Kaspersky Endpoint Security for Business SELECT

Kaspersky Endpoint Security for Business, herhangi bir cihazda ve herhangi bir platformda, her büyüklükten işletmeyi her tür siber tehdide karşı korur. Güçlü ve çok katmanlı güvenlik, kapsamlı yönetim özellikleri ile desteklenmektedir.

- İşletmenizin büyüklüğünden veya hangi platformları kullandığınızdan bağımsız olarak ihtiyaçlarınıza uyum sağlayan, kullanımı kolay, esnek çözüm.
- Büyük veri tehdit istihbaratı, otomatik öğrenme ve insan uzmanlığını benzersiz bir şekilde birleştirilerek sunulan çok katmanlı koruma.
- Granüler güvenlik yönetimi, tüm güvenlik sorunlarını ekstra entegrasyon ve yönetim çözümlerine ihtiyaç duymadan yönetmeyi ve kontrol etmeyi kolaylaştırır.
- Müşterilere mümkün olan en iyi korumayı sunduğu, bağımsız testlerle kanıtlanmıştır. Kaspersky Lab, dünyanın en çok test edilen, en çok ödül alan ve sektörde en yüksek algılama oranına sahip güvenliğidir.
-

- Kaspersky Endpoint Security for Business Select, BT altyapınızda bulunan tüm cihazlar için dayanıklı sistem kontrollerini güçlü güvenlik ile birleştirir ve tümünü tek, merkezi, yüksek düzeyde entegre yönetim konsolundan gerçekleştirir.
  - *İşletmenizin karşı karşıya olduğu siber tehditlere karşı koruma*

    Kaspersky Endpoint Security for Business Select, daha yüksek koruma seviyeleri sunan büyük veri tehdit istihbaratı, otomatik öğrenme ve insan uzmanlığını benzersiz bir şekilde birleştirilerek bilinen, bilinmeyen ve gelişmiş tehditlere karşı çok katmanlı koruma sunar.

  - *İş akışınızı ve süreçlerinizi destekleyen koruma*

    Gerçek platform bağımsızlığı, Kaspersky Endpoint Security for Business Select'in, kullandıkları cihaz veya platformdan ya da bunları nerede kullandıklarından bağımsız olarak tüm kullanıcıları koruması anlamına gelir.

  - *Granüler güvenlik yönetimi*

    Kaspersky Endpoint Security for Business Select, tek, yüksek düzeyde entegre yönetim konsolu olan Kaspersky Security Center'ı içerir; bu sayede ağdaki tüm cihazlar üzerinde merkezi bir kontrol sunulur. Belirli ihtiyaçlarınıza göre kendi ilkelerinizi oluşturun veya Kaspersky Lab uzmanları tarafından geliştirilen, önceden yapılandırılmış ilkeler kullanarak hemen işe koyulun.

GVG Bilişim Hizmetleri Sanayi ve Ticaret Limited Şirketi
Uğur Mumcunun Sokağı 61/2 G.O.P. 06600 Çankaya Ankara
Tel: +90 312 475 42 90 Fax: +90 312 475 26 90

- *Esneklik ve tam ölçeklenebilirlik*

  - Kaspersky Security for Virtualization
  - Kaspersky Security for Mail Server
  - Kaspersky Security for Storage
  - Kaspersky Security for Internet Gateway
  - Kaspersky Security for Collaboration
  - Kaspersky Vulnerability and Patch Management

ÖZELLİKLER;

- Dizüstü bilgisayarlar, iş istasyonları, sunucular ve mobil cihazlar için endüstrinin öncü güvenlik uzmanları tarafından tasarlanan ve oluşturulan güçlü çok katmanlı koruma*.

**Tam özellik seti platforma göre değişiklik gösterir.*

- *Masaüstü bilgisayarlar, sunucular ve mobil cihazlar için çok katmanlı güvenlik*

Çok katmanlı güvenlik ve kontrol

Kaspersky Endpoint Security for Business Select, sürekli değişen siber tehdit ortamına karşı tüm cihazları ve ortamları korumak için birçok teknolojiyi bir araya getirir. Güvenlik kontrolleri ile Automatic Exploit Prevention, Host-Based Intrusion Prevention System ve diğerleri, izinsiz kötü amaçlı yazılım girişi olasılığını önemli ölçüde azaltır. Birçok diğer teknoloji ve süreç, uç noktadaki kötü amaçlı yazılımı algılayıp tanımlayarak anında durdurur ve bu yazılımın eylemlerini geri alır.

Otomatik öğrenme ve insan zekasının en iyisi

Kaspersky Lab'in benzersiz HuMachine™ yaklaşımı, büyük veri tehdit istihbaratı, otomatik öğrenme ve insan uzmanlığını bir araya getirerek karmaşıklık veya yönetim sorunları olmadan daha yüksek düzeyde çok katmanlı algılama sunar.

Bulut zekasının gücünü kullanma

Dünya çapındaki milyonlarca Kaspersky müşterisi, kendi cihazlarından Kaspersky Security Network'e (KSN) gönüllü olarak anonim tehdit verileri sağlıyor. Bu bulut tabanlı tehdit laboratuvarı, şüpheli dosyalardan çok büyük hacimlerde meta veri toplayıp depolayarak içeriklerin tamamen analiz edilmesine gerek kalmadan dosyaların ve URL'lerin güvenliği ile ilgili hızlı, hassas kararlar alınmasını sağlar. Bu da, bilinmeyen tehditlere karşı koruma sunar.

GVG Bilişim Hizmetleri Sanayi ve Ticaret Limited Şirketi
Uğur Mumcunun Sokağı 61/2 G.O.P. 06600 Çankaya Ankara
Tel: +90 312 475 42 90 Fax: +90 312 475 26 90

Şüpheli davranışı algılama

Kaspersky Endpoint Security for Business Select, hem çalıştırma öncesi hem de çalıştırma aşamasında davranışsal algılama yöntemini kullanır. Davranışsal algılama, çok büyük miktarlarda şüpheli dosya meta verisi depolayan Kaspersky Security Network tarafından desteklenmektedir.

Öykünmeden faydalanan davranışsal algılama, dosya başlatılmadan önce bilinmeyen ve gelişmiş tehditleri tanımlamada önemli bir rol oynar. Bir uygulama başlatıldığında Sistem İzleyici, dosyaları izleyerek ve bilinen kötü amaçlı uygulamalarla kıyaslayarak herhangi bir şüpheli etkinlik olup olmadığına bakar. Kötü amaçlı dosya engellenir ve tüm eylemler otomatik olarak geri alınır.

Açıklardan yararlanmaya karşı koruma

Hiçbir uygulama veya işletim sistemi, güvenlik açıklıklarından %100 arınmış bir çözüm sunamaz. Kötü amaçlı yazılım bu güvenlik açıklıklarından yararlanarak ağınıza sızabilir, iş istasyonlarınız ve sunucularınıza bulaşabilir ve işlerinizi aksatabilir. Yenilikçi Otomatik Kullanma Engelleme (AEP) teknolojimiz, kötü amaçlı yazılımların işletim sistemleri veya ağınızda çalışan uygulamalardaki güvenlik açıklarından faydalanmasını önlemeye yardımcı olur. Otomatik Kullanma Engelleme, bilinmeyen tehditlere karşı ekstra güvenlik takibi ve koruma katmanı sunmak amacıyla Adobe Reader, Internet Explorer, Microsoft Office ve Java gibi en sık hedef alınan uygulamaları özel olarak izler.

Kurumsal ağı koruma

Bağlantı noktası tarama, hizmet reddetme saldırıları ve arabellek taşması saldırıları gibi kurumsal ağları hedefleyen tehditlerin sayısı giderek artmakta. Kaspersky Endpoint Security for Business Select'te bulunan Ağ Saldırısı Engelleyici teknolojisi, kurumsal ağınızdaki şüpheli davranışları algılar ve izler ve şüpheli bir davranış meydana geldiğinde sistemlerinizin nasıl yanıt vereceğini önceden yapılandırmanıza olanak sağlar.

- *Uygulamaları, cihazları ve İnternet erişimini yönetmek için güvenlik kontrolleri*

Uygulama denetimi için dinamik beyaz liste

Piyasada binlerce yeni uygulama mevcut ve bu sayı gün geçtikçe artıyor. Hangilerinin tehlikeli olma potansiyeli taşıdığını, hangilerinin taşımadığını takip etmek zor bir iştir. Kaspersky'nin dinamik beyaz liste yaklaşımı, sistem yöneticilerinin beyaz listenizde yer almayan tüm uygulamaları engelleyen Varsayılan Olarak Reddet ilkesini etkinleştirmelerini sağlar. Şirket bünyemizdeki beyaz listeye alma laboratuvarı, uygulamaları sürekli kontrol ederek beyaz listeye alınan uygulamalar veri tabanına ekler (bu veri tabanında 1,3 milyar benzersiz dosya yer alır ve her gün 1 milyon dosya eklenmektedir). Kaspersky müşterileri bu veri tabanına erişim sağlayarak bunu olduğu gibi kullanabilir veya belirli işletme gereksinimlerine uyarlayabilirler. Test modu, işletme için önemli olan uygulamaların kazara engellenmemesini ve işlevsellik üzerinde istenmeyen bir etki bırakmamasını sağlar.

Sunucular ve iş istasyonlarından uygulamaları kontrol etme

Sistem İzleyici teknolojimiz bir uygulamanın davranışlarını, uygulama sunucuda veya çalışan makinesinde çalıştırıldığında izleyerek kötü amaçlı yazılım etkinliklerini belirler. Kötü amaçlı dosyalar engellenir ve kötü amaçlı yazılım etkinlikleri iş istasyonlarından geri alınır.

Riskleri en aza indirmek için uygulama önceliklerini kontrol etme

Kötü amaçlı olarak sınıflandırılmış olmasalar bile bazı uygulamaların etkinlikleri yüksek riskli olarak kabul edilebilir. Çoğu durumda, bu etkinliklerin kısıtlanması önerilir. Application Privilege Control (Host-Based Intrusion Prevention System – HIPS) teknolojimiz, uygulamaya atanan "güvenlik seviyesi"ne göre uç nokta içindeki eylemleri kısıtlar ve uygulamaların, sistem ve kullanıcı dosyaları dahil belirli kaynaklara erişim sağlamasını sınırlar. Uygulamaların ses ve video kayıt cihazlarına erişimi de kontrol edilebilir.

Yetkisiz cihazların erişim sağlamasını önleme

Kaspersky'nin cihaz kontrolleri, yetkisiz cihazların ağınıza erişim sağlamasını önlemek için günün saatine, coğrafi konuma veya cihaz türüne göre kontrolleri ayarlamanızı sağlar. Granüler yönetim ve ilke ataması için kontrolleri Active Directory ile uyumlu hale getirebilir ve Cihaz Kontrol kuralları oluştururken maskeler kullanabilir ve de gerekirse birden fazla cihazı beyaz listeye alabilirsiniz. Kaspersky Endpoint Security for Business aynı zamanda çıkarılabilir USB cihazlarında gerçekleştirilen tüm "sil ve kopyala" işlemlerini kaydeder ve CD/DVD'lerdeki "okuma ve yazma" işlemlerinde kullanıcı haklarını yönetir.

Esnek Wi-Fi kontrolü

Halka açık güvenli olmayan Wi-Fi ağları, cihazları ve kurumsal ağı saldırılara açık hale getirir. Çalışanlara özel güvenilir ağ listesi oluşturarak güvenilir Wi-Fi ağlarına erişime izin verebilir ve çalışan mobilitesini etkilemeden diğer ağların kullanımını engelleyebilirsiniz.

İnternet erişimini izleme ve kontrol etme

İş saatleri dahil çevrimiçi olarak gittikçe daha çok zaman geçiriyoruz. Kaspersky'nin web kontrol araçları, İnternet erişimi ilkelerini belirlemenizi ve İnternet kullanımını izlemenizi sağlar. Kullanıcıların oyun web siteleri, sosyal ağlar veya kumar siteleri gibi web siteleri ve/veya web sitesi kategorilerindeki etkinliklerini yasaklamak, sınırlandırmak, denetlemek ve bu etkinliklere izin vermek kolaydır. Coğrafi kontroller ve saat kontrolleri Active Directory ile uyumlu hale getirilerek ilkelerin yönetilmesine ve belirlenmesine yardımcı olur.

- *Masaüstü bilgisayarı aşan güvenlik*

Tüm sunucu ortamlarını koruma

İşletmelerin BT altyapılarını Windows sunucusu, Linux ve FreeBSD küme sunucularından Microsoft ve Citrix terminal sunucularına kadar çeşitli sunucu platformlarında çalıştırmaları alışılmadık bir durum değildir. Kaspersky bunların tümünü korur ve optimize edilmiş işlemler, sunucu performansında minimum

etki anlamına gelir. Dosya sunucularınızdan birinde arıza meydana gelmesi durumunda teknolojilerimiz otomatik olarak dosya sunucunuz ile aynı anda yeniden başlatılır.

Mobil güvenlik sağlama

Mobil cihazlar bugün tüm işletmelerde kullanılıyor ve kurumsal ağınıza giden potansiyel bir yol açıyor. Kaspersky Endpoint Security for Business Select, mobil cihazları en yeni mobil tehditlere karşı korur; kimlik avı koruması teknolojisi bilgi çalmaya çalışan web sitelerine karşı korur; anti-spam istenmeyen aramaları ve mesajları filtreler.

Konteynerleştirme teknolojisi, kurumsal verileri ve uygulamaları kullanıcının kişisel verilerinden ayırarak cihazın kaybolma durumunda kurumsal verileri güvende tutar. Şifreleme ve uzaktan çalıştırılan koruma özellikleri, kişisel verileri ve ayarları etkilemeden kurumsal kapsayıcıyı güvenli bir şekilde silebilir.

- *Merkezi yönetim*

Yönetilebilirlik özelliklerini artırma

Sistem yöneticileri stres altındalar ve yönetim ile rapor oluşturmaya harcanan zaman diğer önemli, temel işletme görevlerine harcanabilir. Kaspersky Endpoint Security for Business Select, işletmenizdeki Kaspersky Lab uç nokta güvenliği teknolojilerinin eksiksiz görüntülenmesini ve kontrolünü sağlayan merkezi, yüksek düzeyde entegre yönetim aracı olan Kaspersky Security Center'ı (KSC) içerir. KSC, kullanışlı "tek pencereli" konsoldan mobil cihazlar, dizüstü bilgisayarlar, masaüstü bilgisayarlar, dosya sunucuları ve sanal makinelerin yönetimini kolaylaştırır ve aynı zamanda rapor oluşturur.

Yaygın MDM platformlarını destekleyerek mobil cihazları yönetme

Tüm mobil cihazlarınızı merkezi olarak yönetmek için tüm öncü mobil cihaz yönetimi platformlarıyla entegre olan bir güvenlik çözümüne ihtiyacınız vardır. Kaspersky Endpoint Security for Business Select; Microsoft® Exchange ActiveSync®, iOS MDM ve Samsung KNOX™ platformlarını destekler ve her biri için zorunlu şifreleme, parola kullanımını zorunlu hale getirme, kamera kullanımı, APN/VPN ayarları gibi kolay ilke oluşturmayı sağlar. Android for Work, kurumsal profil oluşturma ve kurumsal uygulama ve cihaz yönetimine olanak tanır.

Yüksek düzeyde entegrasyon özelliği

Kaspersky Endpoint Security Select'te bulunan teknoloji, şirket bünyesinde yüksek düzeyde entegre bir kod ile geliştirilmiştir; bu da, uğraşmanız gereken herhangi bir uyumluluk sorunu olmayacağı anlamına gelir ve ölçeklenebilirlik kolaydır. BT ortamınızı korumak için daha fazlasını yapan kusursuz şekilde entegre edilmiş güvenlik teknolojilerinden faydalanın ve merkezi yönetim sayesinde zamandan tasarruf edin.