.

Sizin için sunduklarımız

- Gerçek güvenlik. Dosyasız saldırı **koruması, ML tabanlı davranış analizi ve kötüye kullanımlara, fidye yazılımlarına ve finansal casus yazılımlara karşı özel koruma** gibi Kaspersky teknolojilerinin **benzersiz performansı sayesinde**, tüm uç noktalarınızı yaygın ve yeni ortaya çıkan tehditlere karşı tamamen koruyoruz.
- Proaktif koruma. Onlar başlamadan saldırıları durduracağız. Uyarlamalı Anomali **Kontrolü ile ön yürütme koruması, davranış analizi temelinde engelleme kurallarının basitliğini otomatik ayarın akıllılığıyla** birleştirir.
- Büyüyen BT güvenliği olgunluğunuz için eksiksiz bir ekosistem. Otomatik yanıt ve analiz, EDR ve **SIEM** çözümleri **ile** entegrasyonları güçlendirir.
- Paranızın karşılığı. Katmanlı yaklaşımımız, şu anda yalnızca ihtiyaç duyduğunuz yetenekler için ödeme yaptığınız anlamına gelir.
- Geleceğe yönelik koruma. Yükseltme sorunsuzdur – sadece katmanlar arasında ilerleyin. Tamamen ölçeklenebilir çözümümüz, siz **büyüdükçe yönetilen** binlerce cihazı desteklemeye hazırdır.
- **Kolaylaştırılmış bulut adaptasyonu. Microsoft Office 365** için gelişmiş koruma
- Esneklik. **Tercih ettiğiniz dağıtım seçeneğini seçin**: bulutta, şirket içi ve hibrit dağıtımlarda. Ardından, granül role dayalı erişim kontrolü **(RBAC)** ile farklı ekip üyelerine farklı düzeylerde güvenlik sistemleri erişimi tahsis edin.
- İçinizin rahat olmasını sağlama. Tüm hassas verileriniz, dosya ve tam disk seviyelerinde ve harici cihazlarda şifreleme yönetimi de **dahil olmak üzere bir** veri koruma özelliği seti ile tam olarak korunur. Uzaktan veri silme, bir cihazın kaybolması veya çalınması durumunda verileri siler.
- Çevre savunması. **Web tabanlı saldırıların** ana hedeflerine (kullanıcılarınız ve uç noktaları) ulaşmasını önleme

Kullanım durumları

Sistemlerinizi otomatik olarak savun

Davranış tabanlı algılama, Kaspersky'nin çok katmanlı, yeni nesil koruma yaklaşımının bir parçasıdır. Bu çözüm; dosyasız kötü amaçlı yazılım, fidye yazılımı ve sıfır gün kötü amaçlı yazılım gibi gelişmiş tehditlere karşı korunmanın etkili yollarından biridir.

Kaspersky Security Network'ten gelen verilerin kullanılması, yeni tehditlere daha hızlı yanıt verilmesini sağlar, koruma bileşenlerinin performansını iyileştirir ve yanlış pozitiflerin olasılığını azaltır. Günün sonunda, üstün algılama oranları ve yerleşik uyarlanabilir güvenlik, minimum yanlış pozitiflerle saldırılara hızlı bir yanıt anlamına gelir. Kaspersky, yakın tarihli bir AV-Test çalışmasında % 100 fidye yazılımı koruma oranına sahip tek siber güvenlik satıcısıdır. AV-Test Gelişmiş Uç Nokta Koruması: Fidye Yazılımı Koruma testi, AV-Testi, 30 Eylül 2021

Saldırı yüzeyinizi azaltın

Uzak cihazları kurumsal BT güvenliğinizle uyumlu hale getirin. Uygulama kontrolleri hem üretkenliği (örneğin oyun uygulamalarına veya sosyal ağlara erişimi kısıtlayarak) hem de güvenliği etkiler Çalışanlar, korsan uygulamalar ve şüpheli web sitelerinde kimlik avı ve kötü amaçlı yazılım kurbanı olabilirken, sadece bir USB modem, ağ yazıcısı takmak hassas veri sızıntısına neden olabilir. Tüm bu saldırı vektörleri, artı insan hatasından kaynaklanan risk, granüler Uygulama, Web ve Cihaz kontrolleri uygulanarak önemli ölçüde azaltılabilir.

Adaptif Anomali Kontrolü, ortak politikaları güçlendirebileceğiniz ve sistemin kullanıcı davranışına dayalı olarak kuralları nasıl uygulayacağını görebileceğiniz anlamına gelir.

Zaman, gayret ve maliyetleri en aza indirin

Kaspersky Endpoint Security for Business'ı bulut konsolundan yönetin.

SaaS tabanlı bu yaklaşım donanım yatırımı gerektirmez ve güncellemeler, destek ve kullanılabilirlik için zaman harcamak yerine iş girişimlerine odaklanmanızı sağlar - bulut altyapımız her şeyle ilgilenir.

Ekibinizin uç nokta sertleştirme, uzaktan cihaz yönetimi, işletim sistemi dağıtımı, yama ve şifreleme yönetimi için harcadığı zamanı düşünün. Kaspersky Endpoint Security, tüm bu görevleri ve daha fazlasını kolaylaştırır ve otomatikleştirir – her şeyi yönetmek için tek bir çözüm ve bir web arayüzü sağlar. Artık her görev veya cihaz türü için ayrı konsollar veya farklı ürünler yok.

Güçlü bir veri koruma duruşu oluşturun

Günümüz saldırıları, tehdit aktörlerinin ortak uygulamalarda yeni güvenlik açıkları ve sıfır gün avantajları bulmalarına olanak tanıyan meşru araçlar ve uygulamalar kullanmaktadır. Otomatik yama yönetimi, bu saldırılardan kaynaklanan verileriniz için riski önemli ölçüde azaltırken, veri şifreleme yalnızca meşru kullanıcıların belirli hassas dosyalara veya harici cihazlara erişmesini sağlar. Tam sabit disk şifrelemesi, bir cihazın kaybolması veya çalınması durumunda da verileri korur.

Kaspersky Total Security for Business'ta bulunan entegrasyon ayrıca Microsoft Office 365 işbirliğini ve dosya paylaşımını korur ve PII (Kişisel Tanımlama Bilgileri) sızıntısını önlemeye yardımcı olur.

KENDINIZ IÇIN DENEYIMLEYIN

Neden kendiniz için uyarlanabilir korumamızı deneyimlemiyorsunuz? Kaspersky Endpoint Security for Business ın 30 günlük ücretsiz denemesi için bu sayfayı ziyaret edin.

Aşama aşama bir yaklaşım

Doğru ürün veya hizmeti seçerek kuruluşunuz için bir güvenlik temeli oluşturmak sadece ilk adımdır. İleriye dönük bir kurumsal siber güvenlik stratejisi geliştirmek, uzun vadeli başarının anahtarıdır.

Portföyümüz, kuruluşunuzun büyüklüğü veya BT güvenlik olgunluk seviyeniz ne olursa olsun, kurumsal ihtiyaçlarınıza her aşamada benzersiz bir yaklaşımla yanıt vererek, günümüz işletmelerinin güvenlik taleplerini yansıtmaktadır.

Bu yaklaşım, her tür siber tehdide karşı farklı koruma katmanlarını birleştirir ve tehditleri otomatik olarak önlemeye yardımcı olur – daha sonra işiniz geliştikçe daha sofistike tehditlere karşı koymak için sistematik ve yöntemsel olarak yeni ve gelişmiş yetenekler eklemenizi sağlar. Resmin tamamını görüyoruz, böylece inovasyona korkusuzca odaklanabilirsiniz.

---

* (kişisel tanımlayıcı bilgiler)

Kaspersky Security Foundations

- Kaspersky Endpoint Security for Business
- Kaspersky Hybrid Cloud Security
- Kaspersky Embedded System Security
- Kaspersky Security for Storage
- Kaspersky Security for Mail Server
- Kaspersky Security for Internet Gateway
- Kaspersky Professional Services
- Kaspersky Premium Support and Professional Services

- Kurumsal kullanıcılar ve taşınabilir cihazlar için koruma
- Hibrit ortamlar için sunucu güvenliği
- Sanal Masaüstü Bilgisayarlar için Koruma (VDI)
- Özel uç noktalar ve eski bilgisayarlar için koruma
- En yaygın saldırı vektörüne karşı koruma – e – posta
- Web tabanlı tehditlere karşı ön koruma
- Dağıtım, yapılandırma ve bakım yardımı

Kaspersky ekosisteminin tam potansiyelinden yararlanın

Kaspersky Security Foundations

Bulut tarafından yönetilen tehdit önleme aşamamız, her kuruluşun herhangi bir cihaz, VDI ve hibrit sunucu altyapısındaki mal siber tehditlerini otomatik olarak durdurmasını sağlar.

- Uzmanlaşmış ve eski uç noktalar da dahil olmak üzere tüm cihazları korur
- Her BT varlığı üzerinde görünürlük ve kontrol sağlar
- Kullanıcı hatalarını önlemeye veya azaltmaya yardımcı olur
- Bankayı kırmadan ihtiyaç duyduğunuz sistem yönetimi otomasyonunu sağlar

Kaspersky Optimum Security

İşletmeleri yeni, bilinmeyen ve sinsi tehditlerden korumaya yardımcı olur. Etkili tehdit algılama ve yanıt çözümü, kaynaklar için kolay. 7/24 güvenlik izleme, otomatik tehdit avcılığı ve Kaspersky uzmanları tarafından desteklenen rehberli ve yönetilen yanıtlar.

- Sinsi tehditlere karşı uç nokta korumasını yükseltir
- Temel olay müdahale süreçlerinin oluşturulmasını destekler
- Siber güvenlik kaynak kullanımını optimize eder

Kaspersky Expert Security

APT'ler (Gelişmiş Kalıcı Tehditler) ve hedefli saldırılar da dahil olmak üzere en sofistike güncel tehditlerle başa çıkmada herhangi bir BT güvenlik odaklı kuruluşun günlük ihtiyaçlarını karşılamak için tasarlanmıştır.

- Uzmanlarınızın iş yüklerini optimize eder
- Bilgi ve becerilerini geliştirir
- Uzmanlarınızı yedekler

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

kaspersky.com.tr

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

kaspersky.com.tr/transparency adresini ziyaret ederek daha fazla bilgi alın

Proven. Transparent. Independent.