Kaspersky Endpoint Security for Business ADVANCED

İşletmeniz büyüdükçe, korumanız gereken veri miktarı ve yönetmeniz gereken cihazlar ve BT sistemleri de onunla birlikte büyür. Güvenlik açıklarını tespit edip kapatmak, tehditleri anında durdurmak ve sistem yönetimi görevlerini kolaylaştırmak için doğru araçlara ihtiyacınız var. Kaspersky Endpoint Security for Business Advanced, BT güvenliği ile BT verimliliğini bir araya getirerek her büyüklükten işletme için esnek, proaktif veri koruma ve çevik siber güvenlik sunar.

- İşletmenizin büyüklüğünden veya hangi platformları kullandığınızdan bağımsız olarak ihtiyaçlarınıza uyum sağlayan, kullanımı kolay, esnek çözüm.
- Büyük veri tehdit istihbaratı, otomatik öğrenme ve insan uzmanlığının benzersiz bir şekilde birleştirilmesiyle güçlendirilmiş çok katmanlı koruma.
- Granüler güvenlik yönetimi, tüm güvenlik sorunlarını ekstra entegrasyon ve yönetim çözümlerine ihtiyaç duymadan yönetmeyi ve kontrol etmeyi kolaylaştırır.
- Güçlü şifreleme hassas verileri korur ve uyumluluk gereksinimlerini karşılar
- Kapsamlı müşteri yönetimi araç seti, BT sistemleri yönetimi verimliliğini artırır
- 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.

AVANTAJLAR

- İşletmelerin BT ortamları, hiç olmadığı kadar karışık ve siber suçlular son derece karmaşık saldırı yöntemleri kullanıyorlar. Kaspersky Endpoint Security for Business Advanced, çok katmanlı koruma sağlamak için kapsamlı güvenlik özellikleri tarafından desteklenen sınıfının en iyisi tehdit korumasını sunar. Güvenlik açığı taraması ve yama yönetimi, güvenlik kontrolleri ve veri koruma, saldırı seçeneklerinin en aza indirilmesini ve hassas iş bilgilerinin güvende kalmasını sağlar.
  - *İşletmenizin karşı karşıya olduğu tüm siber tehditlere karşı koruma*

Kaspersky Endpoint Security for Business Advanced, daha yüksek koruma seviyeleri sunmak için büyük veri tehdit istihbaratı, otomatik öğrenme ve insan uzmanlığının benzersiz bir şekilde birleştirilmesiyle bilinen, bilinmeyen ve gelişmiş tehditlere karşı çok katmanlı koruma sağlar. Güçlü kontrol araçları,

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

uygulamaların nasıl yürütüleceğini yönetmeye, izinsiz çıkarılabilir cihazların kullanımını engellemeye ve internet erişim ilkeleri uygulamaya yardımcı olur.

- *Hassas kurumsal bilgilerin kaybolmasını önler*

  Bir dizüstü bilgisayar veya mobil bir cihazın kaybolması gizli bilgilerin yanlış kişilerin eline geçmesine yol açabilir. Şifreleme özelliklerimiz dosyaların, klasörlerin, disklerin ve çıkarılabilir cihazların şifrelenmesini güçlendirmenize yardım eder. Veri şifrelemesini yapılandırmak kolaydır ve ağınızda çalışan diğer tüm Kaspersky Lab güvenlik teknolojilerini kontrol etmek için kullanılan aynı yönetim konsolundan yönetilebilir.

- *Mobil uç noktaları koruyarak işletme verimliliğini artırma*

  Kaspersky Endpoint Security for Business Advanced, mobil iş gücünün görevlerini güvenli bir şekilde yapmasını sağlar. Sıkı mobil güvenlik teknolojileri, en popüler mobil platformları kötü amaçlı yazılımlara, kimlik avına, spam ve diğer saldırılara karşı korumanızı sağlar. Ayrıca Kaspersky Endpoint Security for Business Advanced, tek bir arabirim üzerinden çeşitli Mobil Cihaz Yönetimi (MDM) ve Mobil Uygulama Yönetimi (MAM) işlevlerini etkinleştirerek zamandan tasarruf etmenizi ve birleşik mobil güvenlik ilkelerini kolayca uygulamanızı sağlar.

- *BT sistemlerinin yönetim verimliliğini artırır*

  Günümüzün karmaşık kurumsal BT ortamlarında, her gün gerçekleştirilmesi gereken temel sistem yönetimi görevlerinin sayıca fazla olması yorucu olabilir. Müşteri yönetimi araçlarımız, çeşitli güvenlik ve yönetim görevlerini otomatik hale getirerek BT yönetim işlerindeki karmaşıklığı azaltır. BT ağınızda görünürlüğünü artırdığınız gibi birçok güvenlik ve yönetim işlevini tek bir sistem ve güvenlik yönetim konsolu üzerinden kontrol edebilirsiniz.

- *Güvenlik yönetimini optimize etme*

  Bir şirkette gittikçe artan sayıdaki cihazların güvenliğini yönetmek karmaşık ve zaman alan bir iş olabilir. Tüm güvenlik teknolojileri üzerinde merkezi kontrol sağlamanıza olanak veren, yüksek düzeyde entegre yönetim konsolumuz Kaspersky Security Center'ın dahil edilmesiyle, Kaspersky Endpoint Security for Business Advanced, yönetim karmaşıklığını azaltmanıza yardımcı olur.

  Daha küçük ölçekli şirketler için önceden yapılandırılmış ilkeler seçeneği sunuyoruz; bu sayede tüm ağınızda hızlı bir şekilde güvenlik uygulayabilir ve koruma sağlayabilirsiniz. Daha fazla esnekliğe ihtiyaç duyuyorsanız çözümü güvenlik ihtiyaçlarınıza göre ayarlamak için çok çeşitli kurulum seçenekleri sunuyoruz.

  HP ArcSight ve IBM QRadar gibi güvenlik bilgileri ve olay yönetimi (SIEM) ürünleri ile entegrasyon, kurumsal düzeydeki işletmelerin ihtiyaç duydukları gerçek zamanlı veri izleme özelliklerine sahip olmalarını sağlar.

- *İhtiyacınız olduğunda daha fazla güvenlik ekleme*

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

Hedeflenen Güvenlik Çözümleri ürün serimiz, ihtiyaç duyduğunuzda ekstra koruma ve yönetim teknolojisi eklemenizi sağlar; örneğin:

- Kaspersky Security for Virtualization
- Kaspersky Security for Mail Server
- Kaspersky Security for Storage
- Kaspersky Security for Internet Gateway
- Kaspersky Security for Collaboration

ÖZELLİKLER

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

Çok katmanlı güvenlik ve kontrol

Kaspersky Endpoint Security for Business Advanced, sürekli değişen siber tehdit ortamına karşı tüm cihazları ve ortamları korumak için birçok teknolojiyi bir araya getirir. Automatic Exploit Prevention, Host-Based Intrusion Prevention System ve diğerleri ile birlikte güvenlik kontrolleri, bir kötü amaçlı yazılım ihlali 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.

Şüpheli davranışı algılama

Kaspersky Endpoint Security for Business Advanced, 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 herhangi bir şüpheli etkinlik belirtilerine karşı izler. Kötü amaçlı dosya engellenir ve tüm eylemler otomatik olarak geri alınır.

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

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.

Ağ saldırılarını engelleme

Bağlantı noktası tarama, hizmet reddetme saldırıları ve arabellek taşması saldırıları gibi kurumsal ağları hedefleyen tehditlerin sayısı giderek artmakta. Ağ Saldırısı Engelleyici teknolojisi kurumsal ağınızdaki şüpheli davranışları algılar ve izler ve şüpheli bir davranış belirlendiğinde 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 da dahil belirli kaynaklar erişim için uygulama haklarını sınırlandırır. Uygulamaların ses ve video kayıt cihazlarına erişimi de kontrol edilebilir.

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

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. Yönetmeye ve ilkelerin ayarlanmasına yardımcı olmak için coğrafi kontroller ve saat kontrolleri Active Directory ile uyumlu hale getirilebilir.

- *Şifreleme ile gizli verileri üstün bir şekilde koruma*

Güçlü, uyumlu şifreleme

Kaspersky Endpoint Security for Business Advanced, AES-256 şifreleme algoritmasını kullanarak gizli bilgilerin güçlü şifreleme ile korunmasını sağlar. Dosyalar ve sistemlerin kaybolması veya çalınması durumunda yetkisiz kullanıcılar şifreli verilere erişemez. Şifreleme teknolojimiz FIPS 140-2 ile tamamen uyumludur.

Gelişmiş yönetilebilirlik için entegre şifreleme

Veri şifreleme kolayca yapılandırılabilir ve ağınızda çalışan diğer tüm Kaspersky Lab uç nokta güvenlik teknolojilerini kontrol etmek için kullandığınız yönetim konsolundan yönetilebilir. Şifreleme teknolojilerimiz, birleşik kod tabanı üzerinden şirket bünyesinde tasarlanmıştır; bu sayede şifreleme ayarları, kötü amaçlı yazılımdan koruma savunmalarınızı, uç noktası kontrollerinizi ve diğer uç noktası güvenlik teknolojilerini kapsayan ilkelere uygun şekilde kolaylıkla uygulanır.

Tam Disk ve Dosya Düzeyinde Şifreleme

Tam Disk Şifreleme (FDE), diskin fiziksel bölümlerinde çalışarak "her şeyi anında şifreleme" stratejisini kullanmayı kolaylaştırır. Dosya Düzeyinde Şifreleme (FLE), verilerin ağınızda güvenli bir şekilde

paylaşılmasını sağlar. Bir dosya şifrelendiğinde ek güvenlik için orijinal, şifrelenmemiş dosya sabit sürücüden silinebilir.

Çıkarılabilir Ortam Şifrelemesi

Çıkarılabilir Medya Şifreleme, çıkarılabilir cihazlardaki verileri korumak için Tam Disk Şifreleme ve Dosya Düzeyinde Şifreleme işlemlerini gerçekleştirebilir.

Taşınabilir mod şifreleme

Hassas verileri aktarmanız gerekiyorsa parola korumalı, şifreli, kendi kendine çıkarılabilen dosya paketleri ve klasörleri kolaylıkla oluşturabilirsiniz. Çıkarılabilir ortamda Dosya Düzeyinde Şifrelemeye yönelik özel bir taşınabilir mod, Kaspersky Security ürünleri çalıştırılmayan bilgisayarlara bile güvenli veri aktarımı sağlar.

Basitleştirilmiş oturum açma ve akılı kart/belirteç desteği

Kullanıcı kişisel bilgisayarını açarak kullanıcı adını ve parolasını girdiğinde, Tek Oturum Açma özelliği kullanıcının bilgisayarındaki sabit sürücüde bulunan şifreli verilere hemen erişmesini sağlar. Bu uygulama, şifreleme ve şifre çözme işlemlerinin kullanıcı için şeffaf bir şekilde gerçekleştirilmesini sağlar, etkinlik ve verimliliğin artmasına yardımcı olur. Akıllı kartlar ve belirteçlerle iki aşamalı kimlik doğrulaması da desteklenmektedir.

Microsoft BitLocker yönetimi

Microsoft Windows cihazlarında sabit sürücü şifreleme, Microsoft BitLocker teknolojisi kullanılarak yönetilebilir. Microsoft BitLocker yönetimi, işletim sistemine gömülü şifreleme teknolojisinin kullanımına olanak tanıyarak donanım uyumluluğunu iyileştirirken bir yandan da kullanıcı etkisini en aza indirir.

Intel AES-NI ve daha fazlası için destek

Kaspersky, Intel AES-NI'yı destekleyerek Intel ve AMD işlemci tabanlı sistemlerin büyük bölümünde verilerin şifreleme ve şifre çözme işlemlerinin daha hızlı yapılmasını sağlar**. Tam Disk Şifreleme Teknolojimiz, UEFI tabanlı platformları da desteklemektedir. QWERTY olmayan klavyeler de desteklenmektedir.

**AES-NI, tüm işlemciler tarafından desteklenmez.

- *Güvenliği güçlendirme ve BT sistem yönetimini genişletme*

Güvenlik açıklarını tanımlama ve yama işlemi gerçekleştirme

Hiçbir uygulama veya işletim sistemi, güvenlik açıklıklarından %100 arınmış değildir. Kötü amaçlı yazılım bu güvenlik açıklıklarından yararlanarak ağınıza sızabilir, iş istasyonlarınız ve sunucularınıza bulaşabilir ve işlerinizi aksatabilir. Bir kurumsal ağda birden fazla uygulama çalıştırıp, güvenlik açıklarını manuel olarak tanımlamak ve yazılımı güncel tutmak kullanışsız ve risklidir.

Kaspersky Endpoint Security for Business Advanced'de bulunan güvenlik açığı değerlendirmesi ve yama yönetimi özellikleri, yazılım güvenlik açıklarını azaltma sürecini otomatik hale getirir. Algılanan güvenlik açıkları otomatik olarak öncelik sırasına konularak ve yamalar ile güncellemeler otomatik olarak dağıtılır. Bu, kötü amaçlı yazılımlar tarafından istismar edilme olasılığını en aza indirir.

Donanım ve yazılım varlıklarınızı yönetme

Ağınızdaki tüm cihazlar otomatik olarak bulunup donanım ve yazılım envanterlerine kaydedilir. Donanım envanterinde her bir cihaz ile ilgili ayrıntılı bilgiler yar alır. Yazılım envanteri ise yazılım kullanımını kontrol etmenizi ve izinsiz uygulamaları engellemenizi sağlar. Ağınızda görünen konuk cihazlar bile otomatik olarak bulunabilir ve bu cihazlara kurumsal sistemleriniz ve verilerinizin güvenliğini tehlikeye atmadan erişim ayrıcalıkları verilebilir.

Uygulama dağıtımını optimize etme

Yazılımları vereceğiniz komutla dağıtabilir ya da dağıtım işlemini ofis saatlerinin dışında yapılacak şekilde zamanlayabilirsiniz. Bazı durumlarda, yüklenen yazılım paketini özelleştirmek için ek parametreler belirleyebilirsiniz. Herhangi bir masaüstü veya istemci bilgisayara güvenli, uzaktan bağlantıların kullanılması, sorunları hızlı bir şekilde gidermeye yardımcı olurken, yetkilendirme mekanizması yetkisiz uzaktan erişimi engeller. İzlenebilirlik sağlamak amacıyla uzak erişim oturumu sırasındaki tüm etkinlikler günlüğe kaydedilir.

İşletim sistemi dağıtımını otomatikleştirme ve optimize etme

Teknolojilerimiz, güvenli sistem görüntülerinin oluşturulması, depolanması ve klonlanması işlemlerini otomatik hale getirir ve merkezileştirir. Bu görüntüler özel bir envanterde saklanır ve dağıtım sırasında erişime hazırdır. İstemci iş istasyonu görüntü dağıtımı, daha önce ağda kullanılmış olan PXE sunucuları (Preboot eXecution Environment) veya Kaspersky'nin kendi özellikleri kullanılarak gerçekleştirilebilir. LAN Uyanması sinyallerinin kullanılması, görüntüleri otomatik olarak çalışma saatlerinden sonra dağıtmanıza olanak sağlar. UEFI desteği sunulmaktadır.

Uzak dağıtım ile trafiği azaltma

Yazılımları veya yamaları uzak bir ofise dağıtmanız gerektiğinde, tek bir yerel iş istasyonu tüm uzak ofis için güncelleme aracısı olarak hareket ederek ağınızdaki trafik düzeylerini azaltmanıza yardımcı olur.

SIEM sistemleriyle entegrasyon

Güvenlik bilgileri ve etkinlik yönetimi (SIEM) sistemleri, kurumsal düzeydeki işletmelere gerçek zamanlı izleme sağlama konusunda önemli bir rol oynar. Bu nedenle daha iyi raporlama ve güvenlik işlemlerini kolaylaştırmak için öncü SIEM sistemleriyle entegrasyonu ekledik.

- *Masaüstü bilgisayarın ötesinde güvenlik*

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

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 Advanced, 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 kaybolması durumunda kurumsal verileri güvende tutar. Şifreleme ve uzaktan çalıştırılan koruma özellikleri, kişisel verileri ve ayarları etkilemeden kurumsal konteyneri 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 Advanced, 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 Advanced; 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.

Farklı yöneticilere farklı sorumluluklar atama

Rol Tabanlı Erişim Kontrolü, güvenlik yönetimi ve sistem yönetimi sorumluluklarının birçok yönetici arasında bölünmesini sağlar. Örneğin, bir yöneticiye uç nokta güvenliği, uç nokta kontrolleri ve mobil güvenlik yönetimi işlemlerini atarken bir diğer yöneticiye ise veri şifreleme ve tüm sistem yönetimi işlevleri

sorumluluğu kalabilir. Kaspersky Security Center konsolu, her bir yöneticinin yalnızca kendi sorumluluklarıyla ilgili araçlara ve bilgilere erişebileceği şekilde kolayca özelleştirilebilir.

Yüksek düzeyde entegrasyon özelliği

Kaspersky Endpoint Security Advanced'de 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. Merkezileştirilmiş yönetim zamandan tasarruf sağlarken, BT ortamınızı korumak için daha fazlasını yapan sorunsuz bir şekilde entegre edilmiş güvenlik teknolojileri.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS

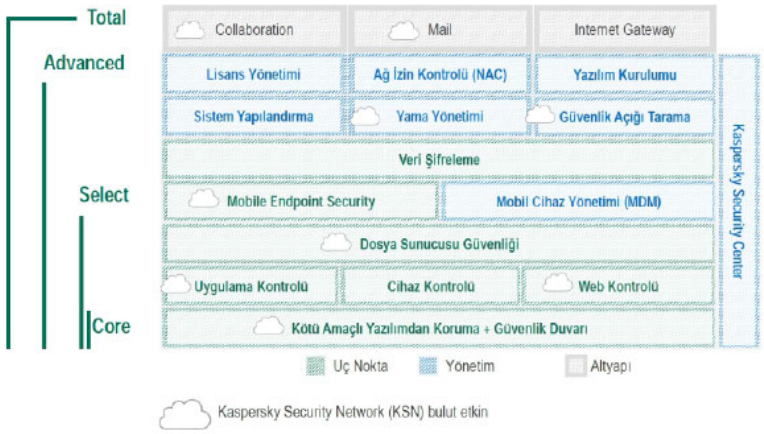
BT profesyonelleri mesleklerinin giderek daha güç hale geldiğini bize her gün hatırlatıyorlar.

Bu iş her zaman zordu ama ağ ve bağlı cihazlardaki karmaşıklık düzeyi kontrolden çıkmışa benziyor. Kaynak yokluğu, küçülen bütçeler ve ilkelerinizi sonuna kadar zorlayan kullanıcılar genellikle işini yapmalarının engellendiği duygusu uyandırır. Veriler, durağan hale gelince, artık birden fazla sistem, akıllı telefon ve tablet arasında taşınırlar ve çoğu zaman kafelerde, havaalanlarında kullanılır ve takside unutulurlar. Ve elbette, zayıf noktaları durdurmak için uygulama yamalama tam zamanlı bir iş haline gelir; bunu da ancak hangi uygulamaların kullanıldığını bilebiliyorsanız yapabilirsiniz. Bu karmaşıklık bazı kuruluşları güvenlikten ödün vermeye zorlamaktadır.

BU DEĞİŞİKLİK VE TEHDİTLERLE BAŞ ETMEK İÇİN KARMAŞIK OLMAYAN BİR YOLA GEREK DUYARSINIZ.

Yöneticiler Kaspersky Endpoint Security for Business ile kendi BT ortamlarını görebilir, denetleyebilir ve koruyabilirler. Gelişen güvenlik ve BT ihtiyaçlarınızı karşılamak için araçlar ve teknolojiler ilerleyen katmanlarda benzersiz şekilde dengelenir. Kaspersky işinizi kolaylaştırabilir.
Kaspersky müşterilerine ihtiyaç duydukları dünya sınıfı korumayı sağlayan, tümü aynı kod tabanından gelen ve birlikte çalışan ve bulut tabanlı Kaspersky Güvenlik Ağı destekli, kapsamlı bir teknoloji listesiyle iftihar ediyor.
Kısacası, dünyanızı görmenizi, denetlemenizi ve korumanızı kolaylaştıran, sektörün temelden itibaren kurulmuş ilk Güvenlik Platformunu veriyoruz

Ayrıntılar



SİZİN İÇİN HANGİ KATMAN DOĞRU?

Core KATMANI

Kaspersky'nin ödüllü temelinden ve güçlü, sunucu temelli olmayan kötü amaçlı yazılımlara karşı koruma
teknolojisi ve koruyucu güvenlik duvarından başlayıp, buna sezgisel yönetim konsolumuz Kaspersky
Security Center'ı ekliyoruz. Kötü amaçlı yazılımlara karşı koruma isteyen müşterilerimizin aradığı çözüm bu.

Select KATMANI

CORE katmanının üzerine Dosya Sunucusu Güvenliğini, Uygulama Beyaz Listesini ve Denetimini, Cihaz Denetimini ve İnternet Denetimini koruma listesine ekliyoruz. Ayrıca bir Uç Nokta Koruması ve Mobil Cihaz Yönetiminden (veya MDM) oluşan bir mobil koruma çözümünü ekliyoruz. İhtiyaçlarınız arasında bir mobil işgücünü korumak ve BT güvenliğini uygulamak da varsa, SELECT sizin için doğru katman olabilir.

Advanced KATMANI

ADVANCED katmanında Kaspersky dosya veya tam disk kriptolama biçiminde veri koruması ekliyor. Diğer bir yeni önerimiz, Kaspersky Systems Management güvenlikle BT verimliliğini birleştiriyor. Bu geniş özellikler kümesi, yöneticinin aşağıdakileri yapmasına olanak veren temel araçları içeriyor:

- Görüntü Yönetimi modülünü kullanarak görüntü oluşturma ve sistemlere dağıtma.
- Gelişmiş Zayıf Nokta Taraması ve Akıllı Yama Yönetiminin güçlü bileşimiyle donanım ve yazılımların zayıf noktalarını düzeltmeye öncelik verme.
- Yazılım Lisans Yönetimiyle lisans kullanımını ve uygunluğunu izleme.
- Ağ Giriş Denetimi (NAC) ile kullanıcılar ve konuklar için verilere ve altyapıya erişim ilkelerini ayarlama.
- Güncellemeleri ve yeni yazılımları kullanıcılara merkezi bir konsoldan uzaktan dağıtma ve kurma.

Kaspersky Total Security for Business

En iyi teklifimiz, Kaspersky Total Security for Business daha önceki tüm katmanları birleştirip, bunlara İnternet, Posta ve Birlikte Çalışan Sunucu koruması ekleyerek güvenlik pozisyonunuzu daha da geliştiriyor.
Bu, kapsamlı güvenlik ihtiyaçları olan ve her ağ düzeyi için en iyi korumayı talep eden kuruluşlar için mükemmel çözümdür.

Müşterileriniz için neden Kaspersky Seçmelisiniz?

Microsoft, IBM, Checkpoint ve Juniper dahil olmak üzere 80'den fazla BT, ağ güvenliği ve iletişim tedarikçisi kendi çözümlerinde yerleşik olarak Kaspersky Lab kötü amaçlı yazılımdan koruma teknolojisini kullanmayı seçti.

Teknolojileri satın alıp bunları entegre etmeye çalışmayız. Tüm özellik ve işlevler aynı ve tek bir kod tabanından oluşturulur.

ÖDÜLLÜ GÜVENLİK ÇÖZÜMLERİ

Gartner 2011 Magic Quadrant for Endpoint Protection Platforms LEADER

AV-TEST APPROVED CORPORATE ENDPOINT PROTECTION av-test.org

info@gvgbilisim.com.tr

GVG BİLİŞİM HİZMETLERİ

Kontrol Tamamen Elinizde